CCNA – Basic Questions

Question 1

What is the first 24 bits in a MAC address called?

A. NIC
B. BIA
C. OUI
D. VAI

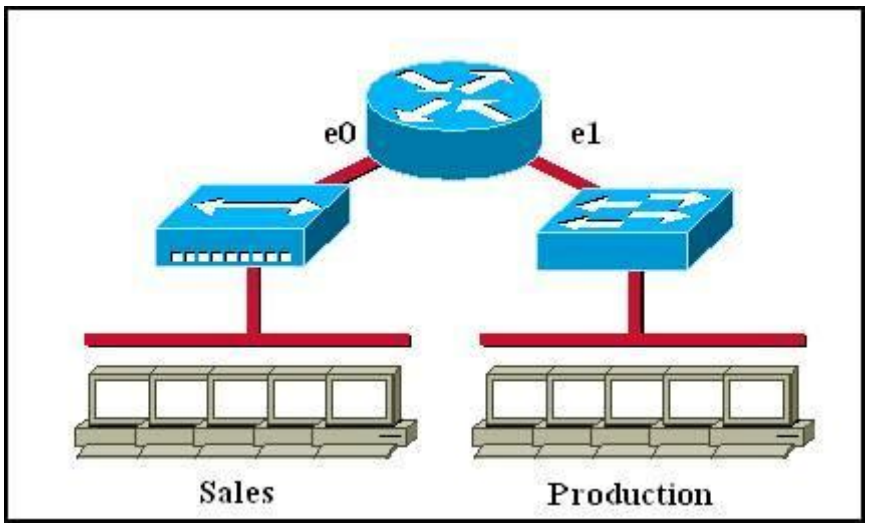
Answer: C

Explanation

Organizational Unique Identifier (OUI) is the first 24 bits of a MAC address for a network device, which indicates the specific vendor for that device as assigned by the Institute of Electrical and Electronics Engineers, Incorporated (IEEE). This identifier uniquely identifies a vendor, manufacturer, or an organization.

Question 2

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



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

Answer: A F

Explanation

Only router can break up broadcast domains so in the exhibit there are 2 broadcast domains: from e0 interface to the left is a broadcast domain and from e1 interface to the right is another broadcast domain -> A is correct.

Both router and switch can break up collision domains so there is only 1 collision domain on the left of the router (because hub doesn't break up collision domain) and there are 6 collision domains on the right of the router (1 collision domain from e1 interface to the switch + 5 collision domains for 5 PCs in Production) -> F is correct.

Question 3

Refer to the exhibit:

```
System flash director
File Length Name/status
1 3802992 c827v-y6-mz.121-1.XB
[3803056 bytes used,4585552 available, 8388608 total]
8192K bytes of processor board System flash(Read/Write)
```

The technician wants to upload a new IOS in the router while keeping the existing IOS. What is the maximum size of an IOS file that could be loaded if the original IOS is also kept in flash?

A. 3MB
B. 5MB
C. 7MB
D. 4MB

Answer: D

Explanation

From the exhibit we learn there are 4585552 bytes (over 4MB) available so it is only enough space for an IOS file of 4MB. If bigger file is copied then the existing IOS file will be erased (overwritten).

Question 4

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

```
Router# show interfaces ethernet 0
Ethernet0 is up, line protocol is up
Hardware is QUICC Ethernet, address is 00c0.ab73.dead (bia 0010.7bcc.7321)
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
<output omitted>
```

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

Answer: E

Explanation

The Maximum Transmission Unit (MTU) defines the maximum Layer 3 packet (in bytes) that the layer can pass onwards.

Question 5

A network interface port has collision detection and carrier sensing enabled on a shared twisted pair network. From this statement, what is known about the network interface port?

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

Answer: C

Explanation

Modern Ethernet networks built with switches and full-duplex connections no longer utilize CSMA/CD. CSMA/CD is only used in obsolete shared media Ethernet (which uses repeater or hub).

Question 6

In an Ethernet network, under what two scenarios can devices transmit? (Choose two)

A. when they receive a special token
B. when there is a carrier
C. when they detect no other devices are sending
D. when the medium is idle
E. when the server grants access

Answer: C D

Explanation

Ethernet network is a shared environment so all devices have the right to access to the medium. If more than one device transmits simultaneously, the signals collide and can not reach the destination.

If a device detects another device is sending, it will wait for a specified amount of time before attempting to transmit.

When there is no traffic detected, a device will transmit its message. While this transmission is occurring, the device continues to listen for traffic or collisions on the LAN. After the message is sent, the device returns to its default listening mode.

So we can see C and D are the correct answers. But in fact "answer C – when they detect no other devices are sending" and "when the medium is idle" are nearly the same.

Question 7

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

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

Answer: A E

Explanation

Physical addresses or MAC addresses are used to identify devices at layer 2 -> A is correct.

MAC addresses are only used to communicate on the same network. To communicate on different network we have to use Layer 3 addresses (IP addresses) -> B is not correct; E is correct.

Layer 2 frame and Layer 3 packet can be recognized via headers. Layer 3 packet also contains physical address -> C is not correct.

On Ethernet, each frame has the same priority to transmit by default -> D is not correct.

All devices need a physical address to identify itself. If not, they can not communicate -> F is not correct.

Question 8
Which two locations can be configured as a source for the IOS image in the boot system command? (Choose two)

A. RAM
B. NVRAM
C. flash memory
D. HTTP server
E. TFTP server
F. Telnet server

Answer: C E

Explanation

The following locations can be configured as a source for the IOS image:
+ Flash (the default location)
+ TFTP server
+ ROM (used if no other source is found)

Question 9

What is the difference between a CSU/DSU and a modem?

A. A CSU/DSU converts analog signals from a router to a leased line; a modem converts analog signals from a router to a leased line.
B. A CSU/DSU converts analog signals from a router to a phone line; a modem converts digital signals from a router to a leased line.
C. A CSU/DSU converts digital signals from a router to a phone line; a modem converts analog signals from a router to a phone line.
D. A CSU/DSU converts digital signals from a router to a leased line; a modem converts digital signals from a router to a phone line.

Answer: D

Question 10

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

Answer: A

Explanation

When you turn the router on, it runs through the following boot process.

The Power-On Self Test (POST) checks the router's hardware. When the POST completes successfully, the System OK LED indicator comes on.
The router checks the configuration register to identify where to load the IOS image from. A setting of 0×2102 means that the router will use information in the startup-config file to locate the IOS image. If the startup-config file is missing or does not specify a location, it will check the following locations for the IOS image:

1. Flash (the default location)
2. TFTP server
3. ROM (used if no other source is found)

The router loads the configuration file into RAM (which configures the router). The router can load a configuration file from:

+ NVRAM (startup-configuration file)
+ TFTP server
If a configuration file is not found, the router starts in setup mode.

CCNA – OSI & TCP/IP Model

Question 1

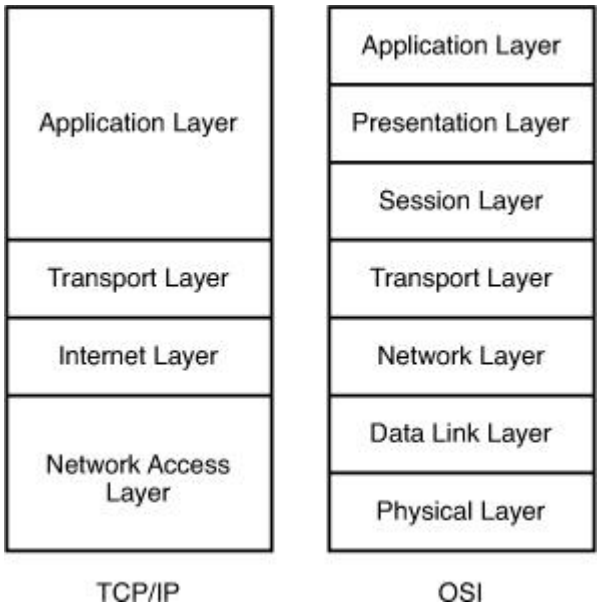
Where does routing occur within the DoD TCP/IP reference model?

A. application
B. internet
C. network
D. transport

Answer: B

Explanation

The picture below shows the comparison between TCP/IP model & OSI model. Notice that the Internet Layer of TCP/IP is equivalent to the Network Layer which is responsible for routing decision.



Question 2

Refer to exhibit.

```
Router#show running-config
Building configuration…
Current configuration : 659 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
```

```
service password-encryption
!
hostname Router
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
ip access-group 101 in
duplex auto
speed auto
!
access-1ist 101 deny tcp any any eq 22
access-1ist 101 permit ip any any
!
line con 0
password 7 0822455D0A16
login
line vty 0 4
login
line vty 5 14
login
!
end
```

A network administrator cannot establish a Telnet session with the indicated router. What is the cause of this failure?

A. A Level 5 password is not set.
B. An ACL is blocking Telnet access.
C. The vty password is missing.
D. The console password is missing.

Answer: C

Question 3

Before installing a new, upgraded version of the IOS, what should be checked on the router, and which command should be used to gather this information? (Choose two)

A. the amount of available ROM
B. the amount of available flash and RAM memory
C. the version of the bootstrap software present on the router
D. show version
E. show processes
F. show running-config

Answer: B D

Explanation

When upgrading new version of the IOS we need to copy the IOS to the Flash so first we have to check if the Flash has enough memory or not. Also running the new IOS may require more RAM than the older one so we should check the available RAM too. We can check both with the "show version" command.

Question 4

Refer to the exhibit. An administrator pings the default gateway at 10.10.10.1 and sees the output as shown. At which OSI layer is the problem?

```
C:\> ping 10.10.10.1
Pinging 10.10.10.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 10.10.10.1:
Packets: sent – 4, Received = 0, Lost – 4 (100% loss)
```

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

Answer: E

Explanation

The Network layer is responsible for network addressing and routing through the internetwork. So a ping fails, you may have an issue with the Network layer (although lower layers like Data Link & Physical may cause the problem).

Question 5

At which layer of the OSI model does PPP perform?

A. Layer 2
B. Layer 3
C. Layer 4
D. Layer 5

Answer: A

Question 6

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

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

Answer: A D

Explanation

The transport layer segments data into smaller pieces for transport. Each segment is assigned a sequence number, so that the receiving device can reassemble the data on arrival.

The transport layer also use flow control to maximize the transfer rate while minimizing the requirements to retransmit. For example, in TCP, basic flow control is implemented by acknowledgment by the receiver of the receipt of data; the sender waits for this acknowledgment before sending the next part.

-> A is correct.

The data link layer adds physical source and destination addresses and an Frame Check Sequence (FCS) to the packet (on Layer 3), not segment (on Layer 4) -> B is not correct.

Packets are created when network layer encapsulates a segment (not frame) with source and destination host addresses and protocol-related control information. Notice that the network layer encapsulates messages received from higher layers by placing them into datagrams (also called packets) with a network layer header -> C is not correct.

The Network layer (Layer 3) has two key responsibilities. First, this layer controls the logical addressing of devices. Second, the network layer determines the best path to a particular destination network, and routes the data appropriately.

-> D is correct.

The Physical layer (presentation layer) translates bits into voltages for transmission across the physical link -> E is not correct.

Question 7

A network administrator is verifying the configuration of a newly installed host by establishing an FTP connection to a remote server. What is the highest layer of the protocol stack that the network administrator is using for this operation?

A. application
B. presentation
C. session
D. transport
E. internet
F. data link

Answer: A

Explanation

FTP belongs to Application layer and it is also the highest layer of the OSI model.

Question 8

At which layer of the OSI model is RSTP used to prevent loops?

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

Answer: A

Question 9

Which layer in the OSI reference model is responsible for determining the availability of the receiving program and checking to see if enough resources exist for that communication?

A. transport
B. network
C. presentation
D. session
E. application

Answer: E

Question 10

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

Answer: D

Explanation

When using the term “frame” we can easily recognize it belongs to the Data Link layer. In this layer, an Frame Check Sequence (FCS) field is added to the frame to verify that the frame data is received correctly.

CCNA – IOS Questions

Question 1

Which command encrypts all plaintext passwords?

A. Router# service password-encryption
B. Router(config)# password-encryption
C. Router(config)# service password-encryption
D. Router# password-encryption

Answer: C

Question 2

What can be done to secure the virtual terminal interfaces on a router? (Choose two)

A. Administratively shut down the interface.
B. Physically secure the interface.
C. Create an access list and apply it to the virtual terminal interfaces with the access-group command.
D. Configure a virtual terminal password and login process.
E. Enter an access list and apply it to the virtual terminal interfaces using the access-class command.

Answer: D E

Explanation

It is a waste to administratively shut down the interface. Moreover, someone can still access the virtual terminal interfaces via other interfaces -> A is not correct.

We can not physically secure a virtual interface because it is "virtual" -> B is not correct.

To apply an access list to a virtual terminal interface we must use the "access-class" command. The "access-group" command is only used to apply an access list to a physical interface -> C is not correct; E is correct.

The most simple way to secure the virtual terminal interface is to configure a username & password to prevent unauthorized login -> D is correct.

Question 3

Refer to the exhibit. Why is flash memory erased prior to upgrading the IOS image from the TFTP server?

```
Router# copy tftp flash
Address or name of remote host []? 192.168.2.167
Source filename []? c1600-k8sy-mz.123-16a.bin
Destination filename [c1600-k8sy-mz.123-16a.bin]?
Accessing tftp://192.168.2.167/ c1600-k8sy-mz.l23-16a.bin…
Erasing flash before copying? [confirm]
Erasing the flash filesystem will remove all files! continue? [confirm]
Erasing device
Eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
Eeeeeeeeeeeeeeeeeeeeeeeeeeeeee …erased
Erase of flash: complete
Loading c1600-k8sy-mz.l23-16a.bin from 192.168.2.167 (via Ethernet0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK – 6888962/13777920 bytes]

verifying checksum… OK (0x7BF3)
6888962 bytes copied in 209.920 secs (32961 bytes/sec)
Router#
```

A. The router cannot verify that the Cisco IOS image currently in flash is valid
B. Flash memory on Cisco routers can contain only a single IOS image.
C. Erasing current flash content is requested during the copy dialog.
D. In order for the router to use the new image as the default, it must be the only IOS image in flash.

Answer: C

Explanation

During the copy process, the router asked “Erasing flash before copying? [confirm]” and the administrator confirmed (by pressing Enter) so the flash was deleted.

Note: In this case, the flash has enough space to copy a new IOS without deleting the current one. The current IOS is deleted just because the administrator wants to do so. If the flash does not have enough space you will see an error message like this:

```
%Error copying tftp://192.168.2.167/ c1600-k8sy-mz.l23-16a.bin (Not enough space on device)
```

Question 4

How does using the **service password encryption** command on a router provide additional security?

A. by encrypting all passwords passing through the router
B. by encrypting passwords in the plain text configuration file
C. by requiring entry of encrypted passwords for access to the device
D. by configuring an MD5 encrypted key to be used by routing protocols to validate routing exchanges
E. by automatically suggesting encrypted passwords for use in configuring the router

Answer: B

Explanation

By using this command, all the (current and future) passwords are encrypted. This command is primarily useful for keeping unauthorized individuals from viewing your password in your configuration file.

Question 5

What is a global command?

A. a command that is available in every release of IOS, regardless of the version or deployment status
B. a command that can be entered in any configuration mode
C. a command that is universal in application and supports all protocols
D. a command that is implemented in all foreign and domestic IOS versions
E. a command that is set once and affects the entire router

Answer: E

Explanation

A global command is a command in this form:

Device(config)#

This mode can affect the entire router/switch.

For more information about modes in Cisco devices, please read my Cisco Command Line Interface CLI tutorial.

Question 6

Refer to the exhibit.

```
line vty 0 4
password 7 030752180599
login
transport input ssh
```

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

Answer: D

Question 7

Which router IOS commands can be used to troubleshoot LAN connectivity problems? (Choose three)

A. ping
B. tracert
C. ipconfig
D. show ip route
E. winipcfg
F. show interfaces

Answer: A D F

Explanation

The ping command can be used to test if the local device can reach a specific destination -> A is correct.

"tracert" is not a valid command in Cisco IOS commands, the correct command should be "traceroute" -> B is not correct.

The ipconfig command is not a valid command in Cisco IOS too -> C is not correct.

The "show ip route" command can be used to view the routing table of the router. It is a very useful command to find out many connectivity problems (like directly connected networks, learned network via routing protocols…) -> D is correct.

"winipcfg" is an old tool in Windows 95/98 to view IP settings of the installed network interfaces. But it is not a valid command in Cisco IOS commands -> E is not correct.

The "show interfaces" command is used to check all the interfaces on the local device only. It has very limited information to trouble LAN connectivity problem but it is the most reasonable to choose -> F is acceptable.

Question 8

Which command shows your active Telnet connections?

A. show sessions
B. show cdp neighbors
C. show users
D. show queue

Answer: A

Question 9

Which command would you configure globally on a Cisco router that would allow you to view directly connected Cisco devices?

A. enable cdp
B. cdp enable
C. cdp run
D. run cdp

Answer: C

Question 10

A network administrator needs to allow only one Telnet connection to a router. For anyone viewing the confguration and issuing the show run command, the password for Telnet access should be encrypted. Which set of commands will accomplish this task?

A. service password-encryption
access-list 1 permit 192.168.1.0 0.0.0.255
line vty 0 4
login
password cisco
access-class 1

B. enable password secret
line vty 0
login
password cisco

C. service password-encryption
line vty 1
login
password cisco

D. service password-encryption
line vty 0 4
login
password cisco

Answer: C

Question 11

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

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

Answer: E

Explanation

The secret password (configured by the command "enable secret ") is always encrypted even if the "service password-encryption" command is not used. Moreover, the secret password is not removed from the configuration with this command, we still see it in encrypted form in the running-config -> D is not correct.

The “enable password ” does not encrypt the password and can be viewed in clear text in the running-config. By using the “service password-encryption” command, that password is encrypted (both current and future passwords) -> A is not correct, E is correct.

Answer B – Only the enable password will be encrypted seems to be correct but it implies the secret password will not be encrypted and stay in clear text, which is not correct.

For your information, the secret password is encrypted with MD5 one-way hash algorithm which is harder to break than the encryption algorithm used by the “service password-encryption” command.

CCNA – WAN Questions

Question 1

Which PPP subprotocol negotiates authentication options?

A. NCP
B. ISDN
C. SUP
D. LCP
E. DLCI

Answer: D

Question 2

A network administrator needs to configure a serial link between the main office and a remote location. The router at the remote office is a non-Cisco router. How should the network administrator configure the serial interface of the main office router to make the connection?

A. Main(config)# interface serial 0/0
Main(config-if)# ip address 172.16.1.1 255.255.255.252
Main(config-if)# no shut

B. Main(config)# interface serial 0/0
Main(config-if)# ip address 172.16.1.1 255.255.255.252
Main(config-if)# encapsulation ppp
Main(config-if)# no shut

C. Main(config)# interface serial 0/0
Main(config-if)# ip address 172.16.1.1 255.255.255.252
Main(config-if)# encapsulation frame-relay
Main(config-if)# authentication chap
Main(config-if)# no shut

D. Main(config)# interface serial 0/0
Main(config-if)#ip address 172.16.1.1 255.255.255.252
Main(config-if)#encapsulation ietf
Main(config-if)# no shut

Answer: B

Question 3

Which two options are valid WAN connectivity methods? (Choose two)

A. PPP
B. WAP
C. DSL
D. L2TPv3
E. Ethernet

Answer: A C

Question 4

Which Layer 2 protocol encapsulation type supports synchronous and asynchronous circuits and has built-in security mechanisms?
A. HDLC
B. PPP
C. X.25
D. Frame Relay

Answer: B

Explanation

PPP supports both synchronous (like analog phone lines) and asynchronous circuits (such as ISDN or digital links). With synchronous circuits we need to use clock rate.

Note: Serial links can be synchronous or asynchronous. Asynchronous connections used to be only available on low-speed (<2MB) serial interfaces, but now, there are the new HWICs (High-Speed WAN Interface Cards) which also support asynchronous mode. To learn more about them please visit http://www.cisco.com/en/US/prod/collateral/modules/ps5949/ps6182/prod_qas0900aecd80274424.html.

Question 5

Which command is used to enable CHAP authentication with PAP as the fallback method on a serial interface?

A. (config-if)# authentication ppp chap fallback ppp
B. (config-if)# authentication ppp chap pap
C. (config-if)# ppp authentication chap pap
D. (config-if)# ppp authentication chap fallback ppp

Answer: C

Explanation

The command "ppp authentication chap pap" command indicates the CHAP authentication is used first. If it fails or is rejected by other side then uses PAP instead. If you want to use PAP first (then CHAP) you can use the "ppp authentication pap chap" command.

Question 6

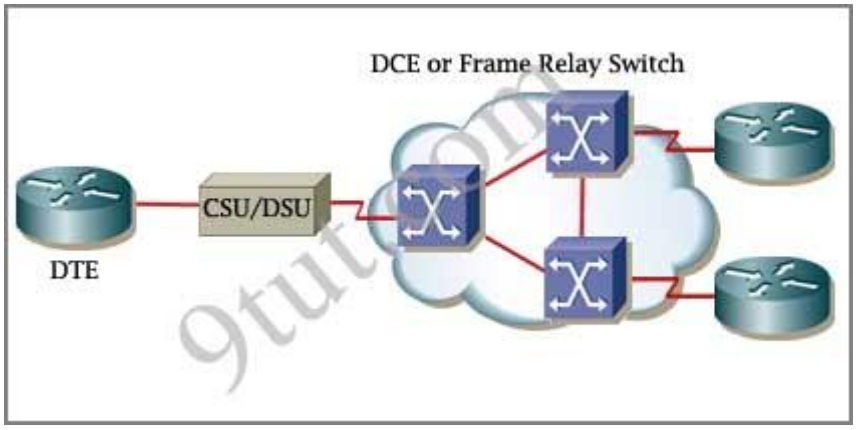
Which of the following describes the roles of devices in a WAN? (Choose three.)

A. A CSU/DSU terminates a digital local loop
B. A modem terminates a digital local loop
C. A CSU/DSU terminates an analog local loop
D. A modem terminates an analog local loop
E. A router is commonly considered a DTE device
F. A router is commonly considered a DCE device

Answer: A D E

Explanation

The idea behind a WAN is to be able to connect two DTE networks together through a DCE network. The network's DCE device (includes CSU/DSU) provides clocking to the DTE-connected interface (the router's serial interface).



Question 7

Which two statements about using the CHAP authentication mechanism in a PPP link are true? (Choose two)

A. CHAP uses a two-way handshake.
B. CHAP uses a three-way handshake.
C. CHAP authentication periodically occurs after link establishment.
D. CHAP authentication passwords are sent in plaintext.
E. CHAP authentication is performed only upon link establishment.
F. CHAP has no protection from playback attacks.

Answer: B C

CCNA – Switch Questions

Question 1

Refer to the exhibit.

```
Switch-1# show mac address-table
Dynamic Addresses Count:                     3
Secure Addresses (User-defined) Count:       0
Static Addresses (User-defined) Count:       0
System Self Addresses Count:                 41
Total Mac addresses:                         50
Non-static Address Table:
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
0010.0de0.e289       Dynamic       1     FastEthernet0/1
0010.7b00.1540       Dynamic       2     FastEthernet0/3
0010.7b00.1545       Dynamic       2     FastEthernet0/2
```

Switch-1 needs to send data to a host with a MAC address of 00b0.d056.efa4. What will Switch-1 do with this data?

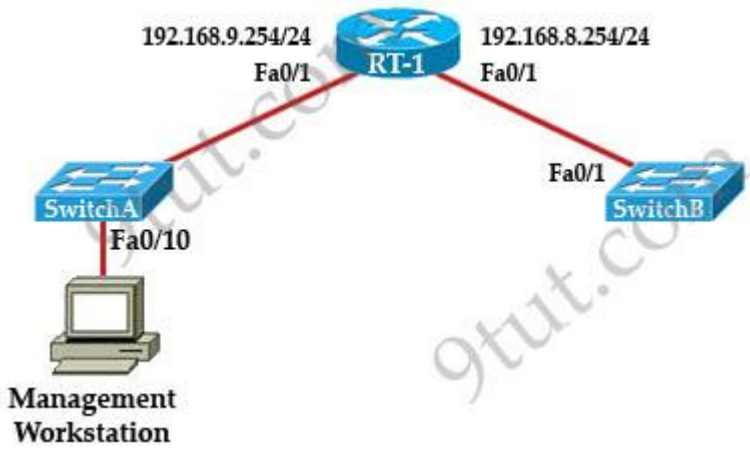
A. Switch-1 will drop the data because it does not have an entry for that MAC address.
B. Switch-1 will forward the data to its default gateway.
C. Switch-1 will flood the data out all of its ports except the port from which the data originated.
D. Switch-1 will send an ARP request out all its ports except the port from which the data originated.

Answer: C

Explanation

The MAC address of 00b0.d056.efa4 has not been learned in its MAC address table so Switch-1 will broadcast the frame out all of its ports except the port from which the data originated.

Question 2



A technician has installed SwitchB and needs to configure it for remote access from the management workstation connected SwitchA. Which set of commands is required to accomplish this task?

A.
SwitchB(config)#interface FastEthernet 0/1
SwitchB(config)#ip address 192.168.8.252 255.255.255.0
SwitchB(config)#no shutdown

B.
SwitchB(config)#ip default-gateway 192.168.8.254
SwitchB(config)#interface vlan 1
SwitchB(config)#ip address 192.168.8.252 255.255.255.0
SwitchB(config)#no shutdown

C.
SwitchB(config)#interface vlan 1
SwitchB(config)#ip address 192.168.8.252 255.255.255.0

SwitchB(config)#ip default-gateway 192.168.8.254 255.255.255.0
SwitchB(config)#no shutdown

D.
SwitchB(config)#ip default-network 192.168.8.254
SwitchB(config)#interface vlan 1
SwitchB(config)#ip address 192.168.8.252 255.255.255.0
SwitchB(config)#no shutdown

Answer: B

Explanation

To remote access to SwitchB, it must have a management IP address on a VLAN on that switch. Traditionally, we often use VLAN 1 as the management VLAN (but in fact it is not secure).

In the exhibit, we can recognize that the Management Workstation is in a different subnet from the SwitchB. For intersubnetwork communication to occur, you must configure at least one default gateway. This default gateway is used to forward traffic originating from the switch only, not to forward traffic sent by devices connected to the switch.

Question 3

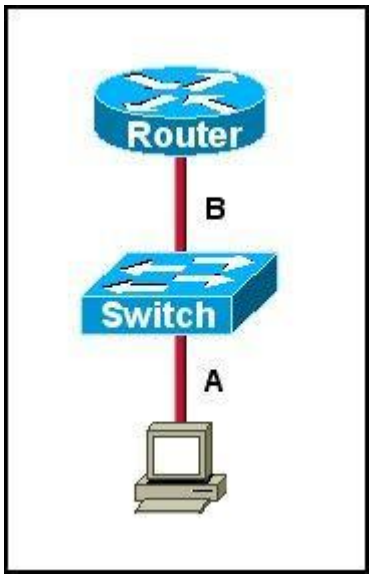
A switch is configured with all ports assigned to vlan 2 with full duplex FastEthernet to segment existing departmental traffic. What is the effect of adding switch ports to a new VLAN on the switch?

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

Answer: D

Question 4

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



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

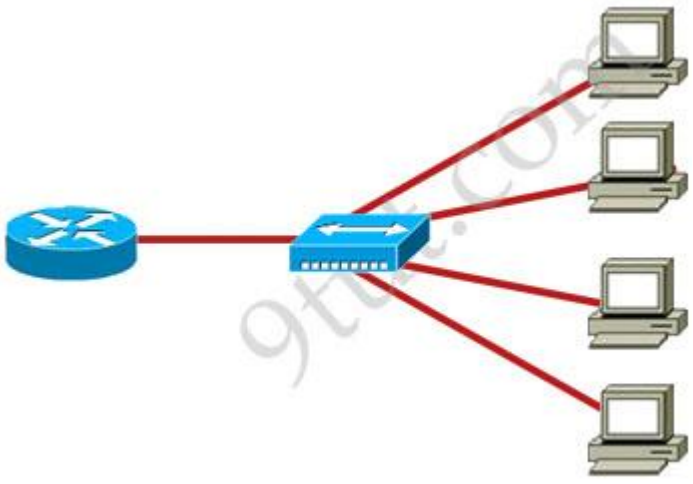
Answer: B D F

Explanation

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

Question 5

Refer to the exhibit.



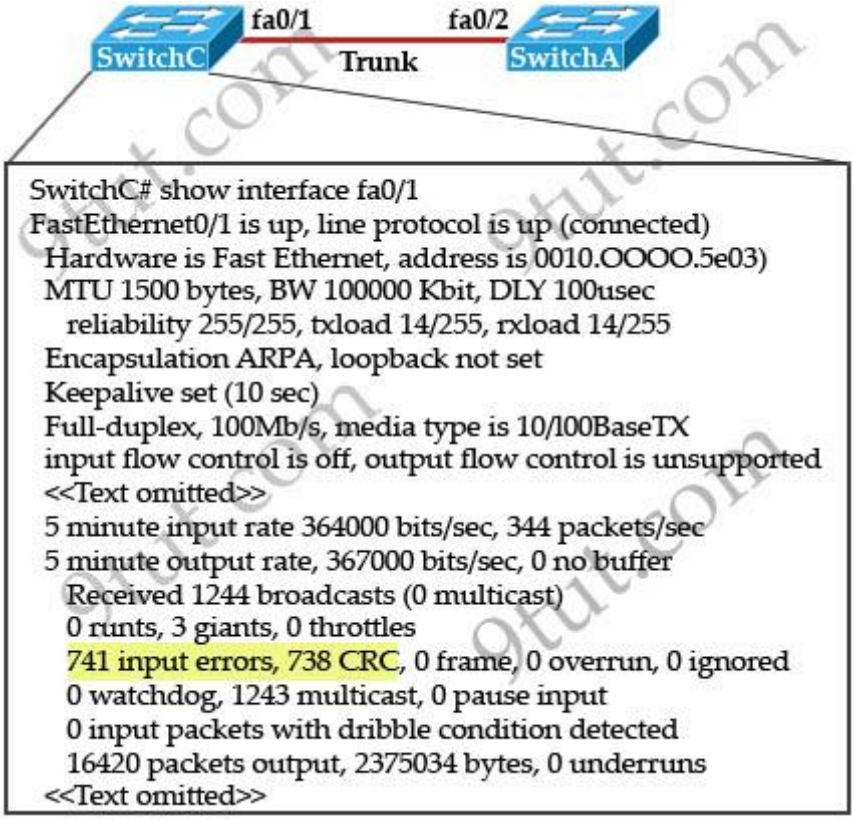
What two results would occur if the hub were to be replaced with a switch that is configured with one Ethernet VLAN? (Choose two)

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

Answer: C D

Question 6

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



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

Answer: C

Question 7

Which three statements accurately describe layer 2 Ethernet switches? (choose three)

A. Microsegmentation decreases the number of collisions on the network.
B. If a switch receives a frame for an unknown destination.it uses ARP to resolve the address.
C. Spanning Tree Protocol allows switches to automatically share vlan information.
D. In a properly functioning network with redundant switched paths, each switched segment will contain one root bridge with all its ports in the forwarding state. All other switches in that broadcast domain will have only one root port.
E. Establishing vlans increases the number of broadcast domains.
F. Switches that are configured with vlans make forwarding decisions based on both layer 2 and layer 3 address information.

Answer: A D E

Question 8

Why will a switch never learn a broadcast address?

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

Answer: C

Question 9

Refer to the exhibit:

```
Switch1# show mac address-table
System Self Addresses Count: 41
Total MAC addresses: 50
Non-static Address Table:
Destination Address  AddressType  VLAN  Destination Port
-------------------  -----------  ----  --------------------
00A0.0de0.e289       Dynamic      1     FastEthernet0/1
00A0.7b00.1540       Dynamic      2     FastEthernet0/5
00A0.7b00.1545       Dynamic      2     FastEthernet0/5
00A0.5c74.0076       Dynamic      1     FastEthernet0/1
00A0.5cf4.0077       Dynamic      3     FastEthernet0/1
00A0.5cf4.1315       Dynamic      1     FastEthernet0/1
00A0.70cb.f301       Dynamic      2     FastEthernet0/1
00A0.70cb.3f01       Dynamic      5     FastEthernet0/2
00A0.1e42.9978       Dynamic      4     FastEthernet0/1
00A0.1e9f.3900       Dynamic      3     FastEthernet0/1
00A0.70cb.33f1       Dynamic      6     FastEthernet0/3
00A0.70cb.103f       Dynamic      6     FastEthernet0/4

<output omitted>

Switch1#show cdp neighbors
Capability Codes:    R - Router, T - Trans Bridge, B - Source Route Bridge
                     S - Switch, H - Host, I - IGMP, r - Repeater

Device ID   Local Intrfce   Holdtime   Capability   Platform   Port ID
Switch2     Fas 0/1         157            S        2950-12    Fas 0/1
Switch3     Fas 0/2         143            S        2950-12    Fas 0/5

Switch1#
```

Which two statements are true of the interfaces on Switch1? (Choose two)

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

Answer: C F

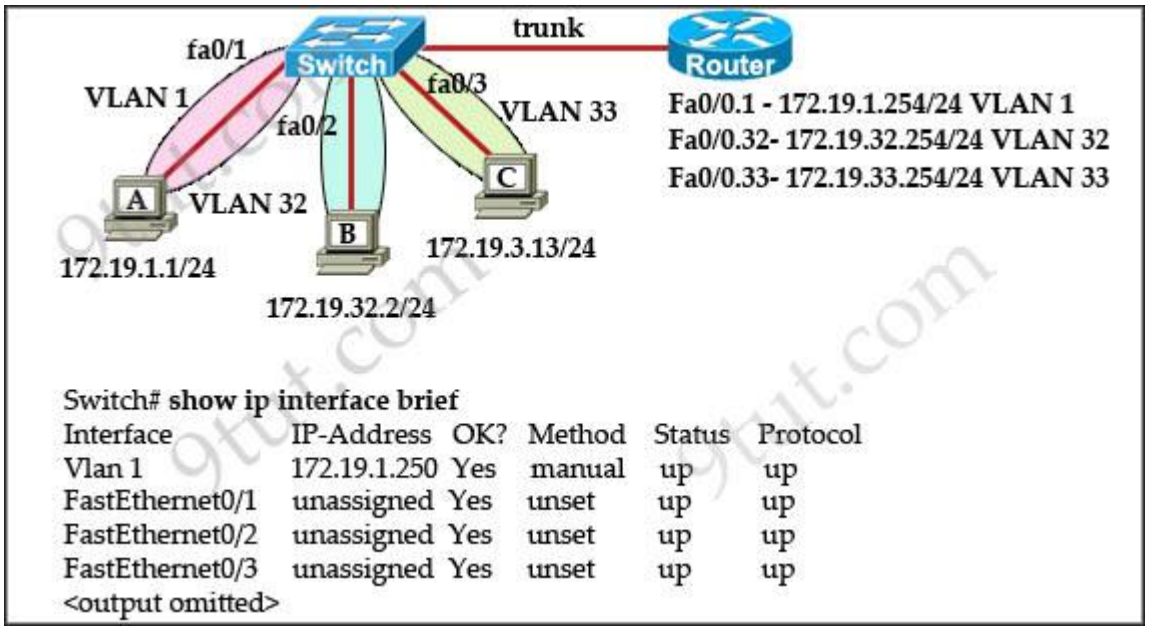
Explanation

FastEthernet0/1 can receive traffic from multiple VLANs -> it is configured as a trunk.

There are two MAC addresses learned from FastEthernet0/5 -> a hub is used on this port.

Question 10

The network administrator normally establishes a Telnet session with the switch from host A. The administrator's attempt to establish a connect via Telnet to the switch from host B fails, but pings from host B to other two hosts are successful. What is the issue for this problem?



Switch# **show ip interface brief**

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan 1	172.19.1.250	Yes	manual	up	up
FastEthernet0/1	unassigned	Yes	unset	up	up
FastEthernet0/2	unassigned	Yes	unset	up	up
FastEthernet0/3	unassigned	Yes	unset	up	up

<output omitted>

A. Host B and the switch need to be in the same subnet.
B. The switch needs an appropriate default gateway assigned.
C. The switch interface connected to the router is down.
D. Host B need to be assigned an IP address in vlan 1.

Answer: B

Explanation

Host A (172.19.1.1) and the management IP address of the Switch (172.19.1.250) are in the same subnet so telnet from host A to the switch can be successful even if a default gateway is not set on host A.

But host B (172.19.32.2) and the management IP address of the Switch (172.19.1.250) are not in the same subnet so host B needs a default gateway to telnet to the switch. The default gateway on host B should be 172.19.32.254.

CCNA – Switch Questions 2

Question 1

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

A. source MAC address
B. source IP address
C. source switch port
D. destination IP address
E. destination port address
F. destination MAC address

Answer: F

Question 2

The network administrator cannot connect to Switch1 over a Telnet session, although the hosts attached to Switch1 can ping the interface Fa0/0 of the router. Given the information in the graphic and assuming that the router and Switch2 are configured properly, which of the following commands should be issued on Switch1 to correct this problem?

A. Switch1 (config)# line con0
Switch1 (config-line)# password cisco
Switch1 (config-line)#login

B. Switch1 (config)# interface fa0/1
Switch 1(config-if)# ip address 192.168.24.3 255.255.255.0

C. Switch1 (config)# ip default-gateway 192.168.24.1

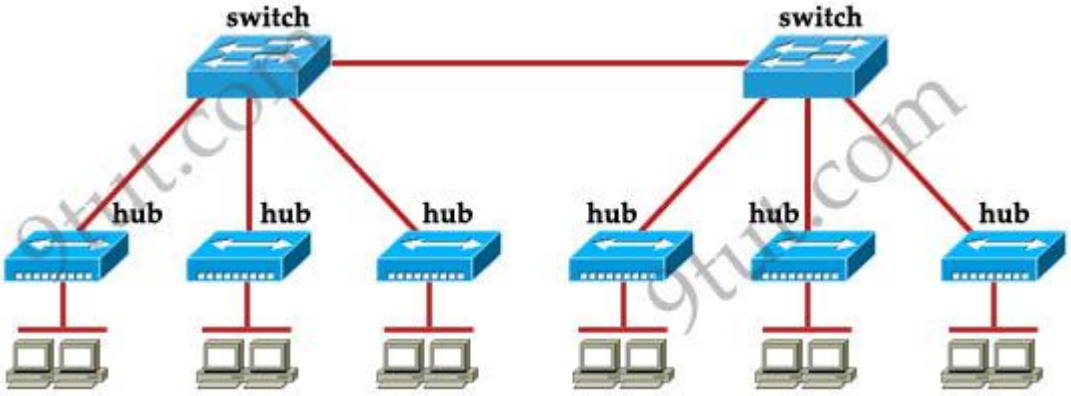
D. Switch1 (config)# interface fa0/1
Switch 1(config-if)# duplex full
Switch 1(config-if)# speed 100

E. Switch1 (config)# interface fa0/1
Switch 1(config-if)# switchport mode trunk

Answer: C

Question 3

How many broadcast domains are shown in the graphic assuming only the default vlan is configured on the switches?



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

Answer: A

Explanation

Only router can break up broadcast domains but in this exhibit no router is used so there is only 1 broadcast domain.

For your information, there are 7 collision domains in this exhibit (6 collision domains between hubs & switches + 1 collision between the two switches).

Question 4

Refer to the exhibit. Which of these statements correctly describes the state of the switch once the boot process has been completed?

```
00:00:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
00:00:40: %SPANTREE-5-EXTENDED_SYSID: Extended SysId enabled for type vlan
00:00:42: %SYS-5-CONFIG_I: Configured from memory by console
00:00:42: %SYS-5-RESTART: System restarted --
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(25)SEE2, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 28-Jul-06 11:57 by yenanh
00:00:44: %LINK-5-CHANGED: Interface Vlan1, changed state to administratively down
00:00:44: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
00:00:44: %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to up
00:00:44: %LINK-3-UPDOWN: Interface FastEthernet0/11, changed state to up
00:00:45: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
00:00:45: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
00:00:45: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/11, changed state to up
00:00:48: %LINK-3-UPDOWN: Interface FastEthernet0/12, changed state to up
00:00:49: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/12, changed state to up
```

A. As FastEthernet0/12 will be the last to come up, it will not be blocked by STP.
B. Remote access management of this switch will not be possible without configuration change.
C. More VLANs will need to be created for this switch.
D. The switch will need a different IOS code in order to support VLANs and STP.

Answer: B

Explanation

From the output we notice that the administrator has just shut down Interface Vlan1, which is the default VLAN so no one can access it remotely (like telnet) -> B is correct.

Answer A is not correct as STP calculation does not depend on which port comes up first or last. STP recalculates when there is a change in the network.

A normal switch can operate without VLAN -> C is not correct.

This IOS does support VLAN because it has VLAN 1 on it -> D is not correct.

CCNA – VLAN Questions

Question 1

What are three benefits of implementing VLANs? (Choose three)

A. A more efficient use of bandwidth can be achieved allowing many physical groups to use the same network infrastructure
B. Broadcast storms can be mitigated by decreasing the number of broadcast domains,thus increasing their size.
C. A higher level of network security can be reached by separating sensitive data traffic from other network traffic.
D. Port-based vlans increase switch-port use efficient,thanks to 802.1Q trunks
E. A more efficient use of bandwidth can be achieved allowing many logical networks to use the same network infrastructure.
F. Broadcast storms can be mitigated by increasing the number of broadcast domains,thus reducing their size.
G. VLANs make it easier for IT staff to configure new logical groups,because the vlans all belong to the same broadcast domain.

Answer: C E F

Question 2

VLAN 3 is not yet configured on your switch. What happens if you set the **switchport access vlan 3** command interface configuration mode?

A. The command is accepted and the respective VLAN is added to vlan.dat.
B. The command is rejected.
C. The command is accepted and you must configure the VLAN manually.
D. The port turns amber.

Answer: A

Explanation

Even VLAN 3 is not yet configured on the switch, we can set the switchport access vlan 3 command without no problem and it also displays when we type the “show running-config” command.

Question 3

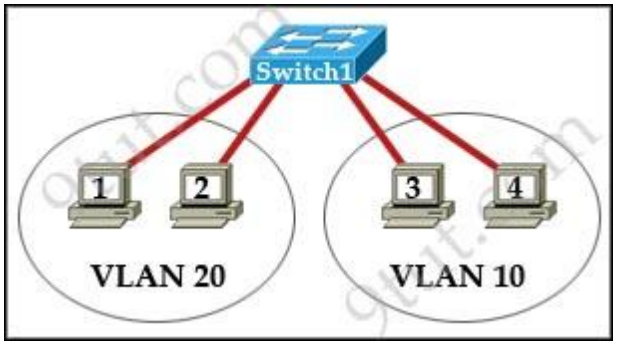
What are three advantages of VLANs? (Choose three)

A. VLANs establish broadcast domains in switched networks.
B. VLANs utilize packet filtering to enhance network security.

C. VLANs provide a method of conserving IP addresses in large networks.
D. VLANs provide a low-latency internetworking alternative to routed networks.
E. VLANs allow access to network services based on department, not physical location.
F. VLANs can greatly simplify adding, moving, or changing hosts on the network.

Answer: A E F

Question 4



On corporate network, hosts on the same VLAN can communicate with each other, but they are unable to communicate with hosts on different VLANs. What is needed to allow communication between the VLANs?

A. a router with subinterfaces configured on the physical interface that is connected to the switch
B. a router with an IP address on the physical interface connected to the switch
C. a switch with an access link that is configured between the switches
D. a switch with a trunk link that is configured between the switches

Answer: A

Question 5

Cisco Catalyst switches CAT1 and CAT2 have a connection between them using ports Fa0/13. An 802.1Q trunk is configured between the two switches. On CAT1, VLAN 10 is chosen as native, but on CAT2 the native VLAN is not specified. What will happen in this scenario?

A. 802.1Q giants frames could saturate the link.
B. VLAN 10 on CAT1 and VLAN 1 on CAT2 will send untagged frames.
C. A native VLAN mismatch error message will appear.
D. VLAN 10 on CAT1 and VLAN 1 on CAT2 will send tagged frames.

Answer: C

Explanation

A “native VLAN mismatch” error will appear by CDP if there is a native VLAN mismatch on an 802.1Q link. “VLAN mismatch” can cause traffic from one vlan to leak into another vlan.

Question 6

Which of the following are benefits of VLANs? (Choose three)

A. They increase the size of collision domains.
B. They allow logical grouping of users by function.
C. They can enhance network security.
D. They increase the size of broadcast domains while decreasing the number of collision domains.
E. They increase the number of broadcast domains while decreasing the size of the broadcast domains.
F. They simplify switch administration.

Answer: B C E

Explanation

When using VLAN the number and size of collision domains remain the same -> A is not correct.

VLANs allow to group users by function, not by location or geography -> B is correct.

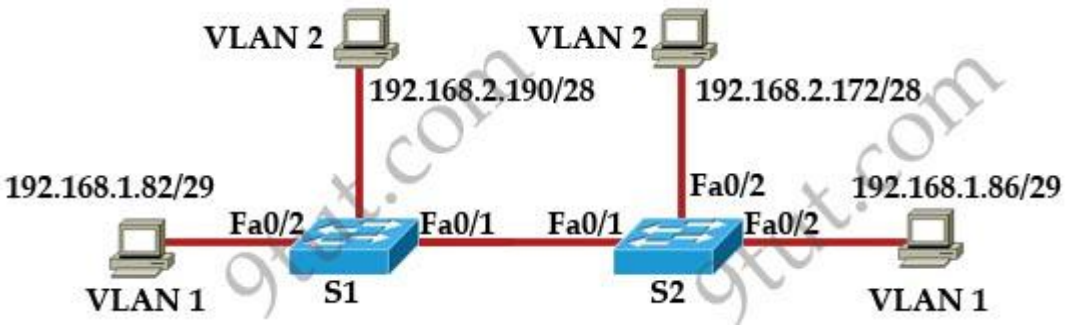
VLANs help minimize the incorrect configuration of VLANs so it enhances the security of the network -> C is correct.

VLAN increases the size of broadcast domains but does not decrease the number of collision domains -> D is not correct.

VLANs increase the number of broadcast domains while decreasing the size of the broadcast domains which increase the utilization of the links. It is also a big advantage of VLAN -> E is correct.

VLANs are useful but they are more complex and need more administration -> F is not correct.

Question 7



```
S1#show interface trunk
Port        Mode         Encapsulation        Status        Native vlan
Fa0/1       on           802. 1q              Trunking      1

Port        Vlans allowed a trunk
Fa0/1       1.1005

Port        Vlans allowed and active in management domain
Fa0/1       12
```

```
S2#show interface trunk
Port        Mode         Encapsulation        Status        Native vlan
Fa0/1       on           802. 1q              Trunking      2

Port        Vlans allowed a trunk
Fa0/1       1.1005

Port        Vlans allowed and active in management domain
Fa0/1       12
```

A frame from VLAN1 of switch S1 is sent to switch S2 where the frame received on VLAN2. What causes this behavior?

A. trunk mode mismatches
B. vlans that do not correspond to a unique IP subnet
C. native vlan mismatches
D. allowing only vlan 2 on the destination.

Answer: C

Explanation

For 802.1q encapsulation, the native VLAN must matched at both side; otherwise the link will not work. In this case the native VLAN of S1 is 1 while the native VLAN of S2 is 2.

Question 8

Which statement about vlan operation on Cisco Catalyst switches is true?

A. when a packet is received from an 802.1Q trunk, the vlan id can be determined from the source MAC address table.
B. unknown unicast frames are retransmitted only to the ports that belong to the same vlan.
C. ports between switches should be configured in access mode so that vlans can span across the ports.
D. broadcast and multicast frames are retransmitted to ports that are configured on different vlan.

Answer: B

Explanation

Answer A is not correct because when a packet is received from an 802.1Q trunk, it always carries VLAN ID information in the VLAN tag portion so the switch does not need to look up its source MAC address table to determine the VLAN ID of that packet.

Question 9

Which two benefits are provided by creating VLANs? (Choose two)
A. added security
B. dedicated bandwidth
C. provides segmentation
D. allows switches to route traffic between subinterfaces
E. contains collisions

Answer: A C

Question 10

Assuming the default switch configuration which vlan range can be added modified and removed on a Cisco switch?

A. 2 through 1001
B. 1 through 1001
C. 1 through 1002
D. 2 through 1005

Answer: A

Explanation

VLAN 1 is the default VLAN on Cisco switch. It always exists and can not be added, modified or removed.

VLANs 1002-1005 are default VLANs for FDDI & Token Ring and they can’t be deleted or used for Ethernet.

```
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig1/1, Gig1/2
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0
```

CCNA – Trunking Questions

Question 1

Refer to the topology and router output shown in the exhibit:

Sw11# show vlan brief

VLAN	Name	Status	Ports
1	default	active	
10	Marketing	active	Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15
15	Accounting	active	Fa0/16, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/24
20	Admin	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Switch#

A technician is troubleshooting host connectivity issues on the switches. The hosts in VLANs 10 and 15 on Sw11 are unable to communicate with hosts in the same VLANs on Sw12. Hosts in the Admin VLAN are able to communicate. The port-to-VLAN assignments are identical on the two switches. What could be the problem?

A. The Fa0/1 port is not operational on one of the switches.
B. The Link connecting the switches has not been configured as a trunk.
C. At lease one port needs to be configured in VLAN 1 for VLANs 10 and 15 to be able to communicate.
D. Port FastEthernet 0/1 needs to be configured as an access link on both switches.
E. A router is required for hosts on Sw11 in VLANs 10 and 15 to communicate with hosts in the same VLAN on Sw12.

Answer: B

Explanation

The show vlan command only displays access ports, the trunk ports are not shown in this command (we can use the “show interface trunk” command to see trunked ports). In the output we can see the ports Fa0/1 connecting between two switches in VLAN 20 -> they are access ports and only VLAN 20 can communicate. To make all VLANs can communicate (with the same VLAN at the other switch), the link between two switches must be set as trunk -> B is correct.

Question 2

In a switched environment, what does the IEEE 802.1Q standard describe?

A. the operation of VTP
B. a method of VLAN trunking
C. an approach to wireless LAN communication
D. the process for root bridge selection
E. VLAN pruning

Answer: B

Question 3

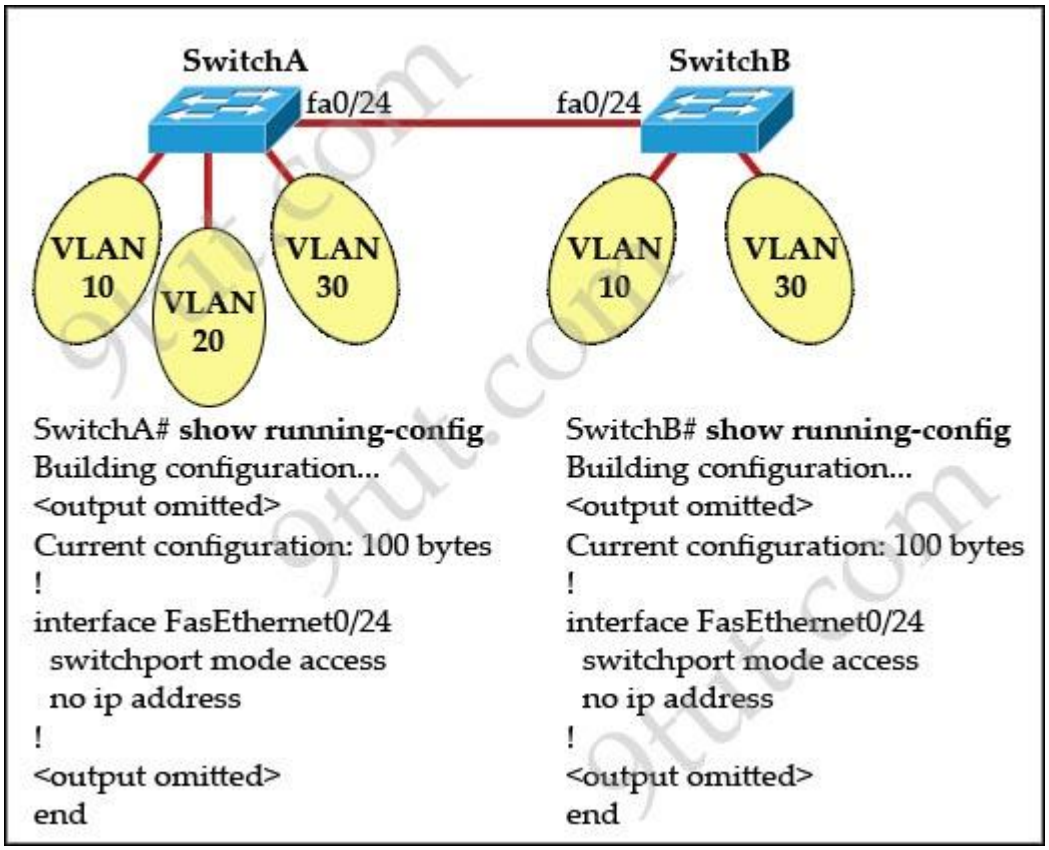
As a network technician, do you know which are valid modes for a switch port used as a VLAN trunk? (Choose three)

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

Answer: B C D

Question 4

Refer to the exhibit:



All switch ports are assigned to the correct VLANs, but none of the hosts connected to SwitchA can communicate with hosts in the same VLAN connected to SwitchB. Based on the output shown, what is the most likely problem?

A. The access link needs to be configured in multiple VLANs.
B. The link between the switches is configured in the wrong VLAN
C. The link between the switches needs to be configured as a trunk.
D. VTP is not configured to carry VLAN information between the switches.
E. Switch IP addresses must be configured in order for traffic to be forwarded between the switches.

Answer: C

Question 5

Which IEEE standard protocol is initiated as a result of successful DTP completion in a switch over FastEthernet?

A. 802.3ad
B. 802.1w
C. 802.1Q
D. 802.1d

Answer: C

Explanation

Dynamic Trunking Protocol (DTP) is a Cisco proprietary protocol for negotiating trunking on a link between two devices and for negotiating the type of trunking encapsulation (802.1Q) to be used.

Question 6

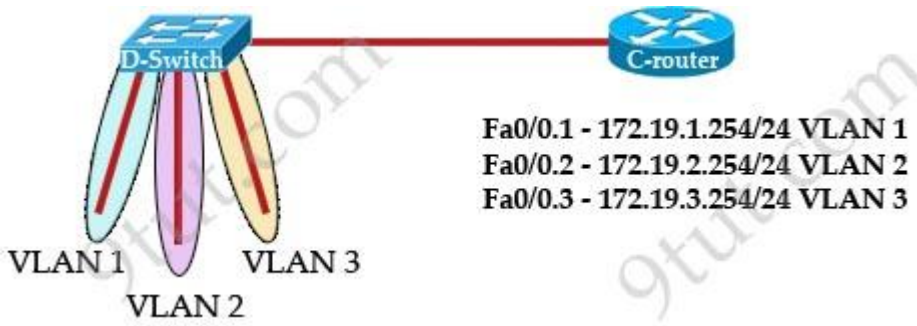
Which three of these statements regarding 802.1Q trunking are correct? (Choose three)

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

Answer: A C E

Question 7

Refer to the exhibit:



C-router is to be used as a "router-on-a-stick" to route between the VLANs. All the interfaces have been properly configured and IP routing is operational. The hosts in the VLANs have been configured with the appropriate default gateway. What can be said about this configuration?

A. These commands need to be added to the configuration:
C-router(config)# router eigrp 123
C-router(config-router)# network 172.19.0.0

B. No further routing configuration is required.

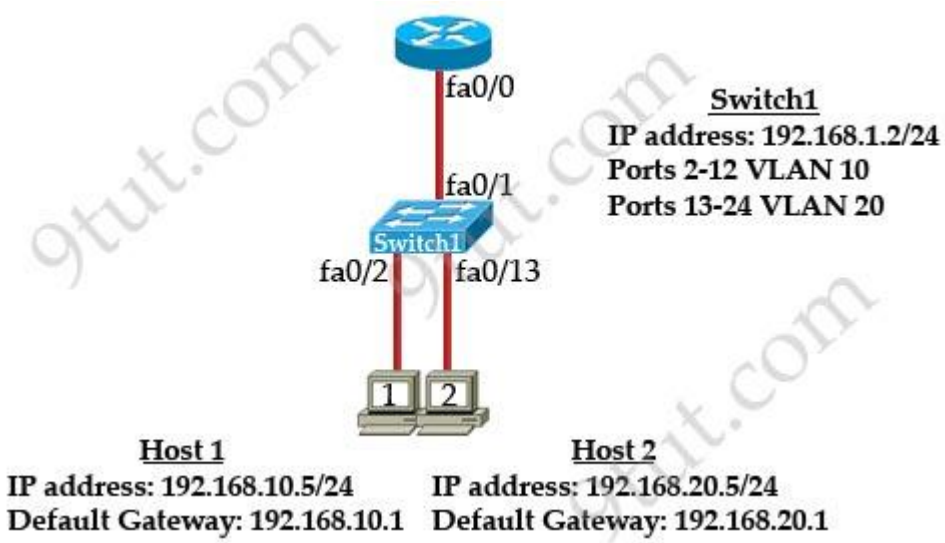
C. These commands need to be added to the configuration:
C-router(config)# router ospf 1
C-router(config-router)# network 172.19.0.0 0.0.3.255 area 0

D. These commands need to be added to the configuration:
C-router(config)# router rip
C-router(config-router)# network 172.19.0.0

Answer: B

Question 8

Refer to the exhibit:



What commands must be configured on the 2950 switch and the router to allow communication between host 1 and host 2? (Choose two)

A. Router(config)#interface fastethernet 0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shut down

B. Router(config)#interface fastethernet 0/0
Router(config-if)#no shutdown
Router(config)#interface fastethernet 0/0.1
Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#interface fastethernet 0/0.2
Router(config-subif)#encapsulation dot1q 20
Router(config-subif)#ip address 192.168.20.1 255.255.255.0

C. Router (config)#router eigrp 100
Router(config-router)#network 192.168.10.0
Router(config-router)#network 192.168.20.0

D. Switch1(config)# vlan database
Switch1(config-vlan)# vtp domain XYZ
Switch1(config-vlan)# vtp server

E. Switch1(config) # interface fastEthernet 0/1
Switch1(config-if)# switchport mode trunk

F. Switch1(config)# interface vlan 1
Switch1(config-if)# ip default-gateway 192.168.1.1

Answer: B E

Question 9

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

A. It is a layer 2 messaging protocol which maintains vlan configurations across network.
B. It includes an 8-bit field which specifies the priority of a frame.
C. It is used exclusively for tagging vlan frames and does not address network reconvergence following switched network topology changes.
D. It modifies the 802.3 frame header and thus requires that the FCS be recomputed.
E. It is a trunking protocol capable of earring untagged frames.

Answer: D E

Explanation

IEEE 802.1Q is the networking standard that supports Virtual LANs (VLANs) on an Ethernet network. It is a protocol that allows VLANs to communicate with one another using a router. 802.1Q trunks support tagged and untagged frames.

If a switch receives untagged frames on a trunk port, it believes that frame is a part of the native VLAN. Also, frames from a native VLAN are not tagged when exiting the switch via a trunk port.

The 802.1q frame format is same as 802.3. The only change is the addition of 4 bytes fields. That additional header includes a field with which to identify the VLAN number. Because inserting this header changes the frame, 802.1Q encapsulation forces a recalculation of the original FCS field in the Ethernet trailer.

Note: Frame Check Sequence (FCS) is a four-octet field used to verify that the frame was received without loss or error. FCS is based on the contents of the entire frame.

Question 10

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

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

Answer: B C D

CCNA – Trunking Questions 2

Question 1

What is the function of the command **switchport trunk native vlan 999** on a trunk port?

A. It designates VLAN 999 for untagged traffic.
B. It blocks VLAN 999 traffic from passing on the trunk.
C. It creates a VLAN 999 interface.
D. It designates VLAN 999 as the default for all unknown tagged traffic.

Answer: A

Question 2

Which three elements must be used when you configure a router interface for vlan trunking? (Choose three)

A. one IP network or subnetwork for each subinterface
B. subinterface numbering that matches vlan tages
C. subinterface encapsulation identifiers that match vlan tags
D. a management domain for each subinterface G E. one physical interface for each subinterface
F. one subinterface per vlan

Answer: A C F

Question 3

Which two link protocols are used to carry multiple VLANs over a single link? (Choose two)

A. VTP
B. 802.1q
C. IGP

D. ISL
E. 802.3u

Answer: B D

Explanation

Cisco switches support two trunking protocols 802.1q & ISL. 802.1q is an open standard and is thus compatible between most vendors' equipment while Inter-Switch Link (ISL) is Cisco proprietary.

Question 4

Which two commands can be used to verify a trunk link configuration status on a Cisco switch? (choose two)

A. show interfaces trunk
B. show interfaces switchport
C. show ip interface brief
D. show interfaces vlan

Answer: A B

Explanation

The "show interfaces trunk" command and "show interfaces switchport" command can be used to verify the status of an interface (trunking or not). The outputs of these commands are shown below (port Ethernet 1/0 has been configured as trunk):

```
S10#show interfaces switchport
Name: Et1/0
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Operational Dot1q Ethertype:  0x8100
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Operational Native VLAN tagging: disabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

The “show ip interface brief” command only gives us information about the IP address, the status (up/down) of an interface:

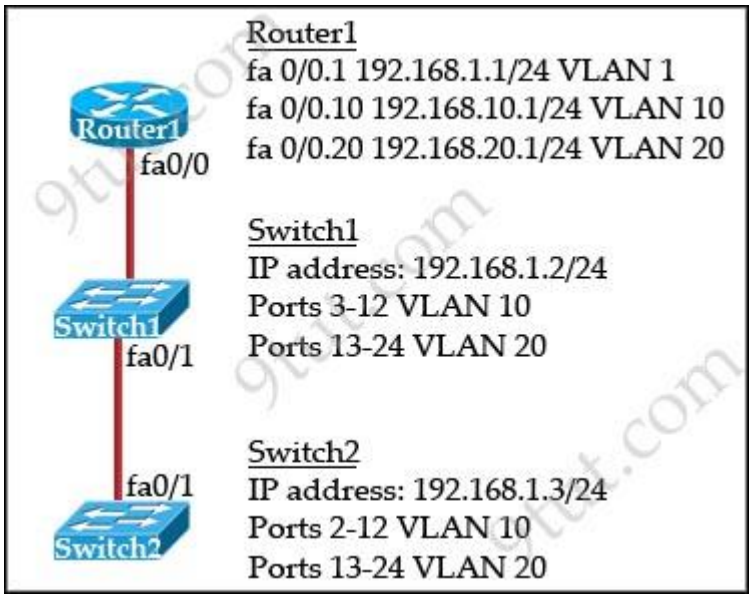
```
S10#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            unassigned      YES NVRAM  administratively down down
Ethernet0/1            unassigned      YES NVRAM  administratively down down
Ethernet0/2            unassigned      YES NVRAM  administratively down down
Ethernet0/3            unassigned      YES NVRAM  administratively down down
Ethernet1/0            unassigned      YES unset  up                    up
Ethernet1/1            unassigned      YES NVRAM  administratively down down
Ethernet1/2            unassigned      YES NVRAM  administratively down down
Ethernet1/3            unassigned      YES NVRAM  administratively down down
Vlan1                  unassigned      YES NVRAM  administratively down down
```

The “show interfaces vlan” command only gives us information about that VLAN, not about which ports are the trunk links:

```
S10#show interfaces vlan 1
Vlan1 is administratively down, line protocol is down
  Hardware is EtherSVI, address is aabb.cc80.0a00 (bia aabb.cc80.0a00)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 1 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Question 5

Refer to the exhibit:



How should the FastEthernet0/1 port on the 2950 model switches that are shown in the exhibit be configured to allow connectivity between all devices?

A. The ports only need to be connected by a crossover cable.

B. SwitchX (config)#interface FastEthernet 0/1
SwitchX(config-if)#switchport mode trunk

C. SwitchX (config)#interface FastEthernet 0/1
SwitchX(config-if)#switchport mode access
SwitchX(config-if)#switchport access vlan 1

D. SwitchX (config)#interface FastEthernet 0/1
SwitchX(config-if)#switchport mode trunk
SwitchX(config-if)#switchport trunk vlan 1
SwitchX(config-if)#switchport trunk vlan 10
SwitchX(config-if)#switchport trunk vlan 20

Answer: B

CCNA – EtherChannel

Notes:

The Port Aggregation Protocol (PAgP) and Link Aggregation Control Protocol (LACP) facilitate the automatic creation of EtherChannels by exchanging packets between Ethernet interfaces. The Port Aggregation Protocol (PAgP) is a Cisco-proprietary solution, and the Link Aggregation Control Protocol (LACP) is standards based.

LACP modes:

+ on: the link aggregation is forced to be formed without any LACP negotiation. A port-channel is formed only if the peer port is also in “on” mode.
+ off: disable LACP and prevent ports to form a port-channel
+ passive: the switch does not initiate the channel, but does understand incoming LACP packets
+ active: send LACP packets and willing to form a port-channel

The table below lists if an EtherChannel will be formed or not for LACP:

LACP	Active	Passive
Active	Yes	Yes
Passive	Yes	No

PAgP modes:

+ on: The link aggregation is forced to be formed without any PAgP negotiation. A port-channel is formed only if the peer port is also in “on” mode.
+ off: disable PAgP and prevent ports to form a port-channel
+ desirable: send PAgP packets and willing to form a port-channel
+ auto: does not start PAgP packet negotiation but responds to PAgP packets it receives

The table below lists if an EtherChannel will be formed or not for PAgP:

PAgP	Desirable	Auto
Desirable	Yes	Yes
Auto	Yes	No

An EtherChannel in Cisco can be defined as a Layer 2 EtherChannel or a Layer 3 EtherChannel.
+ For Layer 2 EtherChannel, physical ports are placed into an EtherChannel group. A logical port-channel interface will be created automatically. An example of configuring Layer 2 EtherChannel can be found in **Question 1** in this article.

+ For Layer 3 EtherChannel, a Layer 3 Switch Virtual Interface (SVI) is created and then the physical ports are bound into this Layer 3 SVI.

For more information about EtherChannel, please read our EtherChannel tutorial.

Question 1

Refer to the exhibit.

SW1

```
interface FastEthernet 0/1
 channel-group 1 mode auto
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface FastEthernet 0/2
 channel-group 1 mode auto
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

A network administrator is configuring an EtherChannel between SW1 and SW2. The SW1 configuration is shown. What is the correct configuration for SW2?

A. interface FastEthernet 0/1
channel-group 1 mode active
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet 0/2
channel-group 1 mode active
switchport trunk encapsulation dot1q
switchport mode trunk

B. interface FastEthernet 0/1
channel-group 2 mode auto
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet 0/2
channel-group 2 mode auto
switchport trunk encapsulation dot1q
switchport mode trunk

C. interface FastEthernet 0/1
channel-group 1 mode desirable
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet 0/2
channel-group 1 mode desirable
switchport trunk encapsulation dot1q
switchport mode trunk

D. interface FastEthernet 0/1
channel-group 1 mode passive
switchport trunk encapsulation dot1q

switchport mode trunk
!
interface FastEthernet 0/2
channel-group 1 mode passive
switchport trunk encapsulation dot1q
switchport mode trunk

Answer: C

Explanation

From the configuration of SW1, we see it is using Port Aggregation Protocol (PAgP) with “auto” mode so the other end (SW2) must also runs PAgP with “desirable” mode to actively sending request to form an Etherchannel.

Question 2

Refer to the exhibit.


```
SW1#show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I  - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------
1      Po1(SU)       LACP        Fa0/2(P)    Fa0/1(D)

SW1#show interface fa0/1
FastEthernet0/1 is down, line protocol is down (disabled)
  Hardware is AmdP2, address is aabb.cc00.0510
       (bia aabb.cc00.0510)
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 10Mb/s
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:04, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes);
       Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
```

```
SW2#show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I  - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------
1      Po1(SU)       LACP        Fa0/2(P)    Fa0/1(D)

SW2#show interface fa0/1
FastEthernet0/1 is down, line protocol is down (disabled)
  Hardware is AmdP2, address is aabb.cc00.0510
       (bia aabb.cc00.0510)
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 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 00:00:04, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes);
       Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
```

If the devices produced the given output, what is the cause of the EtherChannel problem?

A. SW1's Fa0/1 interface is administratively shut down.
B. There is an encapsulation mismatch between SW1's Fa0/1 and SW2's Fa0/1 interfaces.
C. There is an MTU mismatch between SW1's Fa0/1 and SW2's Fa0/1 interfaces.
D. There is a speed mismatch between SW1's Fa0/1 and SW2's Fa0/1 interfaces.

Answer: D

Explanation

All interfaces in an EtherChannel must be configured identically to form an EtherChannel. Specific settings that must be identical include:

+ **Speed settings**
+ Duplex settings
+ STP settings
+ VLAN membership (for access ports)
+ Native VLAN (for trunk ports)
+ Allowed VLANs (for trunk ports)
+ Trunking Encapsulation (ISL or 802.1Q, for trunk ports)

In the output of the "show interface fa0/1″ commands we see the speed of interface Fa0/1 of SW1 is "100Mb/s" while that of SW2 is "10Mb/s" so the speed is mismatched here -> an Etherchannel will not be formed.

Question 3

A network administrator creates a layer 3 EtherChannel, bundling four interfaces into channel group 1. On what interface is the IP address configured?

A. the port-channel 1 interface
B. the highest number member interface
C. all member interfaces
D. the lowest number member interface

Answer: A

Explanation

When an EtherChannel is created, a logical interface will be created on the switches or routers representing for that EtherChannel. You can configure this logical interface in the way you want. For example, assign access/trunk mode on switches or assign IP address for the logical interface on routers… An example of a Layer 3 Etherchannel port is shown below:

```
interface PortChannel12
description Link to R2
ip address 10.2.4.13 255.255.255.252
```

Question 4

What parameter can be different on ports within an EtherChannel?

A. speed
B. DTP negotiation settings
C. trunk encapsulation
D. duplex

Answer: B

Explanation

All interfaces in an EtherChannel must be configured identically to form an EtherChannel. Specific settings that must be identical include:
+ Speed settings
+ Duplex settings
+ STP settings
+ VLAN membership (for access ports)
+ Native VLAN (for trunk ports)
+ Allowed VLANs (for trunk ports)
+ Trunking Encapsulation (ISL or 802.1Q, for trunk ports)

-> DTP negotiation settings can be different on ports within an EtherChannel.

Question 5

Refer to the exhibit.

```
FastEthernet0/3:
Port state        = 1
Channel group     = 2      Mode = Passive      Gcchange = -
Port-channel      = Po2    GC   = -            Pseudo port-channel = Po2
Port index        = 0      Load = 0x00         Protocol  = LACP
```

What set of commands was configured on interface Fa0/3 to produce the given output?

A. interface FastEthernet 0/3
channel-group 1 mode desirable
switchport trunk encapsulation dot1q
switchport mode trunk

B. interface FastEthernet 0/3
channel-group 2 mode passive
switchport trunk encapsulation dot1q
switchport mode trunk

C. interface FastEthernet 0/3
channel-group 2 mode active
switchport trunk encapsulation dot1q
switchport mode trunk

D. interface FastEthernet 0/3
channel-group 2 mode on
switchport trunk encapsulation dot1q
switchport mode trunk

Answer: B

Explanation

From the output we see these lines:

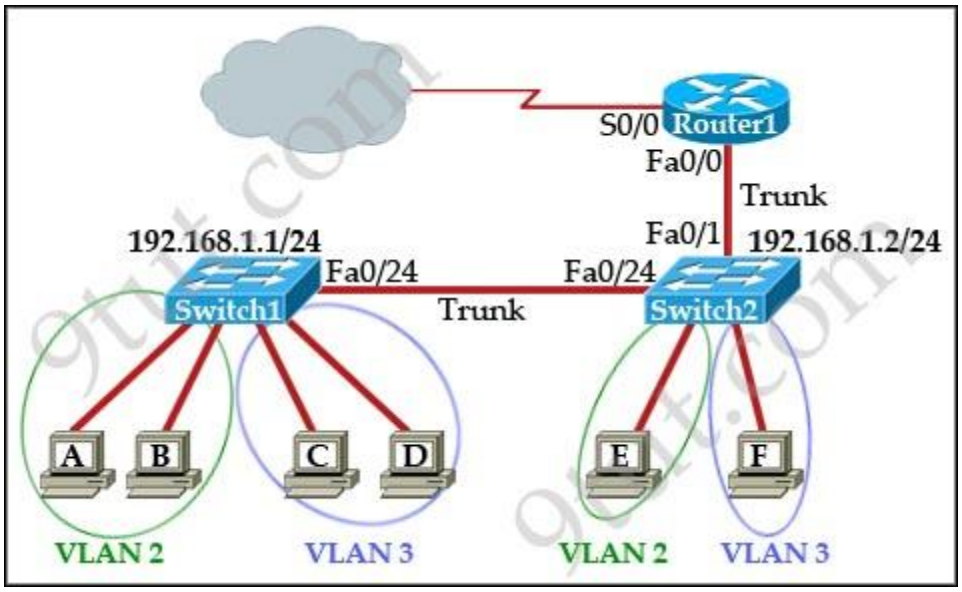
+ Port-channel = Po2 -> must use the command “channel-group 2 …”
+ Mode = Passive -> must set the mode to passive.
+ Protocol = LACP -> In fact, from the “passive” mode we have already learned it is running LACP.

Therefore the correct command should be “channel-group 2 mode passive”.

CCNA – InterVLAN Questions

Question 1

Refer to the exhibit:



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

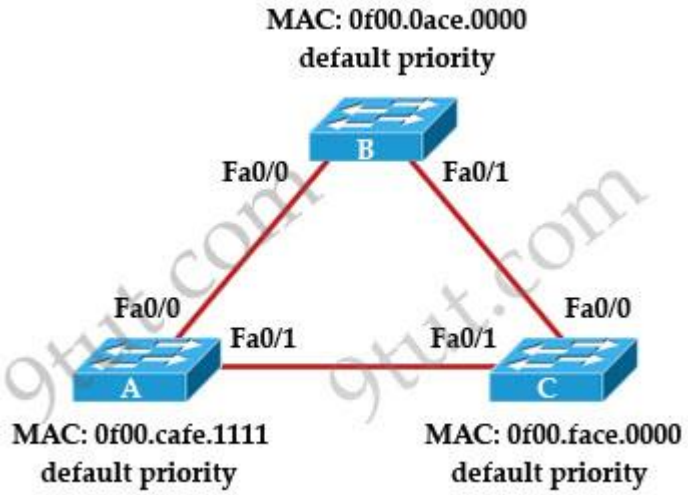
A. Host E and host F use the same IP gateway address.
B. Routed and Switch2 should be connected via a crossover cable.
C. Router1 will not play a role in communications between host A and host D.
D. The FastEthernet 0/0 interface on Router1 must be configured with subinterfaces.
E. Router1 needs more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

Answer: D F

CCNA – STP

Question 1

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

First by comparing their MAC addresses we learn that switch B will be root bridge as it has lowest MAC. Therefore all of its ports are designated ports -> C & D are correct.

On the link between switch A & switch C there must have one designated port and one non-designated (blocked) port. We can figure out which port is designated port by comparing their MAC address again. A has lower MAC so Fa0/1 of switch A will be designated port while Fa0/1 of switch C will be blocked -> B is correct.

Question 2

What value is primarily used to determine which port becomes the root port on each non-root switch in a spanning-tree topology?

A. lowest port MAC address
B. port priority number and MAC address.
C. VTP revision number
D. highest port priority number.
E. path cost

Answer: E

Explanation

The path cost to the root bridge is the most important value to determine which port will become the root port on each non-root switch. In particular, the port with lowest cost to the root bridge will become root port (on non-root switch).

Question 3

What is one benefit of PVST+?

A. PVST+ reduces the CPU cycles for all the switches in the network.
B. PVST+ automatically selects the root bridge location, to provide optimization.
C. PVST+ allows the root switch location to be optimized per vlan.
D. PVST+ supports Layer 3 load balancing without loops.

Answer: C

Explanation

Per VLAN Spanning Tree (PVST) maintains a spanning tree instance for each VLAN configured in the network. It means a switch can be the root bridge of a VLAN while another switch can be the root bridge of other VLANs in a common topology. For example, Switch 1 can be the root bridge for Voice data while Switch 2 can be the root bridge for Video data. If designed correctly, it can optimize the network traffic.

Question 4

Which two protocols are used by bridges and/or switches to prevent loops in a layer 2 network? (Choose two)

A. 802.1d
B. VTP
C. 802.1q
D. STP
E. SAP

Answer: A D

Question 5

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

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

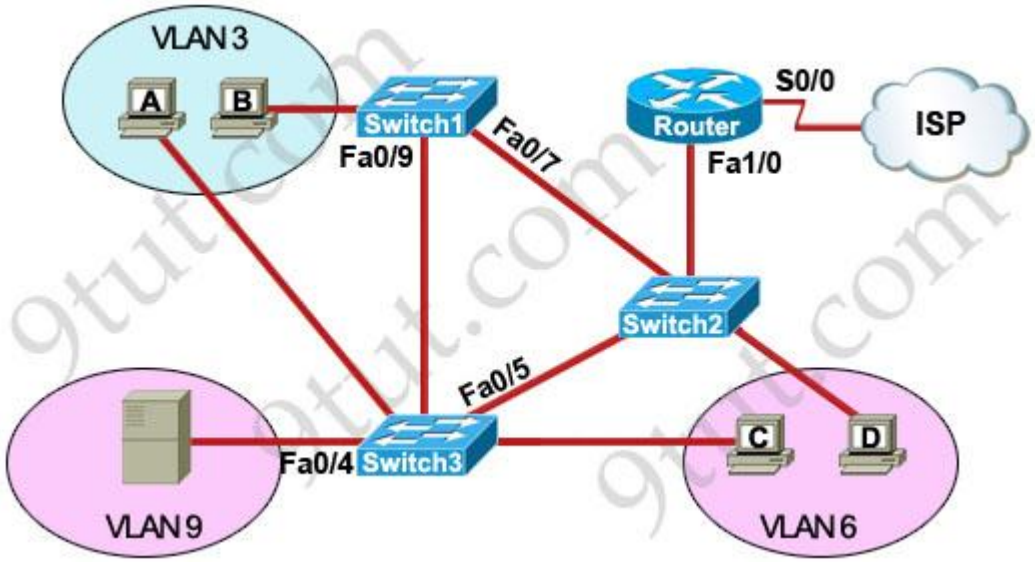
Answer: B

Explanation

If we connect two switches via 2 or more links and do not enable STP on these switches then a loop (which creates multiple copies of the same unicast frame) will occur. It is an example of an improperly implemented redundant topology.

Question 6

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

Question 7

Which port state is introduced by Rapid-PVST?

A. learning
B. listening
C. discarding
D. forwarding

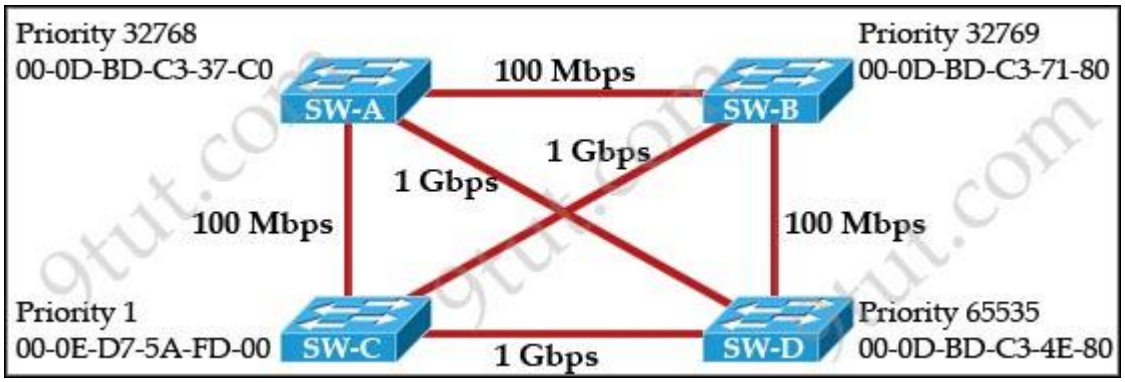
Answer: C

Explanation

PVST+ is based on IEEE802.1D Spanning Tree Protocol (STP). But PVST+ has only 3 port states (discarding, learning and forwarding) while STP has 5 port states (blocking, listening, learning, forwarding and disabled). So discarding is a new port state in PVST+.

Question 8

Refer to the exhibit. Based on the information given, which switch will be elected root bridge and why?



A. Switch A, because it has the lowest MAC address
B. Switch A, because it is the most centrally located switch
C. Switch B, because it has the highest MAC address
D. Switch C, because it is the most centrally located switch
E. Switch C, because it has the lowest priority
F. Switch D, because it has the highest priority

Answer: E

Question 9

Which term describes a spanning-tree network that has all switch ports in either the blocking or forwarding state?

A. redundant
B. spanned
C. provisioned
D. converged

Answer: D

Explanation

Spanning Tree Protocol convergence (Layer 2 convergence) happens when bridges and switches have transitioned to either the forwarding or blocking state. When layer 2 is converged, root bridge is elected and all port roles (Root, Designated and Non-Designated) in all switches are selected.

Question 10

Refer to the exhibit. Given the output shown from this Cisco Catalyst 2950, what is the most likely reason that interface FastEthernet 0/10 is not the root port for VLAN 2?

Switch# show spanning-tree interface fastethernet0/10

Vlan	Role	Sts	Cost	Prio.Nbr	Type
VLAN0001	Root	FWD	19	128.1	P2p
VLAN0002	Altn	BLK	19	128.2	P2p
VLAN0003	Root	FWD	19	128.2	P2p

A. This switch has more than one interface connected to the root network segment in VLAN 2.
B. This switch is running RSTP while the elected designated switch is running 802.1d Spanning Tree.
C. This switch interface has a higher path cost to the root bridge than another in the topology.
D. This switch has a lower bridge ID for VLAN 2 than the elected designated switch.

Answer: C

CCNA – STP 2

Question 1

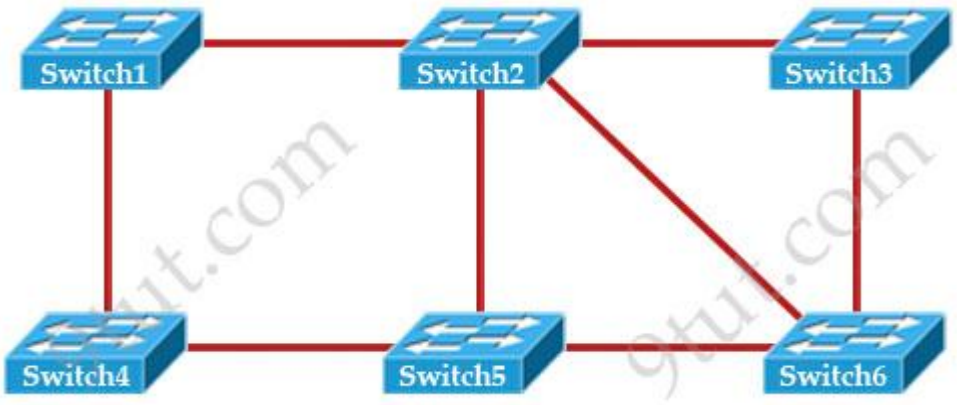
Three switches are connected to one another via trunk ports. Assuming the default switch configuration, which switch is elected as the root bridge for the spanning-tree instance of VLAN 1?

A. the switch with the highest MAC address
B. the switch with the lowest MAC address
C. the switch with the highest IP address
D. the switch with the lowest IP address

Answer: B

Question 2

Based on the network shown in the graphic



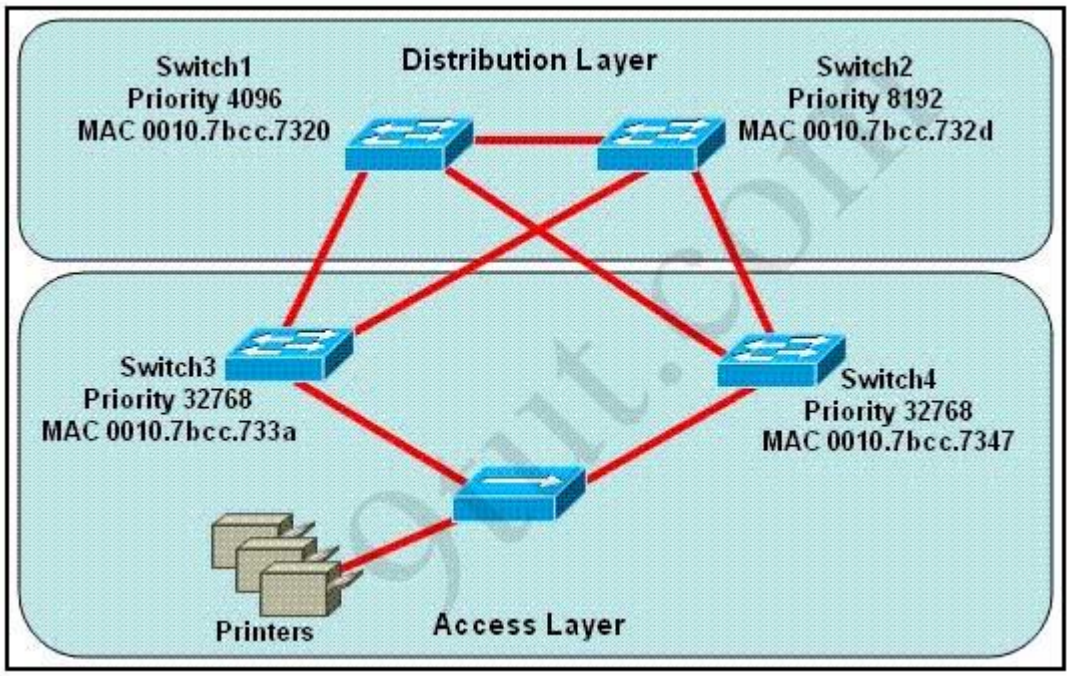
Which option contains both the potential networking problem and the protocol or setting that should be used to prevent the problem?

A. routing loops, hold down timers
B. Switching loops, split horizon
C. routing loops, split horizon
D. Switching loops, VTP
E. routing loops, STP
F. Switching loops, STP

Answer: F

Question 3

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



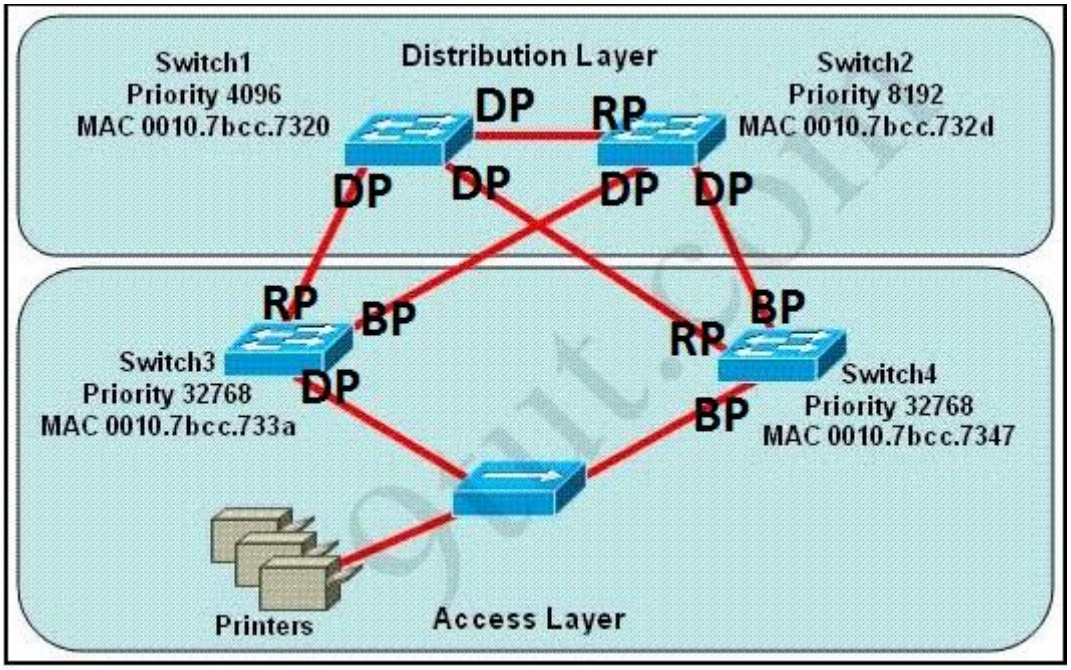
A. Switch1
B. Switch2
C. Switch3
D. Switch4

Answer: C

Explanation

First, the question asks what switch services the printers, so it can be Switch 3 or Switch 4 which is connected directly to the Printers.

Next, by comparing the MAC address of Switch 3 and Switch 4 we found that the MAC of Switch 3 is smaller. Therefore the interface connected to the Printers of Switch 3 will become designated interface and the interface of Switch 4 will be blocked. The picture below shows the roles of all ports:



DP: Designated Port
RP: Root Port
BP: Blocked Port

(Please notice that Switch 1 will become the root bridge because of its lowest priority, not Switch 3)

CCNA – RSTP

Note: If you are not sure about Rapid Spanning Tree Protocol, please read our Rapid Spanning Tree Protocol RSTP Tutorial.

Question 1

Which three statements about RSTP are true? (Choose three)

A. RSTP significantly reduces topology reconvening time after a link failure.
B. RSTP expands the STP port roles by adding the alternate and backup roles.
C. RSTP port states are blocking, discarding, learning, or forwarding.
D. RSTP provides a faster transition to the forwarding state on point-to-point links than STP does.
E. RSTP also uses the STP proposal-agreement sequence.
F. RSTP uses the same timer-based process as STP on point-to-point links.

Answer: A B D

Question 2

Refer to the exhibit:

```
Switch# show spanning-tree vlan 1
VLAN0001
     Spanning tree enabled pcotocol rstp
     Root ID   Priority   20481
               Address    0008.217a.5800
               Cost       38
               Port       1 (FastEthernet0/1)
               Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID      Priority   32769 (priority 32768 sys-id-ext 1)
               Address    0008.205e.6600
               Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
               Aging Time 300

Interface      Role  Sts   Cost      Prio.Nbr  Type
---------------- ------ ---- ---------- ---------- --------------------
Fa0/1          Root  FWD   19        128.1     P2p
Fa0/4          Desg FDD    38        128.1     P2p
Fa0/11         Altn  BLK   57        128.1     P2p
Fa0/13         Desg FWD    38        128.1     P2p
```

Why has this switch not been elected the root bridge for VLAN1?

A. It has more than one internee that is connected to the root network segment.
B. It is running RSTP while the elected root bridge is running 802.1d spanning tree.
C. It has a higher MAC address than the elected root bridge.
D. It has a higher bridge ID than the elected root bridge.

Answer: D

Explanation

As we can see from the output above, the priority of the root bridge is 20481 while that of the local bridge is 32769.

Question 3

Which command enables RSTP on a switch?

A. spanning-tree mode rapid-pvst
B. spanning-tree uplinkfast
C. spanning-tree backbonefast
D. spanning-tree mode mst

Answer: A

Question 4

Refer to the exhibit. Which statement is true?

```
SwitchA# show spanning-tree vlan 20

VLAN0020
  Spanning tree enabled protocol rstp
  Root ID     Priority    24596
              Address     0017.596d.2a00
              Cost        38
              Port        11(FastEthernet0/10)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    28692  (priority 28672 sys-id-ext 1)
              Address     0017.596d.1580
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/11           Root FWD 19        128.11   P2p
Fa0/12           Altn BLK 19        128.12   P2p
```

A. The Fa0/11 role confirms that SwitchA is the root bridge for VLAN 20.
B. VLAN 20 is running the Per VLAN Spanning Tree Protocol.
C. The MAC address of the root bridge is 0017.596d.1580.
D. SwitchA is not the root bridge, because not all of the interface roles are designated.

Answer: D

Explanation

Only non-root bridge can have root port. Fa0/11 is the root port so we can confirm this switch is not the root bridge -> A is not correct.

From the output we learn this switch is running Rapid STP, not PVST -> B is not correct.

0017.596d.1580 is the MAC address of this switch, not of the root bridge. The MAC address of the root bridge is 0017.596d.2a00 -> C is not correct.

All of the interface roles of the root bridge are designated. SwitchA has one Root port and 1 Alternative port so it is not the root bridge -> D is correct.

Question 5

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

```
Switch# show spanning-tree vlan 30
VLAN0030
Spanning tree enabled protocol rstp
Root ID Priority 24606
Address 00d0.047b.2800
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 24606 (priority 24576 sys-id-ext 30)
Address 00d0.047b.2800
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300
Interface   Role  Sts   Cost  Prio.Nbr    Type
---------   ----------  ---   -------     ----- ----------
Fa1/1       Desg FWD    4     128.1       p2p
Fa1/2       Desg FWD    4     128.2       p2p
Fa5/1       Desg FWD    4     128.257     p2p
```

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

Answer: A C E

Explanation

From the output, we see that all ports are in Designated role (forwarding state) -> A and E are correct.

The command "show spanning-tree vlan 30″ only shows us information about VLAN 30. We don't know how many VLAN exists in this switch -> B is not correct.

The bridge priority of this switch is 24606 which is lower than the default value bridge priority 32768 -> C is correct.

All three interfaces on this switch have the connection type "p2p", which means Point-to-point environment – not a shared media -> D is not correct.

The only thing we can specify is this switch is the root bridge for VLAN 3o but we can not guarantee it is also the root bridge for other VLANs -> F is not correct.

Question 6

Which two states are the port states when RSTP has converged? (choose two)

A. blocking
B. learning
C. disabled
D. forwarding
E. listening

Answer: A D

Explanation

RSTP only has 3 port states that are discarding, learning and forwarding. When RSTP has converged there are only 2 port states left: discarding and forwarding but the answers don't mention about discarding state so blocking state (answer A) may be considered the best alternative answer.

Question 7

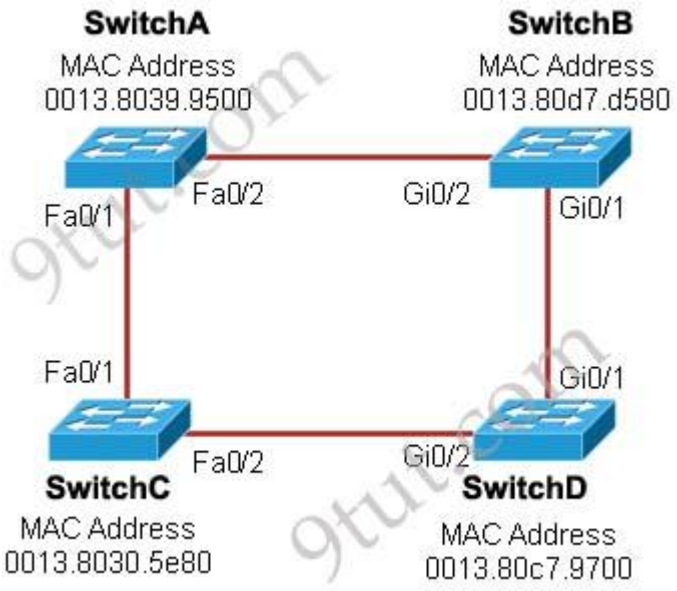
Which two of these statements regarding RSTP are correct? (Choose two)

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

Answer: B E

Question 8

Refer to the exhibit. Each of these four switches has been configured with a hostname, as well as being configured to run RSTP. No other configuration changes have been made. Which three of these show the correct RSTP port roles for the indicated switches and interfaces? (Choose three)



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

Answer: A B F

Explanation

The question says “no other configuration changes have been made” so we can understand these switches have the same bridge priority. Switch C has lowest MAC address so it will become root bridge and 2 of its ports (Fa0/1 & Fa0/2) will be designated ports -> E is incorrect.

Because SwitchC is the root bridge so the 2 ports nearest SwitchC on SwitchA (Fa0/1) and SwitchD (Gi0/2) will be root ports -> B and F are correct.

Now we come to the most difficult part of this question: SwitchB must have a root port so which port will it choose? To answer this question we need to know about STP cost and port cost.

In general, “cost” is calculated based on bandwidth of the link. The higher the bandwidth on a link, the lower the value of its cost. Below are the cost values you should memorize:

Link speed	Cost
10Mbps	100
100Mbps	19

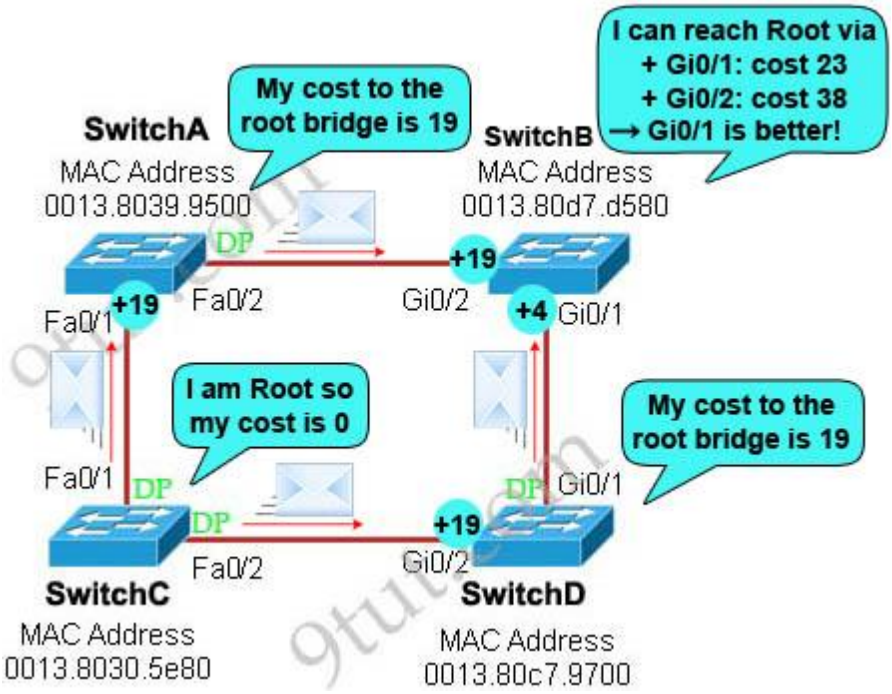
1 Gbps	4

SwitchB will choose the interface with lower cost to the root bridge as the root port so we must calculate the cost on interface Gi0/1 & Gi0/2 of SwitchB to the root bridge. This can be calculated from the "cost to the root bridge" of each switch because **a switch always advertises its cost to the root bridge** in its BPDU. The receiving switch will **add its local port cost value to the cost** in the BPDU.

In the exhibit you also we FastEthernet port is connecting to GigabitEthernet port. In this case GigabitEthernet port will operate as a FastEthernet port so the link can be considered as FastEthernet to FastEthernet connection.

One more thing to notice is that a root bridge always advertises the cost to the root bridge (itself) with an initial value of 0.

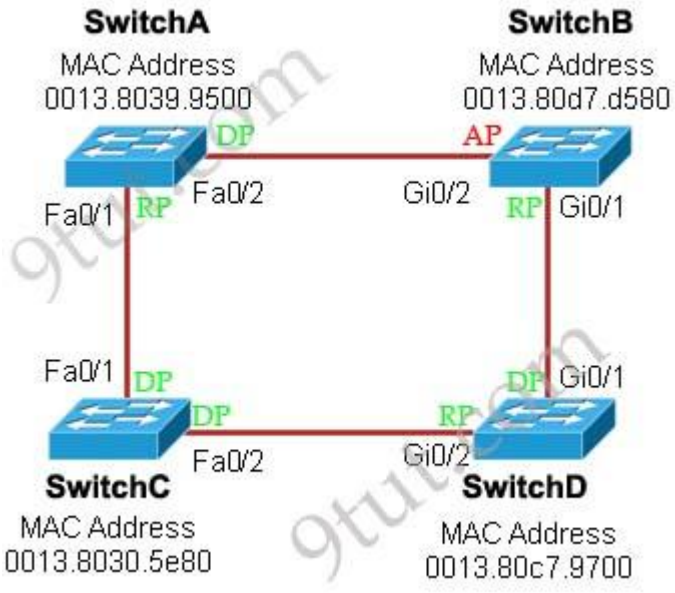
Now let's have a look at the topology again



SwitchC advertises its cost to the root bridge with a value of 0. Switch D adds 19 (the cost value of 100Mbps link although the port on Switch D is GigabitEthernet port) and advertises this value (19) to SwitchB. SwitchB adds 4 (the cost value of 1Gbps link) and learns that it can reach SwitchC via Gi0/1 port with a total cost of 23. The same process happens for SwitchA and SwitchB learns that it can reach SwitchC via Gi0/2 with a total cost of 38 -> Switch B chooses Gi0/1 as its root port -> D is not correct.

Now our last task is to identify the port roles of the ports between SwitchA & SwitchB. It is rather easy as the MAC address of SwitchA is lower than that of SwitchB so Fa0/2 of SwitchA will be designated port while Gi0/2 of SwitchB will be alternative port -> A is correct but C is not correct.

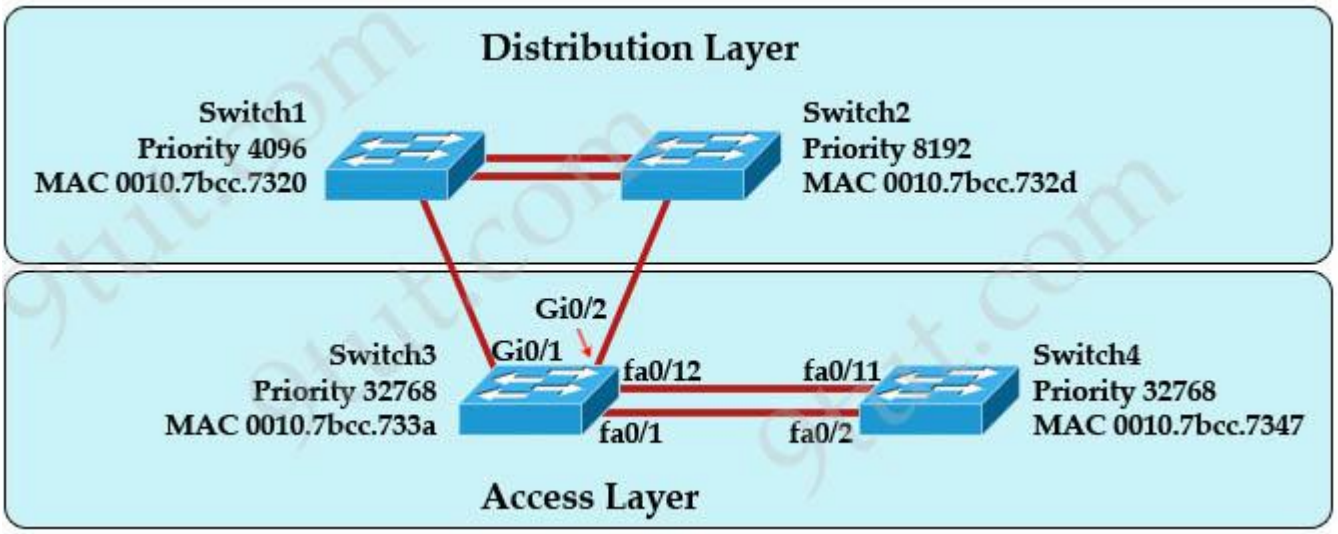
Below summaries all the port roles of these switches:



+ DP: Designated Port (forwarding state)
+ RP: Root Port (forwarding state)
+ AP: Alternative Port (blocking state)

Question 9

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



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

Answer: C

Explanation

In this question, we only care about the Access Layer switches (Switch3 & 4). Switch 3 has a lower bridge ID than Switch 4 (because the MAC of Switch3 is smaller than that of Switch4) so both ports of Switch3 will be in forwarding state. The alternative port will surely belong to Switch4.

Switch4 will need to block one of its ports to avoid a bridging loop between the two switches. But how does Switch4 select its blocked port? Well, the answer is based on the BPDUs it receives from Switch3. A BPDU is superior than another if it has:

1. A lower Root Bridge ID
2. A lower path cost to the Root
3. A lower Sending Bridge ID
4. A lower Sending Port ID

These four parameters are examined in order. In this specific case, all the BPDUs sent by Sswitch3 have the same Root Bridge ID, the same path cost to the Root and the same Sending Bridge ID. The only parameter left to select the best one is the Sending Port ID (Port ID = port priority + port index). In this case the port priorities are equal because they use the default value, so Switch4 will compare port index values, which are unique to each port on the switch, and because Fa0/12 is inferior to Fa0/1, Switch4 will select the port connected with Fa0/1 (of Switch3) as its root port and block the other port -> Port fa0/11 of Switch4 will be blocked (discarding role).

If you are still not sure about this question, please read my RSTP tutorial.

CCNA – Access list Questions

Note: If you are not sure about Access list, please read our Access List Tutorial.

Question 1

Which item represents the standard IP ACL?

A. access-list 50 deny 192.168.1.1 0.0.0.255
B. access-list 110 permit ip any any
C. access-list 2500 deny tcp any host 192.168.1.1 eq 22
D. access-list 101 deny tcp any host 192.168.1.1

Answer: A

Explanation

The standard access lists are ranged from 1 to 99 and from 1300 to 1999 so only access list 50 is a standard access list.

Question 2

A network administrator is configuring ACLs on a Cisco router, to allow traffic from hosts on networks 192.168.146.0, 192.168.147.0, 192.168.148.0, and 192.168.149.0 only. Which two ACL statements, when combined, would you use to accomplish this task? (Choose two)

A. access-list 10 permit ip 192.168.146.0 0.0.1.255
B. access-list 10 permit ip 192.168.147.0 0.0.255.255
C. access-list 10 permit ip 192.168.148.0 0.0.1.255
D. access-list 10 permit ip 192.168.149.0 0.0.255.255
E. access-list 10 permit ip 192.168.146.0 0.0.0.255
F. access-list 10 permit ip 192.168.146.0 255.255.255.0

Answer: A C

Question 3

Refer to the exhibit.

```
ACL 102
access-list 102 deny tcp 172.21.1.1 0.0.0.255 any eq 80
access-list 102 deny ip any any

RouterA#show ip int
FastEthernet0/0 is up, line protocol is up
Internet address is 192.168.1.144/20
Broadcast address is 255.255.255.255
Address determined by DHCP
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is enabled
Outgoing access list is 102
Inbound access list is not set
Proxy ARP is enabled
```

An attempt to deny web access to a subnet blocks all traffic from the subnet. Which interface command immediately removes the effect of ACL 102?

A. no ip access-class 102 in
B. no ip access-class 102 out
C. no ip access-group 102 in
D. no ip access-group 102 out
E. no ip access-list 102 in

Answer: D

Question 4

On which options are standard access lists based?

A. destination address and wildcard mask
B. destination address and subnet mask
C. source address and subnet mask
D. source address and wildcard mask

Answer: D

Question 5

Refer to the exhibit.

ACL 10
Statements are written in this order:
A. permit any
B. deny 172.21.1.128 0.0.0.15
C. permit 172.21.1.129 0.0.0.0
D. permit 172.21.1.142 0.0.0.0

Statements A, B, C, and D of ACL 10 have been entered in the shown order and applied to interface E0 inbound, to prevent all hosts (except those whose addresses are the first and last IP of subnet 172.21.1.128/28) from accessing the network. But as is, the ACL does not restrict anyone from the network. How can the ACL statements be re-arranged so that the system works as intended?

A. ACDB
B. BADC
C. DBAC
D. CDBA

Answer: D

Question 6

Which statement about access lists that are applied to an interface is true?

A. you can apply only one access list on any interface
B. you can configure one access list, per direction, per layer 3 protocol
C. you can place as many access lists as you want on any interface
D. you can configure one access list, per direction, per layer 2 protocol

Answer: B

Explanation

We can have only 1 access list per protocol, per direction and per interface. It means:

+ We can not have 2 inbound access lists on an interface
+ We can have 1 inbound and 1 outbound access list on an interface

Question 7

A network engineer wants to allow a temporary entry for a remote user with a specific username and password so that the user can access the entire network over the internet. Which ACL can be used?

A. reflexive
B. extended
C. standard
D. dynamic

Answer: D

Explanation

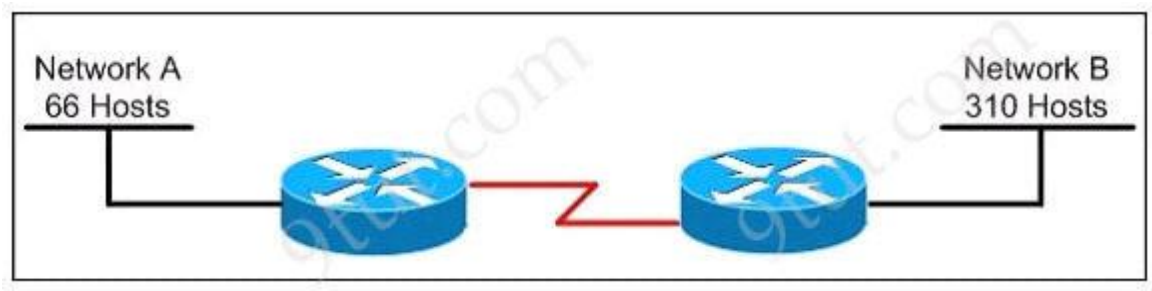
We can use a dynamic access list to authenticate a remote user with a specific username and password. The authentication process is done by the router or a central access server such as a TACACS+ or RADIUS server. The configuration of dynamic ACL can be read here:
http://www.cisco.com/en/US/tech/tk583/tk822/technologies_tech_note09186a0080094524.shtml

CCNA – Subnetting

Note: If you are not sure about Subnetting, please read our Subnetting Tutorial – Subnetting Made Easy.

Question 1

Refer to the exhibit. Which subnet mask will place all hosts on Network B in the same subnet with the least amount of wasted addresses?



A. 255.255.255.0
B. 255.255.254.0
C. 255.255.252.0
D. 255.255.248.0

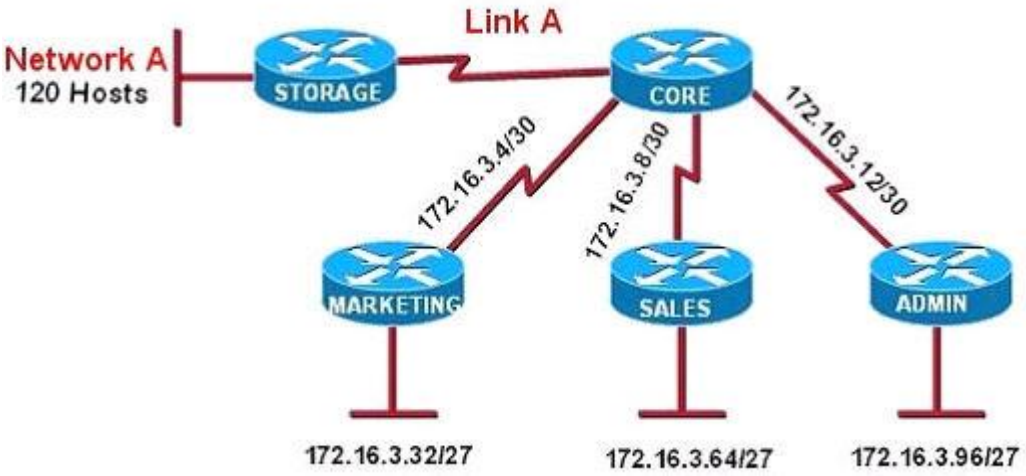
Answer: B

Explanation

310 hosts < 512 = 2^9 -> We need a subnet mask of 9 bits 0 -> 1111 1111.1111 1111.1111 1110.0000 0000 -> 255.255.254.0

Question 2

Refer to the exhibit. All of the routers in the network are configured with the ip subnet-zero command. Which network addresses should be used for Link A and Network A? (Choose two)



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

Answer: B D

Explanation

Network A needs 120 hosts < 128 = 2^7 -> Need a subnet mask of 7 bit 0s -> "/25".

Because the ip subnet-zero command is used, network 172.16.3.0/30 can be used.

Answer E "Link A – 172.16.3.40/30" is not correct because this subnet belongs to MARKETING subnet (172.16.3.32/27).
Answer F "Link A – 172.16.3.112/30" is not correct because this subnet belongs to ADMIN subnet (172.16.3.96/27).

Question 3

You have been asked to come up with a subnet mask that will allow all three web servers to be on the same network while providing the maximum number of subnets. Which network address and subnet mask meet this requirement?

A. 192.168.252.0 255.255.255.252
B. 192.168.252.8 255.255.255.248
C. 192.168.252.8 255.255.255.252
D. 192.168.252.16 255.255.255.240
E. 192.168.252.16 255.255.255.252

Answer: B

Question 4

Which subnet mask would be appropriate for a network address range to be subnetted for up to eight LANs, with each LAN containing 5 to 26 hosts?

A. 0.0.0.240
B. 255.255.255.252
C. 255.255.255.0
D. 255.255.255.224
E. 255.255.255.240

Answer: D

Explanation

A is not correct because it is a wildcard mask (not subnet mask).

This question is a bit unclear but we can suppose we have to begin with default subnet mask and "subnet" it. And the default subnet mask here should be class C: 255.255.255.0

For answer B: 252 = 1111 1100 -> with this subnet mask we can subnet up to 2^6 = 64 subnets but only $2^2 – 2 = 2$ hosts per subnet -> B is not correct.

C is not correct because it is the default subnet mask of class C and that means we don't "subnet" it.

For answer E: 240 = 1111 0000 -> There are 2^4 = 16 subnets but only $2^4 – 2 = 14$ hosts per subnet < 26 hosts -> E does not satisfy the second requirement (of 26 hosts per subnet).

For answer D: 224 = 1110 0000 -> There are 2^3 = 8 subnets and $2^5 – 2 = 30$ hosts > 26 hosts -> This is the correct answer.

Note: The number "5" in " with each LAN containing 5 to 26 hosts" is just used to trick you and it does not have any effect on our answer.

Question 5

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

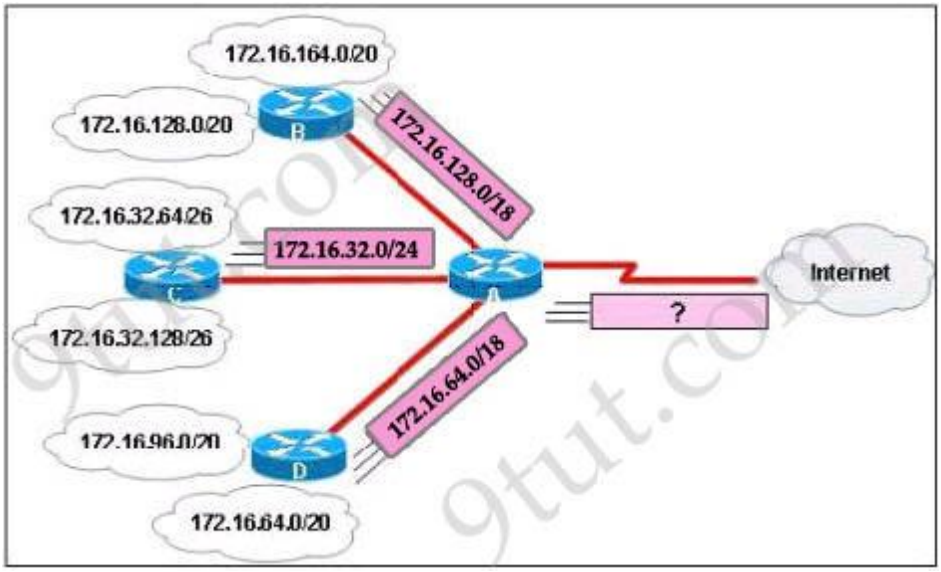
D. IP address: 192.168.20.30
Subnet Mask: 255.255.255.240
Default Gateway: 192.168.20.17

E. IP address: 192.168.20.30
Subnet Mask: 255.255.255.240
Default Gateway: 192.168.20.25

Answer: C

Question 6

Refer to the exhibit. In this VLSM addressing scheme, what summary address would be sent from router A?



A. 172.16.0.0/16
B. 172.16.0.0/20
C. 172.16.0.0/24
D. 172.32.0.0/16
E. 172.32.0.0/17
F. 172.64.0.0/16

Answer: A

Explanation

Router A receives 3 subnets: 172.16.64.0/18, 172.16.32.0/24 and 172.16.128.0/18.

All these 3 subnets have the same form of 172.16.x.x so our summarized subnet must be also in that form -> Only A, B or C is correct.

The smallest subnet mask of these 3 subnets is /18 so our summarized subnet must also have its subnet mask equal or smaller than /18.

-> Only answer A has these 2 conditions -> A is correct.

Question 7

You are working in a data center environment and are assigned the address range 10.188.31.0/23. You are asked to develop an IP addressing plan to allow the maximum number of subnets with as many as 30 hosts each.Which IP address range meets these requirements?

A. 10.188.31.0/27
B. 10.188.31.0/26
C. 10.188.31.0/29
D. 10.188.31.0/28
E. 10.188.31.0/25

Answer: A

Explanation

Each subnet has 30 hosts < 32 = 2^5 so we need a subnet mask which has at least 5 bit 0s -> /27. Also the question requires the maximum number of subnets (which minimum the number of hosts-per-subnet) so /27 is the best choice -> A is correct.

Question 8

Which two benefits are provided by using a hierarchical addressing network addressing scheme? (Choose two)

A. reduces routing table entries
B. auto-negotiation of media rates
C. efficient utilization of MAC addresses
D. dedicated communications between devices
E. ease of management and troubleshooting

Answer: A E

Question 9

The network administrator is asked to configure 113 point-to-point links. Which IP addressing scheme best defines the address range and subnet mask that meet the requirement and waste the fewest subnet and host addresses?

A. 10.10.0.0/18 subnetted with mask 255.255.255.252
B. 10.10.0.0/25 subnetted with mask 255.255.255.252
C. 10.10.0.0/24 subnetted with mask 255.255.255.252
D. 10.10.0.0/23 subnetted with mask 255.255.255.252
E. 10.10.0.0/16 subnetted with mask 255.255.255.252

Answer: D

Explanation

We need 113 point-to-point links which equal to 113 sub-networks < 128 so we need to borrow 7 bits (because 2^7 = 128).

The network used for point-to-point connection should be /30.
So our initial network should be 30 – 7 = 23.

So 10.10.0.0/23 is the correct answer.

You can understand it more clearly when writing it in binary form:

/23 = 1111 1111.1111 1110.0000 0000
/30 = 1111 1111.1111 1111.1111 1100 (borrow 7 bits)

Question 10

Given an IP address 172.16.28.252 with a subnet mask of 255.255.240.0, what is the correct network address?

A. 172.16.16.0
B. 172.16.24.0
C. 172.16.0.0
D. 172.16.28.0

Answer: A

Explanation

Increment: 16 (of the third octet)
Network address: 172.16.16.0

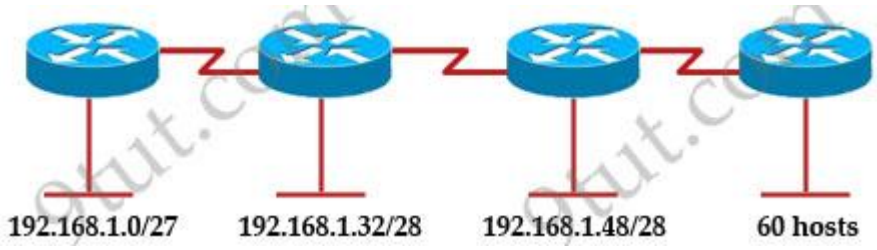
-> A is correct.

CCNA – Subnetting 2

Note: If you are not sure about Subnetting, please read our Subnetting Tutorial – Subnetting Made Easy.

Question 1

Refer to the exhibit. A new subnet with 60 hosts has been added to the network. Which subnet address should this network use to provide enough usable addresses while wasting the fewest addresses?



A. 192.168.1.56/27
B. 192.168.1.64/26
C. 192.168.1.64/27
D. 192.168.1.56/26

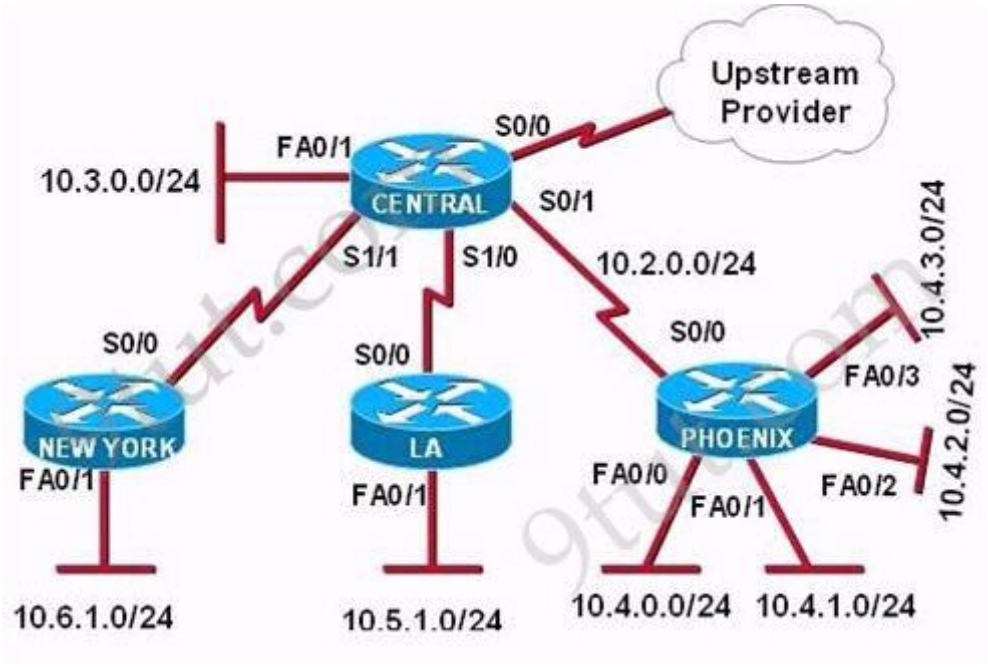
Answer: B

Explanation

60 hosts < 64 = 2^6 -> we need a subnet mask of at least 6 bit 0s -> "/26". The question requires "wasting the fewest addresses" which means we have to allow only 62 hosts-per-subnet -> B is correct.

Question 2

Refer to the exhibit. The Lakeside Company has the internetwork in the exhibit. The Administrator would like to reduce the size of the routing table to the Central Router. Which partial routing table entry in the Central router represents a route summary that represents the LANs in Phoenix but no additional subnets?



A. 10.0.0.0 /22 is subnetted, 1 subnet
D 10.0.0.0 [90/20514560] via 10.2.0.2 6w0d, serial 0/1

B. 10.0.0.0 /28 is subnetted, 1 subnet
D 10.2.0.0 [90/20514560] via 10.2.0.2 6w0d, serial 0/1

C. 10.0.0.0 /30 is subnetted, 1 subnet
D 10.2.2.0 [90/20514560] via 10.2.0.2 6w0d, serial 0/1

D. 10.0.0.0 /22 is subnetted, 1 subnet
D 10.4.0.0 [90/20514560] via 10.2.0.2 6w0d, serial 0/1

E. 10.0.0.0 /28 is subnetted, 1 subnet
D 10.4.4.0 [90/20514560] via 10.2.0.2 6w0d, serial 0/1

F. 10.0.0.0 /30 is subnetted, 1 subnet
D 10.4.4.4 [90/20514560] via 10.2.0.2 6w0d, serial 0/1

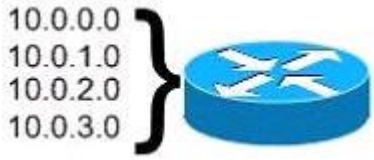
Answer: D

Explanation

All the above networks can be summarized to 10.0.0.0 network but the question requires to "represent the LANs in Phoenix but no additional subnets" so we must summarized to 10.4.0.0 network. The Phoenix router has 4 subnets so we need to "move left" 2 bits of "/24″-> /22 is the best choice -> D is correct.

Question 3

Refer to the exhibit. What is the most appropriate summarization for these routes?



A. 10.0.0.0/21
B. 10.0.0.0/22
C. 10.0.0.0/23
D. 10.0.0.0/24

Answer: B

Explanation

We need to summarize 4 subnets so we have to move left 2 bits ($2^2 = 4$). In this question we can guess the initial subnet mask is /24 because 10.0.0.0, 10.0.1.0, 10.0.2.0, 10.0.3.0 belong to different networks. So "/24″ moves left 2 bits -> /22.

Question 4

A national retail chain needs to design an IP addressing scheme to support a nationwide network. The company needs a minimum of 300 sub-networks and a maximum of 50 host addresses per subnet. Working with only one Class B address, which of the following subnet masks will support an appropriate addressing scheme? (Choose two)

A. 255.255.255.0
B. 255.255.255.128
C. 255.255.252.0
D. 255.255.255.224
E. 255.255.255.192
F. 255.255.248.0

Answer: B E

Explanation

We need to remember the default subnet mask of class B is 255.255.0.0. Next, the company requires a minimum of 300 sub-networks so we have to use at least 512 sub-networks (because 512 is the minimum power of 2 and greater than 300). Therefore we need to get 9 bits for network mask (2^9=512), leaving 7 bits for hosts which is 2^7= 128 > 50 hosts per subnet.This scheme satisfies the requirement -> B is correct.

```
255.255.0.0 = 11111111.11111111.00000000.00000000
                                take 9 bits
255.255.255.128 = 11111111.11111111.11111111.10000000
```

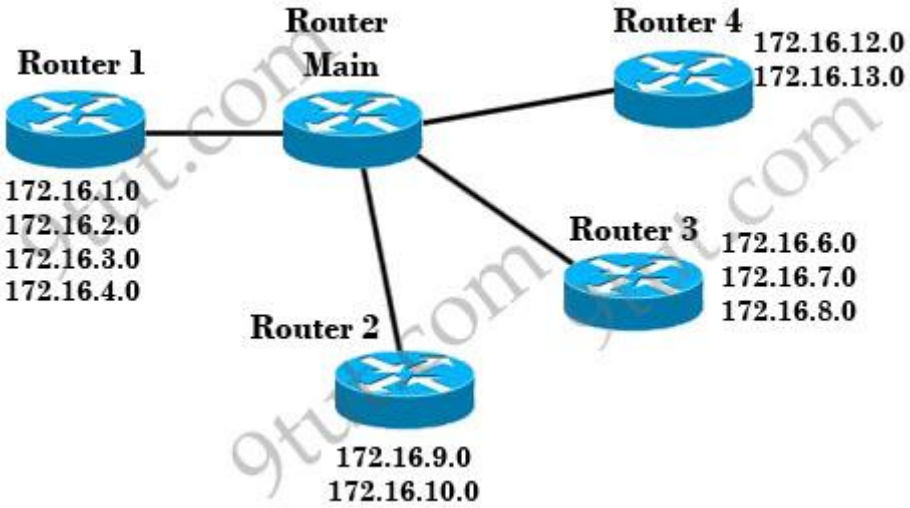
We can increase the sub-networks to 1024 ($1024 = 2^{10}$), leaving 6 bits for hosts that is $2^6 = 64 > 50$ hosts. This scheme satisfies the requirement, too -> E is correct.

```
255.255.0.0 = 11111111.11111111.00000000.00000000
                                take 10 bits
255.255.255.192 = 11111111.11111111.11111111.11000000
```

Notice: The question asks "The company needs a minimum of 300 sub-networks and a maximum of 50 host addresses per subnet" but this is a typo, you should understand it as ""The company needs a minimum of 300 sub-networks and a minimum of 50 host addresses per subnet".

Question 5

Which address range efficiently summarizes the routing table of the addresses for router main?



A. 172.16.0.0/18
B. 172.16.0.0/16
C. 172.16.0.0/20
D. 172.16.0.0/21

Answer: C

Explanation

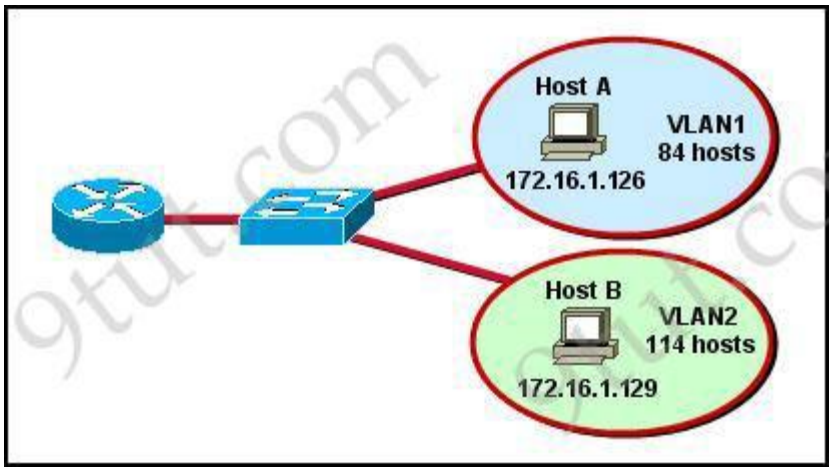
To summarize these networks efficiently we need to find out a network that "covers" from 172.16.1.0 -> 172.16.13.0 (including 13 networks < 16). So we need to use 4 bits (2^4 = 16). Notice that we have to move the borrowed bits to the left (not right) because we are summarizing.

The network 172.16.0.0 belongs to class B with a default subnet mask of /16 but in this case it has been subnetted with a subnet mask of /24 (we can guess because 172.16.1.0, 172.16.2.0, 172.16.3.0… are different networks).

Therefore "move 4 bits to the left" of "/24″ will give us "/20″ -> C is the correct answer.

Question 6

Refer to the diagram. All hosts have connectivity with one another. Which statements describe the addressing scheme that is in use in the network? (Choose three)



A. The subnet mask in use is 255.255.255.192.
B. The subnet mask in use is 255.255.255.128.
C. The IP address 172.16.1.25 can be assigned to hosts in VLAN1
D. The IP address 172.16.1.205 can be assigned to hosts in VLAN1
E. The LAN interface of the router is configured with one IP address.
F. The LAN interface of the router is configured with multiple IP addresses.

Answer: B C F

Explanation

First we should notice that different VLANs must use different sub-networks. In this case Host A (172.16.1.126) and Host B (172.16.1.129) are in different VLANs and must use different sub-networks. Therefore the subnet mask in use here should be 255.255.255.128. In particular, it is 172.16.1.0/25 with 2 sub-networks:

+ Sub-network 1: 172.16.1.0 -> 172.16.1.127 (assigned to VLAN 1)
+ Sub-network 2: 172.16.1.128 -> 172.16.1.255 (assigned to VLAN 2)

-> B is correct.

The IP address 172.16.1.25, which is in the same sub-network with host A so it can be assigned to VLAN 1 -> C is correct.

To make different VLANs communicate with each other we can configure sub-interfaces (with a different IP address on each interface) on the LAN interface of the router -> F is correct.

Question 7

The network administrator needs to address seven LANs. RIP version 1 is the only routing protocol in use on the network and subnet 0 is not being used. What is the maximum number of usable IP addresses that can be supported on each LAN if the organization is using one class C address block?

A. 6
B. 8
C. 14
D. 16
E. 30
F. 32

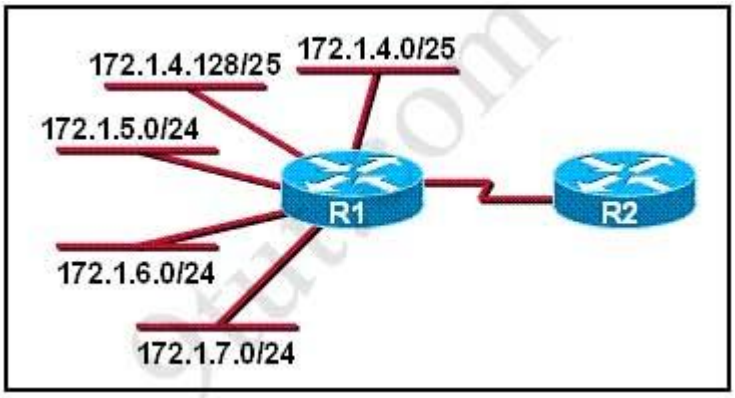
Answer: E

Explanation

"The network administrator needs to address seven LANs" means we have 7 subnets < 8 = 2^3, so we need to borrow 3 bits from the host part (to create 8 subnets). We are using class C address block which has 8 bits 0 (the default subnet mask of class C is 255.255.255.0), so the number of bit 0 left is 8 – 3 = 5. Therefore the hosts per subnet will be 2^5 – 2 = 30 -> E is correct.

Question 8

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



A. 172.1.0.0/22

B. 172.1.0.0/21

C. 172.1.4.0/22

D. 172.1.4.0/24
172.1.5.0/24
172.1.6.0/24
172.1.7.0/24

E. 172.1.4.0/25
172.1.4.128/25
172.1.5.0/24
172.1.6.0/24
172.1.7.0/24

Answer: C

Explanation

Network 172.1.4.0/25 and network 172.1.4.128/25 can be grouped to a single network 172.1.4.0/24

Network 172.1.4.0/24 + Network 172.1.5.0/24 + Network 172.1.6.0/24 + Network 172.1.7.0/24 can be grouped to a single network 172.1.4.0/22 because we have all 4 subnetworks so we can move left 2 bits (2^2=4).

Question 9

```
Gateway of last resort is not set
192.168.25.0/30 is subnetted, 4 subnets
D 192.168.25.20 [90/2681856] via 192.168.15.5, 00:00:10, Serial0/1
D 192.168.25.16 [90/1823638] via 192.168.15.5, 00:00:50, Serial0/1
D 192.168.25.24 [90/3837233] via 192.168.15.5, 00:05:23, Serial0/1
D 192.168.25.28 [90/8127323] via 192.168.15.5, 00:06:45, Serial0/1
C 192.168.15.4/30 is directly connected, Serial0/1
C 192.168.2.0/24 is directly connected, FastEthernet0/0
```

Which address and mask combination a summary of the routes learned by EIGRP?

A. 192.168.25.0 255.255.255.240
B. 192.168.25.16 255.255.255.252
C. 192.168.25.0 255.255.255.252
D. 192.168.25.28 255.255.255.240
E. 192.168.25.16 255.255.255.240
F. 192.168.25.28 255.255.255.240

Answer: E

Explanation

We have 4 routes learned by EIGRP:

D 192.168.25.20 [90/2681856] via 192.168.15.5, 00:00:10, Serial0/1
D 192.168.25.16 [90/1823638] via 192.168.15.5, 00:00:50, Serial0/1
D 192.168.25.24 [90/3837233] via 192.168.15.5, 00:05:23, Serial0/1
D 192.168.25.28 [90/8127323] via 192.168.15.5, 00:06:45, Serial0/1

These subnets are all /30 (as it says "192.168.25.0/30 is subnetted, 4 subnets". We have 4 successive subnets = 2^2 so we can go back 2 bits -> the summarized subnet mask is 30 – 2 = 28 and the summarized network is 192.168.25.16.

CCNA – IP Routing Questions

Question 1

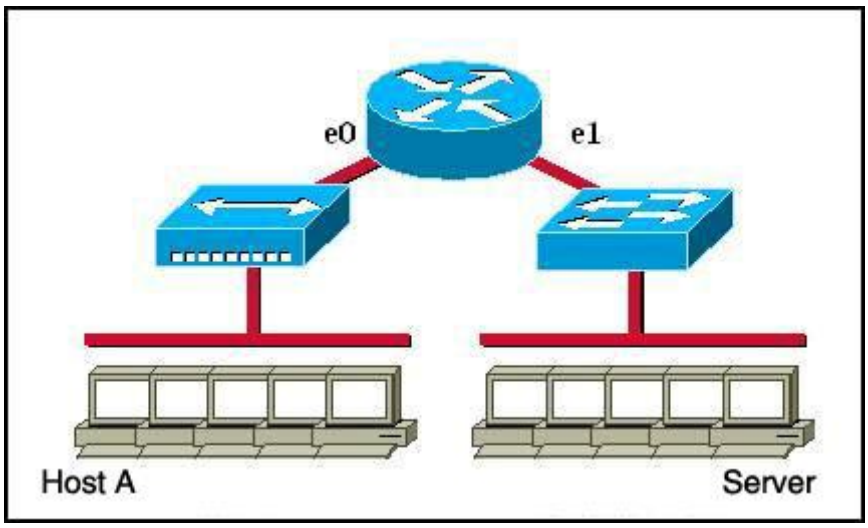
A router receives information about network 192.168.10.0/24 from multiple sources. What will the router consider the most reliable information about the path to that network?

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

Answer: E

Question 2

Refer to the graphic.



Host A is communicating with the server. What will be the source MAC address of the frames received by Host A from the server?

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

Answer: A

Question 3

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

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

Answer: B

Explanation

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

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

Question 4

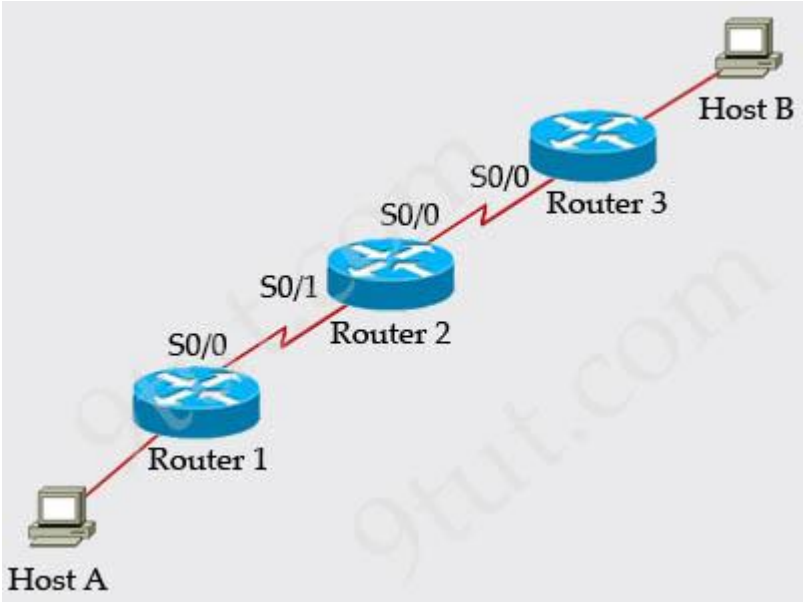
A router has two FastEthernet interfaces and needs to connect to four vlans in the local network. How can you accomplish this task, using the fewest physical interfaces and without decreasing network performance?

A. Add two more FastEthernet interfaces.
B. Add a second router to handle the vlan traffic.
C. Use a hub to connect the four vlans with a FastEthernet interface on router.
D. Implement a router-on-a-stick configuration.

Answer: D

Question 5

Refer to the exhibit, Host A pings interface S0/0 on router 3, what is the TTL value for that ping?



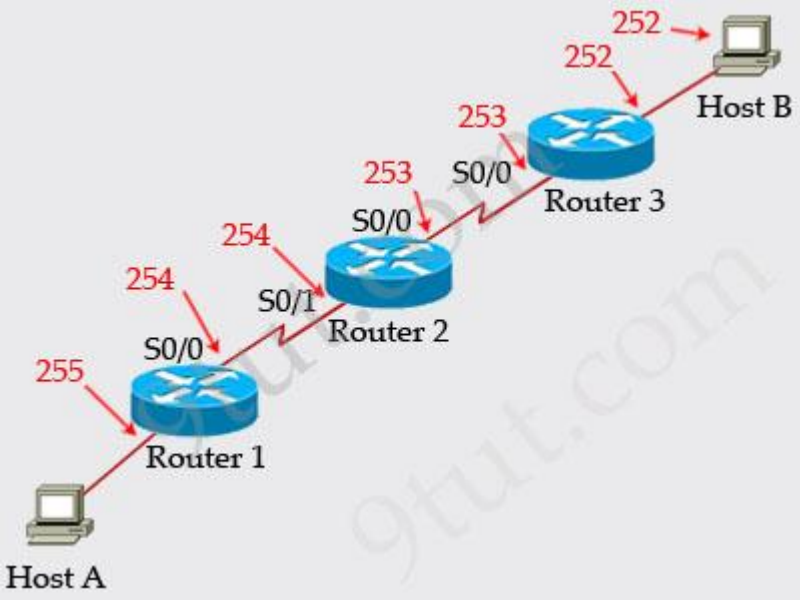
A. 253
B. 252
C. 255
D. 254

Answer: A

Explanation

From the CCNA ICND2 Exam book: "Routers decrement the TTL by 1 every time they forward a packet; if a router decrements the TTL to 0, it throws away the packet. This prevents packets from rotating forever." I want to make it clear that before the router forwards a packet, the TTL is still remain the same. For example in the topology above, pings to S0/1 and S0/0 of Router 2 have the same TTL.

The picture below shows TTL values for each interface of each router and for Host B. Notice that Host A initializes ICMP packet with a TTL of 255:



Question 6

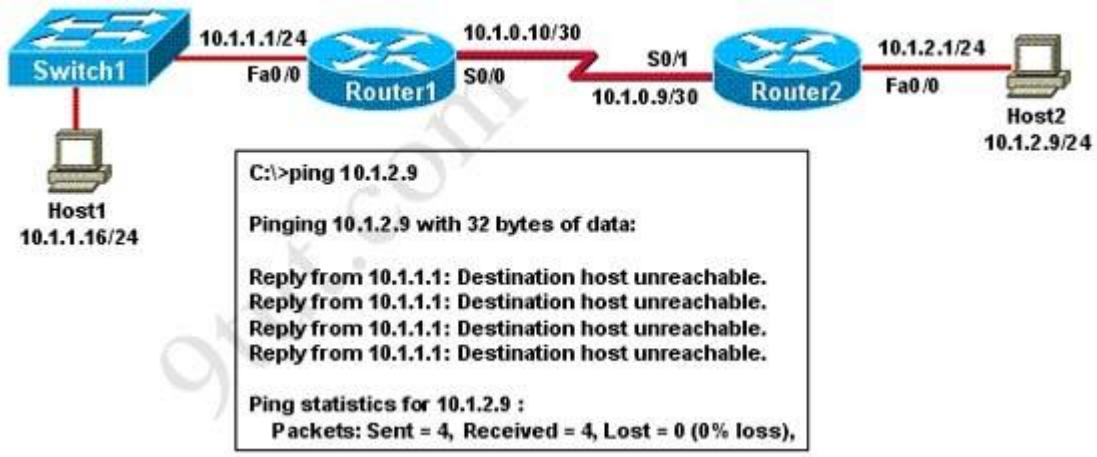
If IP routing is enabled, which two commands set the gateway of last resort to the default gateway? (Choose two)

A. ip default-gateway 0.0.0.0
B. ip route 172.16.2.1 0.0.0.0 0.0.0.0
C. ip default-network 0.0.0.0
D. ip default-route 0.0.0.0 0.0.0.0 172.16.2.1
E. ip route 0.0.0.0 0.0.0.0 172.16.2.1

Answer: C E

Question 7

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



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

Answer: C

Explanation

In this question, Host1 wants to ping Host2 but it receives a reply from the interface Fa0/0 of Router1 (10.1.1.1/24) that the "destination host unreachable".

If the link between Host1 and Switch1 is down or the link between Switch1 and Router1 is down then Host1 can not receive this reply -> A and F are not correct.

Host1 can receive a reply from 10.1.1.1 -> the TCP/IP is working properly -> B is not correct.

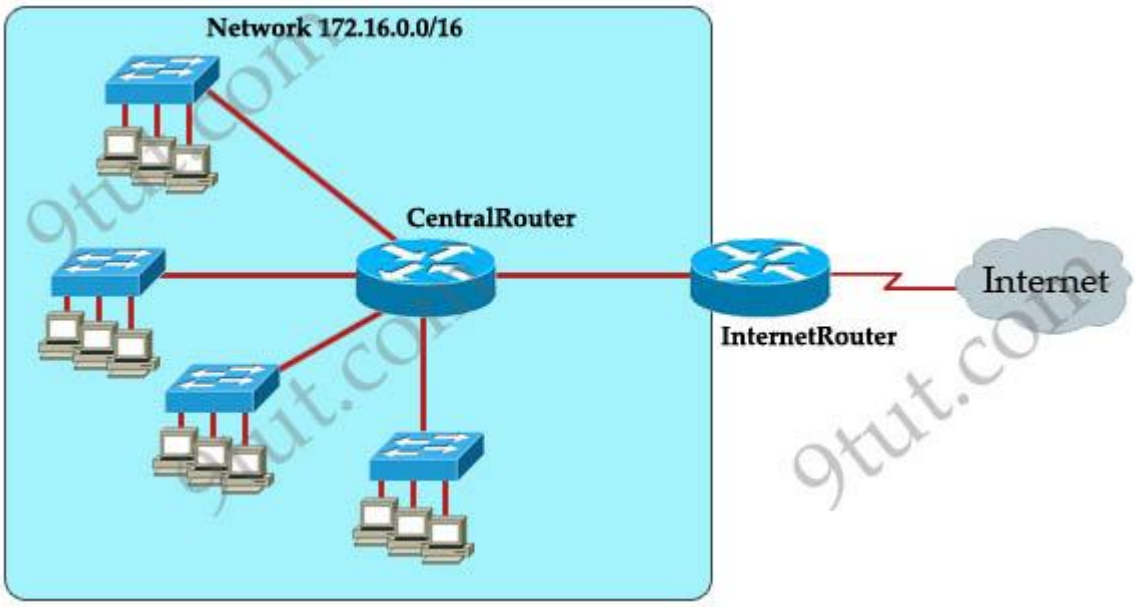
For answer D, if the default gateway was not configured correctly on Host1 (in this case the default gateway should be 10.1.1.1/24) then 10.1.1.1 can not receive the ping packets from Host1 and can not reply for Host1 that the destination is unreachable -> D is not correct.

Interface Fa0/0 on Router1 replies for the ping packets from Host1 so it is up -> E is not correct. If the interface Fa0/0 on Router is shutdown then we will receive a message of "Request timed out", not "Destination host unreachable".

Answer C is correct because we can get a reply from the interface Fa0/0 of Router1 so the link between Host1 and Router1 should be fine -> the problem lies at the other side of Router1. But if the link between Router2 and Host2 is down then we will receive a reply from interface S0/1 of Router2 that the "destination host unreachable". Therefore the problem can just be the link between Router1 and Router2.

Question 8

Refer to the exhibit. The network administrator requires easy configuration options and minimal routing protocol traffic. Which two options provide adequate routing table information for traffic that passes between the two routers and satisfy the requests of the network administrator? (choose two)

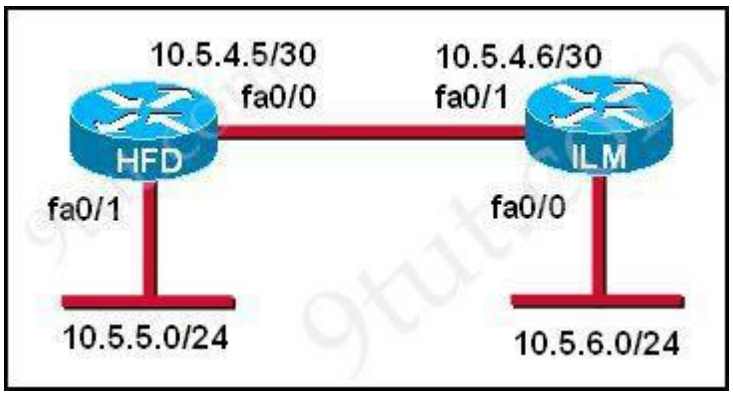


A. a dynamic routing protocol on InternetRouter to advertise summarized routers to CentralRouter.
B. a dynamic routing protocol on CentralRouter to advertise summarized routers to InternetRouter.
C. a static route on InternetRouter to direct traffic that is destined for 172.16.0.0/16 to CentralRouter.
D. a dynamic routing protocol on InternetRouter to advertise all routes to CentralRouter.
E. a dynamic routing protocol on CentralRouer to advertise all routes to InternetRouter
F. a static, default route on CentralRouter that directs traffic to InternetRouter.

Answer: C F

Question 9

Refer to the graphic. A static route to the 10.5.6.0/24 network is to be configured on the HFD router. Which commands will accomplish this? (Choose two)



A. HFD (config) #ip route 10.5.6.0 0.0.0.255 fa0/0
B. HFD(config)# ip route 10.5.6.0 0.0.0.255 10.5.4.6
C. HFD(config)# ip route 10.5.6.0 255.255.255.0 fa0/0
D. HFD(config)# ip route 10.5.6.0 255.255.255.0 10.5.4.6

E. HFD(config)# ip route 10.5.4.6 0.0.0.255 10.5.6.0
F. HFD(config)# ip route 10.5.4.6 255.255.255.0 10.5.6.0

Answer: C D

Explanation

The simple syntax of static route:

ip route destination-network-address subnet-mask {next-hop-IP-address | exit-interface}
+ **destination-network-address:** destination network address of the remote network
+ **subnet mask:** subnet mask of the destination network
+ **next-hop-IP-address:** the IP address of the receiving interface on the next-hop router
+ **exit-interface:** the local interface of this router where the packets will go out

In the statement "ip route 10.5.6.0 255.255.255.0 fa0/0″:

+ 10.5.6.0 255.255.255.0: the destination network
+ fa0/0: the exit-interface

CCNA – IP Routing 2

Question 1

Users on the 172.17.22.0 network cannot reach the server located on the 172.31.5.0 network. The network administrator connected to router Coffee via the console port, issued the **show ip route** command. Based on the output of the **show ip route** command and the topology shown in the graphic, what is the cause of the failure?


```
Coffee #show 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

Gateway of last resort is 172.19.22.2 to network 0.0.0.0

C      172.17.22.0 is directly connected, FastEthernet0/0
C      172.18.22.0 is directly connected, Serial0/0
S*     0.0.0.0/0 [1/0] via 172.19.22.2
```

A. The network has not fully converged.
B. IP routing is not enabled.

C. A static route is configured incorrectly.
D. The FastEthernet interface on Coffee is disabled.
E. The neighbor relationship table is not correctly updated.
F. The routing table on Coffee has not updated.

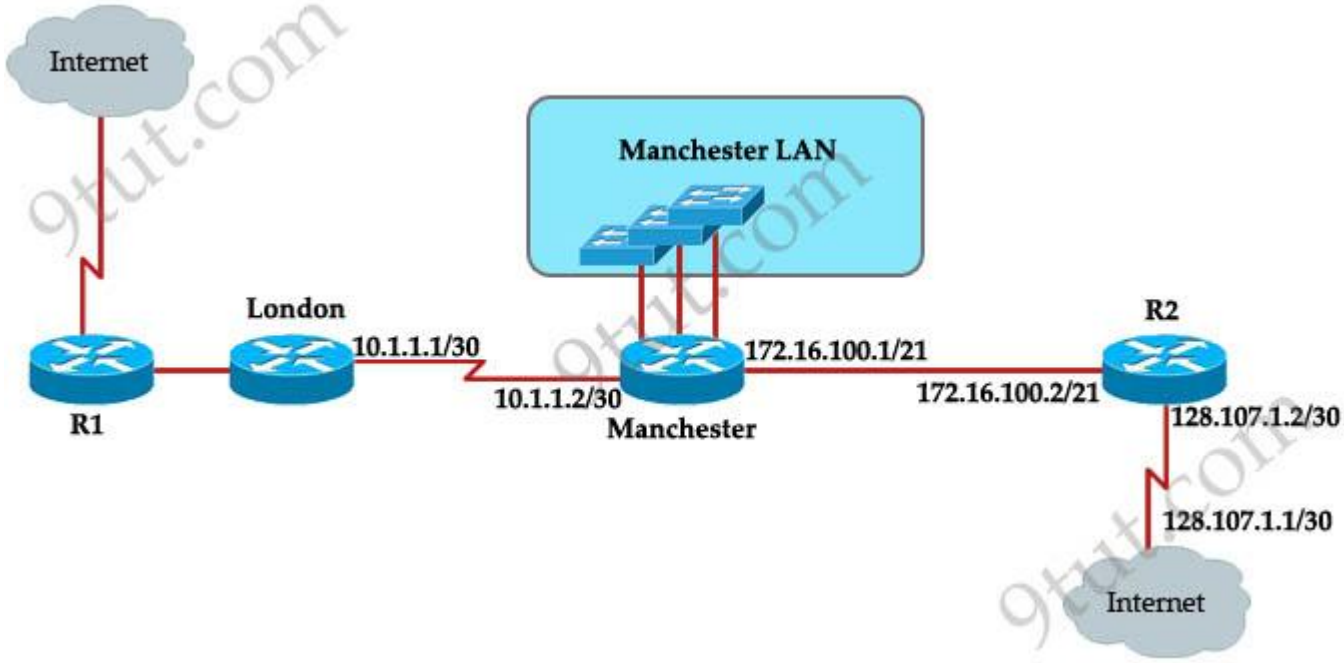
Answer: C

Explanation

There are no dynamic routing protocols running on Coffee router, only a default route is configured to route all traffic to 172.19.22.2 but we don't know about this network. The correct IP address should be the IP address on the interface of Tea router which is connected to Coffee router (maybe 172.18.22.2).

Question 2

The speed of all serial links is E1 and the speed of the all other links is 100Mb/s. A static route will be established on the Manchester router to direct traffic toward to the internet over the most direct path available. What configuration of the Manchester router will establish a route toward to the internet for traffic from workstation on the Manchester LAN?



A. ip route 0.0.0.0 255.255.255.0 172.16.100.2
B. ip route 0.0.0.0 255.255.255.252 128.107.1.1
C. ip route 0.0.0.0 0.0.0.0 128.107.1.1
D. ip route 0.0.0.00.0:0:0 172.16.100.1
E. ip route 0.0.0.0 255.255.255.255 172.16.100.2
F. ip route 0.0.0.0 0.0.0.0 172.16.100.2

Answer: F

Explanation

Maybe “the most direct path available” here means via R2 because it is directly connected with the Internet while the London path needs to go through R1. So we need a command to send traffic to R2 and the correct command is “ip route 0.0.0.0 0.0.0.0 172.16.100.2″.

Question 3

Which two are advantages of static routing when compared to dynamic routing? (choose two)

A. Security increases because only the network administrator may change the routing tables.
B. Configuration complexity decreases as network size increases.
C. Routing updates are automatically sent to neighbors.
D. Route summarization is computed automatically by the router.
E. Routing traffic load is reduced when used in stub network links.
F. An efficient algorithm is used to build routing tables using automatic updates.
G. Routing tables adapt automatically to topology changes.

Answer: A E

Question 4

Refer to the exhibit. According to the routing table, where will the router send a packet destined for 10.1.5.65?

Network	Interface	Next-hop
10.1.1.0/24	e0	directly connected
10.1.2.0/24	e1	directly connected
10.1.3.0/25	s0	directly connected
10.1.4.0/24	s1	directly connected
10.1.5.0/24	e0	10.1.1.2
10.1.5.64/28	e1	10.1.2.2
10.1.5.64/29	s0	10.1.3.3
10.1.5.64/27	s1	10.1.4.4

A. 10.1.1.2
B. 10.1.2.2
C. 10.1.3.3
D. 10.1.4.4

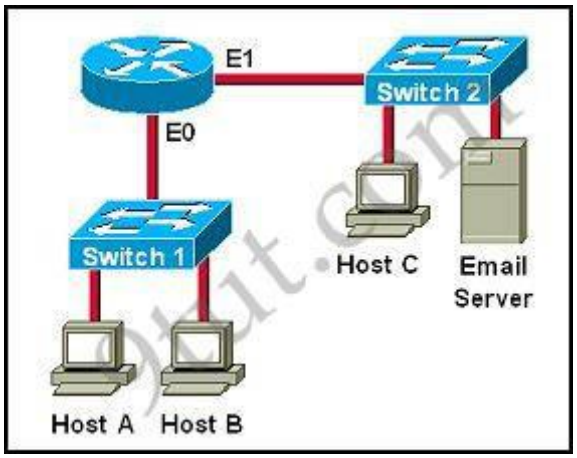
Answer: C

Explanation

The destination IP address 10.1.5.65 belongs to 10.1.5.64/28, 10.1.5.64/29 & 10.1.5.64/27 subnets but the "longest prefix match" algorithm will choose the most specific subnet mask -> the prefix "/29″ will be chosen to route the packet. Therefore the next-hop should be 10.1.3.3 -> C is correct.

Question 5

Which destination addresses will be used by Host A to send data to Host C? (Choose two)



A. the IP address of Switch 1
B. the MAC address of Switch 1
C. the IP address of Host C
D. the MAC address of Host C
E. the IP address of the router's E0 interface
F. the MAC address of the router's E0 interface

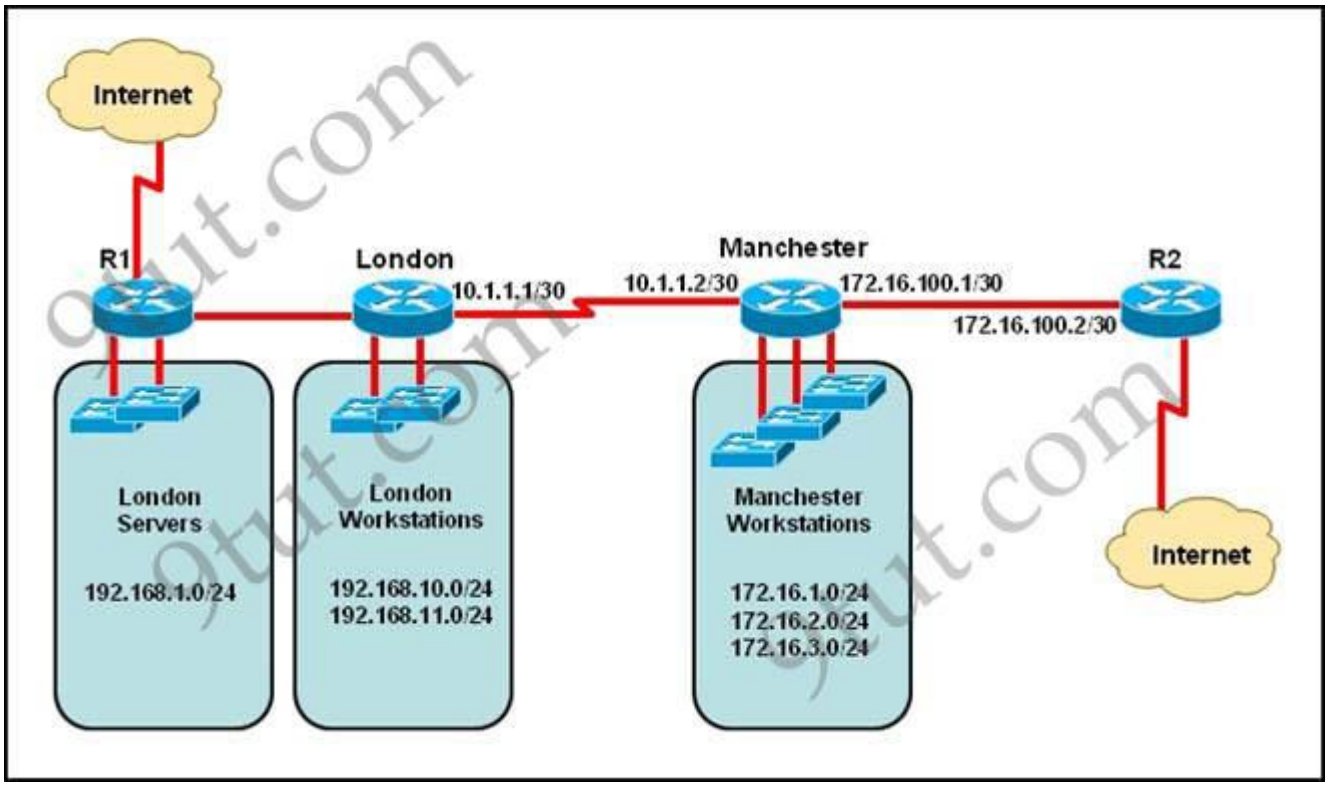
Answer: C F

Explanation

While transferring data through many different networks, the source and destination IP addresses are not changed. Only the source and destination MAC addresses are changed. So in this case Host A will use the IP address of Host C and the MAC address of E0 interface to send data. When the router receives this data, it replaces the source MAC address with it own E1 interface's MAC address and replaces the destination MAC address with Host C's MAC address before sending to Host C -> C and F are correct.

Question 6

Refer to the exhibit. The network administrator must establish a route by which London workstations can forward traffic to the Manchester workstations. What is the simplest way to accomplish this?



A. Configure a dynamic routing protocol on London to advertise all routes to Manchester.
B. Configure a dynamic routing protocol on London to advertise summarized routes to Manchester.
C. Configure a dynamic routing protocol on Manchester to advertise a default route to the London router.
D. Configure a static default route on London with a next hop of 10.1.1.1.
E. Configure a static route on London to direct all traffic destined for 172.16.0.0/22 to 10.1.1.2.
F. Configure Manchester to advertise a static default route to London.

Answer: E

Question 7

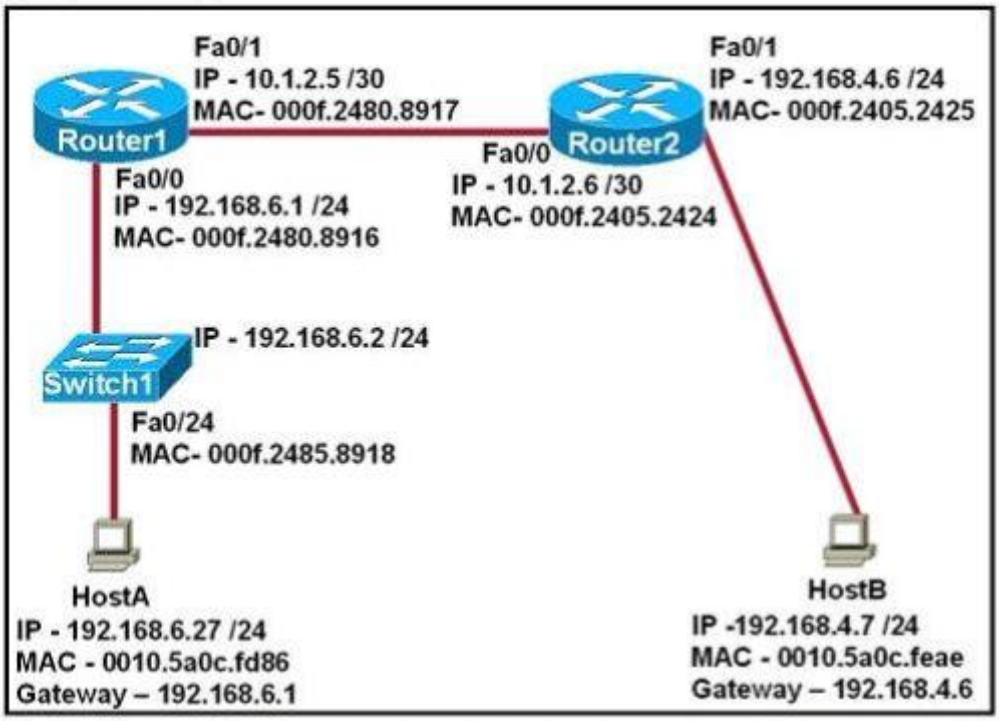
Which parameter can be tuned to affect the selection of a static route as a backup when a dynamic protocol is also being used?

A. link bandwidth
B. hop count
C. link cost
D. administrative distance
E. link delay

Answer: D

Question 8

Refer to the exhibit:



After HostA pings HostB, which entry will be in the ARP cache of HostA to support this transmission?

A.

Interface Address	Physical Address	Type
192.168.4.7	000f.2480.8916	dynamic

B.

Interface Address	Physical Address	Type
192.168.4.7	0010.5a0c.feae	dynamic

C.

Interface Address	Physical Address	Type
192.168.6.1	0010.5a0c.feae	dynamic

D.

Interface Address	Physical Address	Type
192.168.6.1	000f.2480.8916	dynamic

E.

Interface Address	Physical Address	Type
192.168.6.2	0010.5a0c.feae	dynamic

F.

Interface Address	Physical Address	Type
192.168.6.2	000f.2485.8918	dynamic

Answer: D

Explanation

Host A knows host B is in another network so it will send the pings to its default gateway 192.168.6.1. Host A sends a broadcast frame asking the MAC address of 192.168.6.1. These information (IP and MAC address of the default gateway) is saved in its ARP cache for later use.

CCNA – Frame Relay

Note: If you are not sure about Frame Relay, please read our Frame Relay Tutorial.

Question 1

The output of the show frame-relay pvc command shows ”PVC STATUS=INACTIVE”. What does this mean?

A. The PVC is configured correctly and is operating normally,but no data packets have been detected for more than five minutes.
B. The PVC is configured correctly, is operating normally and is no longer actively seeking the address the remote route.
C. The PVC is configured correctly, is operating normally and is waiting for interesting to trigger a call to the remote router.
D. The PVC is configured correctly on the local switch, but there is a problem on the remote end of the PVC.
E. The PVC is not configured on the switch.

Answer: D

Explanation

The PVC STATUS displays the status of the PVC. The DCE device creates and sends the report to the DTE devices. There are 4 statuses:

+ ACTIVE: the PVC is operational and can transmit data
+ INACTIVE: the connection from the local router to the switch is working, but the connection to the remote router is not available
+ DELETED: the PVC is not present and no LMI information is being received from the Frame Relay switch
+ STATIC: the Local Management Interface (LMI) mechanism on the interface is disabled (by using the “no keepalive” command). This status is rarely seen so it is ignored in some books.

Question 2

Which command allows you to verify the encapsulation type (CISCO or IETF) for a frame relay link?

A. show frame-relay map
B. show frame-relay lmi
C. show inter serial
D. show frame-relay pvc

Answer: A

Explanation

The “show frame-relay map” command displays the current map entries and information about the connections, including encapsulation type.

You can check Table 33 in the following link:
http://www.cisco.com/en/US/docs/ios/12_2/wan/command/reference/wrffr4.html#wp1029343

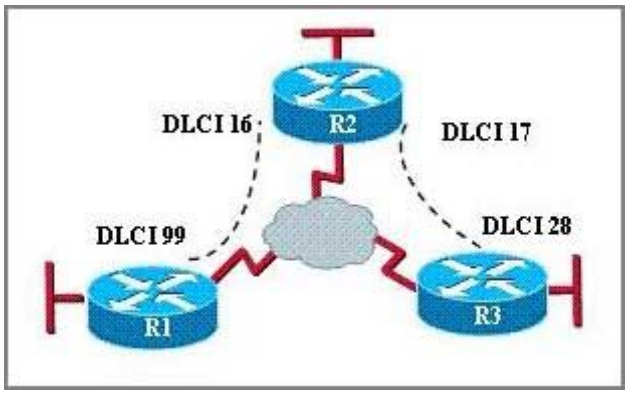
It clearly states there is a Field which can be Cisco or IETF, which “indicates the encapsulation type for this map”. We quote that Table 33 here for your quick reference (you will see what we want to imply in bold):

Field	Description
Serial 1 (administratively down)	Identifies a Frame Relay interface and its status (up or down).
ip 131.108.177.177	Destination IP address.
dlci 177 (0xB1,0x2C10)	DLCI that identifies the logical connection being used to reach this interface. This value is displayed in three ways: its decimal value (177), its hexadecimal value (0xB1), and its value as it would appear on the wire (0x2C10).
static	Indicates whether this is a static or dynamic entry.
CISCO	**Indicates the encapsulation type for this map; either CISCO or IETF.**
TCP/IP Header Compression (inherited), passive (inherited)	Indicates whether the TCP/IP header compression characteristics were inherited from the interface or were explicitly configured for the IP map.

The “show frame-relay lmi” gives us information about the LMI encapsulation type used by the Frame Relay interface, which can be ANSI, CISCO or Q933a. Therefore it is not what the question requires (CISCO or IETF).

Question 3

Refer to the exhibit. Which statement describes DLCI 17?



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

Answer: C

Explanation

DLCI stands for Data Link Connection Identifier. DLCI values are used on Frame Relay interfaces to distinguish between different virtual circuits. DLCIs have local significance because the identifier references the point between the local router and the local Frame Relay switch to which the DLCI is connected.

Question 4

Users have been complaining that their Frame Relay connection to the corporate site is very slow. The network administrator suspects that the link is overloaded. Based on the partial output of the **Router#show frame relay pvc** command shown in the graphic, which output value indicates to the local router that traffic sent to the corporate site is experiencing congestion?

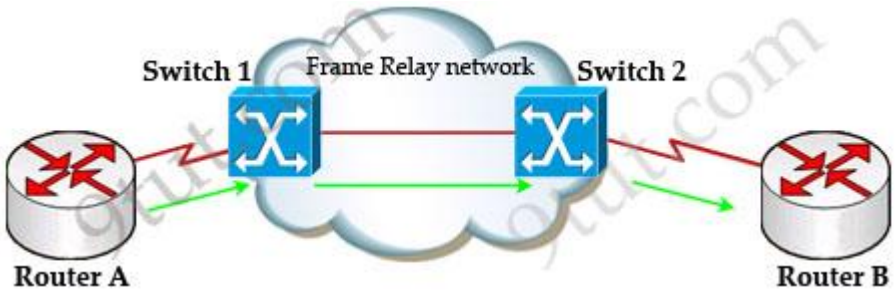
```
PVC Statistics for interface Serial0 (Frame Relay DTE)

        Active   Inactive   Deleted   Static
Local      1          0         0        0
Switched   0          0         0        0
Unused     0          0         0        0

DLCI = 100, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE =
Serial0

 input pkts 1300          output pkts 1270        in bytes 22121000
 out bytes 21802000       dropped pkts 4          in FECN pkts 147
 in BECN pkts 192         out FECN pkts 259       out BECN pkts 214
 in DE pkts 0             out DE pkts 0
 out bcast pkts 107       out bcast bytes 19722
 pvc create time 00:25:50, last time pvc status changed 00:25:40
```

A. DLCI=100
B. last time PVC status changed 00:25:40
C. in BECN packets 192
D. in FECN packets 147
E. in DF packets 0

Answer: C

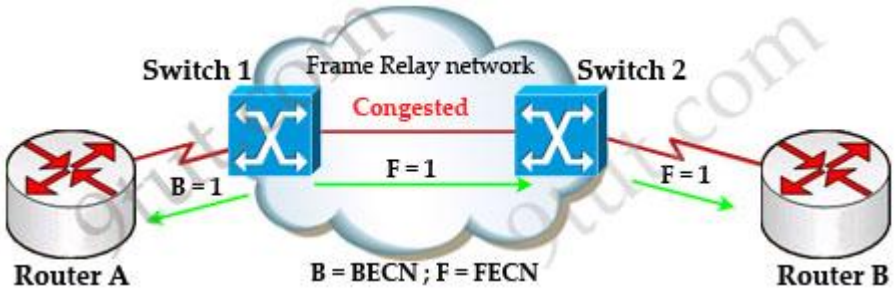
Explanation

First we should grasp the concept of BECN & FECN through an example:



Suppose Router A wants to send data to Router B through a Frame Relay network. If the network is congested, Switch 1 (a DCE device) will set the FECN bit value of that frame to 1, indicating that frame experienced congestion in the path from source to destination. This frame is forwarded to Switch 2 and to Router B (with the FECN bit = 1).

Switch 1 knows that the network is congesting so it also sends frames back to Router A with BECN bit set to 1 to inform that path through the network is congested.



In general, BECN is used on frames traveling away from the congested area to warn source devices that congestion has occurred on that path while FECN is used to alert receiving devices if the frame experiences congestion.

BECN also informs the transmitting devices to slow down the traffic a bit until the network returns to normal state.

The question asks “which output value indicates to the local router that traffic sent to the corporate site is experiencing congestion” which means it asks about the returned parameter which indicates congestion -> BECN.

Question 5

What occurs on a Frame Relay network when the CIR is exceeded?

A. All TCP traffic is marked discard eligible.
B. All UDP traffic is marked discard eligible and a BECN is sent.
C. All TCP traffic is marked discard eligible and a BECN is sent.
D. All traffic exceeding the CIR is marked discard eligible.

Answer: D

Explanation

Committed information rate (CIR): The minimum guaranteed data transfer rate agreed to by the Frame Relay switch. Frames that are sent in excess of the CIR are marked as discard eligible (DE) which means they can be dropped if the congestion occurs within the Frame Relay network.

Note: In the Frame Relay frame format, there is a bit called Discard eligible (DE) bit that is used to identify frames that are first to be dropped when the CIR is exceeded.

Question 6

What command is used to verify the DLCI destination address in a Frame Relay static configuration?

A show frame-relay pvc
B. show frame-relay lmi
C. show frame-relay map
D. show frame relay end-to-end

Answer: C

Question 7

```
Router 1# show running-config

interface serial0/0
bandwidth 64
ip address 172.16.100.2 255.255.0.0
encapsulation frame-relay
frame-relay map ip 172.16.100.1 100 broadcast
```

As a technician, you found the router1 is unable to reach the second router. Both routers are running IOS version 12.0.
Based on this information, what is the most likely cause of the problem?

A. incorrect IP address
B. incorrect bandwidth configuration
C. incorrect map statement
D. incorrect LMI configuration

Answer: C (In fact none is correct)

Explanation

First we have to say this is an unclear question and it is wrong. The "frame-relay map ip" statement is correct thus none of the four answers above is correct. But we guess there is a typo in the output. Maybe the "ip address 172.16.100.2 255.255.0.0″ command should be "ip address 172.16.100.1 255.255.0.0″. That makes answer C correct.

Question 8

Refer to the exhibit. What is the meaning of the term **dynamic** as displayed in the output of the show frame-relay map command shown?

```
R1# show frame-relay map
Serial0/0 (up): ip 172.16.3.1 dlci 100 (0x64, 0x1840), dynamic
              broadcast,, status defined, active
```

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

Answer: E

Explanation

The term dynamic indicates that the DLCI number and the remote router IP address 172.16.3.1 are learned via the Inverse ARP process.

Inverse ARP is a technique by which dynamic mappings are constructed in a network, allowing a device such as a router to locate the logical network address and associate it with a permanent virtual circuit (PVC).

Question 9

Refer to the exhibit. Which WAN protocol is being used?

```
RouterA#show interface pos8/o/o
pos8/0/0 is up, line protocol is up
Hardware is Packet over Sonet
Keepalive set (10 sec)
Scramble disabled
LMI enq sent 2474988, LMI stat recvd 2474969, LMI upd recvd 0, DTE LMI up
Broadcast queue 0/256, broadcasts sent/dropped 25760668/0, interface broadcasts 25348176
Last Input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters 40w6d
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 39000 bits/sec, 60 packets/sec
      63153396 packets Input, 4389121455 bytes, 0 no buffer
      Received 0 broadcasts (0 IP multicast)
      0 runts, 0 giants, 0 throttles
            0 parity
44773 input errors, 39138 CRC, 0 frame, 0 overrun, 0 ignored, 27 abort
945596253 packets output, 62753244360 bytes, 0 underruns
0 output errors, 0 applique, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
```

A. ATM
B. HDLC
C. Frame Relay
D. PPP

Answer: C

Explanation

Local Management Interface (LMI) is a signaling standard protocol used between your router (DTE) and the first Frame Relay switch. From the output we learn this interface is sending and receiving LMI messages -> Frame Relay is being used.

Question 10

The command **frame-relay map ip 10.121.16.8 102 broadcast** was entered on the router. Which of the following statements is true concerning this command?

A. This command should be executed from the global configuration mode.
B. The IP address 10.121.16.8 is the local router port used to forward data.
C. 102 is the remote DLCI that will receive the information.
D. This command is required for all Frame Relay configurations.
E. The broadcast option allows packets, such as RIP updates, to be forwarded across the PVC.

Answer: E

Explanation

The command **frame-relay map ip 10.121.16.8 102 broadcast** means to mapping the distal IP 10.121.16.8 102to the local DLCI 102. When the "broadcast" keyword is included, it turns Frame Relay network as a broadcast network, which can forward broadcasts.

CCNA – Frame Relay 2

Note: If you are not sure about Frame Relay, please read our Frame Relay Tutorial.

Question 1

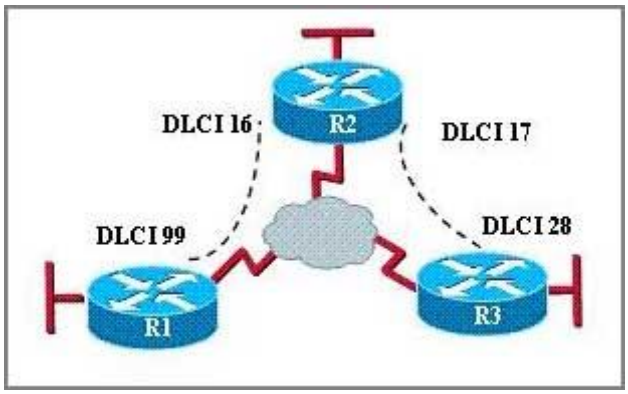
What are two characteristics of Frame Relay point-to-point subinterfaces? (Choose two)

A. They create split-horizon issues.
B. They require a unique subnet within a routing domain.
C. They emulate leased lines.
D. They are ideal for full-mesh topologies.
E. They require the use of NBMA options when using OSPF.

Answer: B C

Question 2

In the Frame Relay network, which IP addresses whould be assigned to the interfaces with point-to-point PVCs?



A. DLCI 16 192.168.10.1/24
DLCI 17 192.168.10.1/24
DLCI 99 192.168.10.2/24
DLCI 28 192.168.10.3/24

B. DLCI 16 192.168.10.1 /24
DLCI 17 192.168.11.1/24
DLCI 99 192.168.12.1/24
DLCI 28 192.168.13.1/24

C. DLCI 16 192.168.10.1/24
DLCI 17 192.168.11.1/24
DLCI 99 192.168.10.2/24
DLCI 28 192.168.11.2/24

D. DLCI 16 192.168.10.1/24
DLCI 17 192.168.10.2/24
DLCI 99 192.168.10.3/24
DLCI 28 192.168.10.4/24

Answer: C

Question 3

What two statistics appear in **show frame-relay map** output? (Choose two)

A. The number of FECN packets that are received by the router
B. The number of BECN packets that are received by the router
C. The ip address of the local router
D. The value of the local DLCI
E. The status of the PVC that is configured on the router

Answer: D E

Explanation

An example of the output of this command is shown below:

```
R0#show frame-relay map
Serial0/0 (up): ip 192.168.1.2 dlci 102(0x66,0x1860), dynamic,
              broadcast,, status defined, active
Serial0/0 (up): ip 192.168.1.3 dlci 103(0x67,0x1870), dynamic,
              broadcast,, status defined, active
R0#
```

From the output we can see the local DLCI (102 & 103) and the status of the PVC configured on the router (both are defined, active).

Question 4

It has become necessary to configure an existing serial interface to accept a second Frame Relay virtual circuit. Which of the following are required to solve this? (Choose three)

A. configure static frame relay map entries for each subinterface network.
B. remove the ip address from the physical interface
C. create the virtual interfaces with the interface command
D. configure each subinterface with its own IP address
E. disable split horizon to prevent routing loops between the subinterface networks
F. encapsulate the physical interface with multipoint PPP

Answer: B C D

Explanation

To configure subinterface for Frame Relay, first we have to remove the IP address from the physical interface and choose a Frame Relay encapsulation.

Question 5

Which encapsulation type is a Frame Relay encapsulation type that is supported by Cisco routers?

A. Q933-A Annex A
B. IETF
C. ANSI Annex D
D. HDLC

Answer: B

Explanation

Cisco supports two Frame Relay encapsulation types: the **Cisco encapsulation** and the **IETF Frame Relay encapsulation**, which is in conformance with RFC 1490 and RFC 2427. The former is often

used to connect two Cisco routers while the latter is used to connect a Cisco router to a non-Cisco router. You can test with your Cisco router when typing the command Router(config-if)#**encapsulation frame-relay ?** on a WAN link. Below is the output of this command (notice Cisco is the default encapsulation so it is not listed here, just press Enter to use it).

```
R1(config-if)#encapsulation frame-relay ?
  ietf  Use RFC1490/RFC2427 encapsulation
  <cr>
```

Note: Three LMI options are supported by Cisco routers are ansi, Cisco, and Q933a. They represent the ANSI Annex D, Cisco, and ITU Q933-A (Annex A) LMI types, respectively.

HDLC is a WAN protocol same as Frame-Relay and PPP so it is not a Frame Relay encapsulation type.

Question 6

What is the result of issuing the frame-relay map ip 192.168.1.2 202 broadcast command?

A. defines the destination IP address that is used in all broadcast packets on DLCI 202
B. defines the source IP address that is used in all broadcast packets on DLCI 202
C. defines the DLCI on which packets from the 192.168.1.2 IP address are received
D. defines the DLCI that is used for all packets that are sent to the 192.168.1.2 IP address

Answer: D

CCNA – NAT PAT Questions

Note: If you are not sure about NAT PAT, please read our Network Address Translation NAT Tutorial.

Question 1

Which two statements about static NAT translations are true? (choose two)

A. They are always present in the NAT table.
B. They allow connection to be initiated from the outside.
C. They can be configured with access lists, to allow two or more connections to be initiated from the outside.
D. They require no inside or outside interface markings because addresses are statically defined.

Answer: A B

Explanation

With static NAT, translations exist in the NAT translation table as soon as you configure static NAT command(s), and they remain in the translation table until you delete the static NAT command(s).

With dynamic NAT, translations do not exist in the NAT table until the router receives traffic that requires translation. Dynamic translations have a timeout period after which they are purged from the translation table.

-> A is correct.

Because static NAT translations are always present in the NAT table so outside hosts can initiate the connection without being dropped -> B is correct.

Static translations can not be configured with access lists. To configure static NAT, we only need to specify source IP, NAT IP, inside interface & outside interface.

-> C is not correct.

We have to specify which is the inside and outside interface -> D is not correct.

For your information, below is an example of configuring static NAT:

R0(config)#int f0/0
R0(config-if)#ip nat inside

R0(config-if)#int f0/1
R0(config-if)#ip nat outside

R0(config)#ip nat inside source static 10.0.0.1 200.0.0.2

(Reference:
http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080093f31.shtml)

Question 2

What are two benefits of using NAT? (choose two)

A. NAT protects network security because private networks are not advertised.
B. NAT accelerates the routing process because no modifications are made on the packets.
C. Dynamic NAT facilitates connections from the outside of the network.
D. NAT facilitates end-to-end communication when IPsec is enable.
E. NAT eliminates the need to re-address all host that require external access.
F. NAT conserves addresses through host MAC-level multiplexing.

Answer: A E

Explanation

By not reveal the internal IP addresses, NAT adds some security to the inside network -> A is correct.

NAT has to modify the source IP addresses in the packets -> B is not correct.

Connection from the outside to a network through "NAT" is more difficult than a normal network because IP addresses of inside hosts are hidden -> C is not correct.

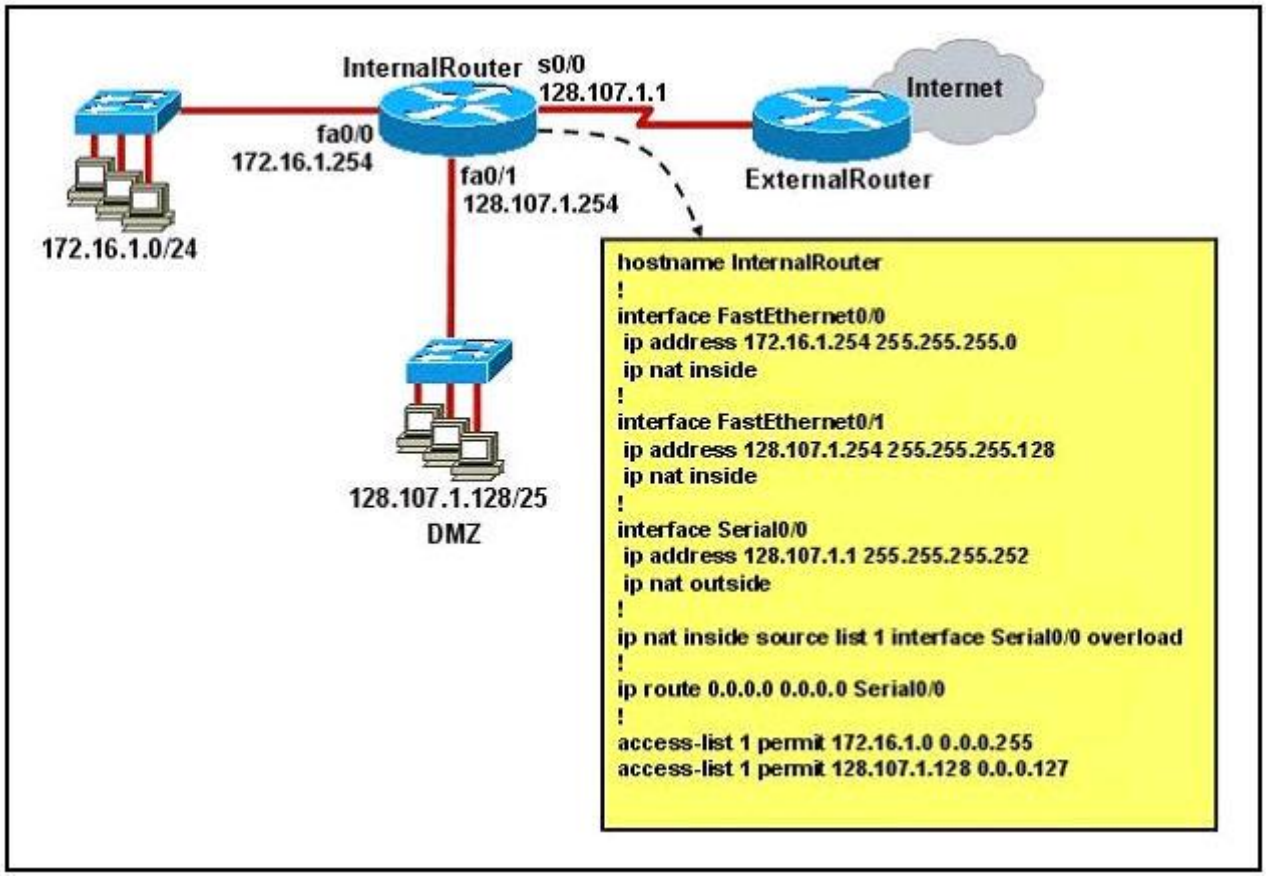
In order for IPsec to work with NAT we need to allow additional protocols, including Internet Key Exchange (IKE), Encapsulating Security Payload (ESP) and Authentication Header (AH) -> more complex -> D is not correct.

By allocating specific public IP addresses to inside hosts, NAT eliminates the need to re-address the inside hosts -> E is correct.

NAT does conserve addresses but not through host MAC-level multiplexing. It conserves addresses by allowing many private IP addresses to use the same public IP address to go to the Internet -> F is not correct.

Question 3

Refer to the exhibit. What statement is true of the configuration for this network?



A. The configuration that is shown provides inadequate outside address space for translation of the number of inside addresses that are supported.

B. Because of the addressing on interface FastEthernet0/1, the Serial0/0 interface address will not support the NAT configuration as shown.
C. The number 1 referred to in the ip nat inside source command references access-list number 1.
D. ExternalRouter must be configured with static routers to network 172.16.2.0/24

Answer: C

Explanation

The "list 1″ refers to the access-list number 1.

CCNA – OSPF Questions

Note: If you are not sure about OSPF, please read our OSPF Tutorial.

Question 1

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

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

Answer: A C D

Question 2

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 RIPv2.

Answer: A C E

Explanation

Answer A and C are obviously correct. For answer E, it allows extensive control of routing updates via Link-State Advertisement (LSA). Administrators can filter these LSAs to meet their requirements easily.

Question 3

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

Question 4

City# show ip interface brief

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

City#

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

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

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

Answer: B C D

Explanation

The "network 192.168.12.64 0.0.0.63″ equals to network 192.168.12.64/26. This network has:
+ Increment: 64 (/26= 1111 1111.1111 1111.1111 1111.1100 0000)
+ Network address: 192.168.12.64
+ Broadcast address: 192.168.12.127
Therefore all interface in the range of this network will join OSPF -> B C D are correct.

Question 5

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

A. 16
B. 2
C. unlimited
D. 4

Answer: D

Explanation

The default number of equal-cost paths that can be placed into the routing of a Cisco OSPF router is 4. We can change this default value by using "maximum-paths" command:

Router(config-router)#maximum-paths 2

Note: Cisco routers support up to 6 equal-cost paths

Question 6

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

Router(config)# router ospf 1
A. All OSPF routers in an area must have the same process ID.
B. Only one process number can be used on the same router.

C. Different process identifiers can be used to run multiple OSPF processes
D. The process number can be any number from 1 to 65,535.
E. Hello packets are sent to each neighbor to determine the processor identifier.

Answer: C D

Question 7

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

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

Answer: A C F

Explanation

Hierarchical design of OSPF (basically means that you can separate the larger internetwork into smaller internetworks called areas) helps us create a network with all features listed above (decrease routing overhead, speed up convergence, confine network instability to single areas of the network).

Question 8

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

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

Answer: A D

Explanation

In the router ospf command, the ranges from 1 to 65535 so o is an invalid number -> A is correct but B is not correct.

Question 9

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

RouterD# show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	192.160.5.3	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

A. 10.1.1.2
B. 10.154.154.1
C. 172.16.5.1
D. 192.168.5.316

Answer: C

Explanation

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

Question 10

What is the default administrative distance of OSPF?
A. 120
B. 100
C. 90
D. 110

Answer: D

CCNA – OSPF Questions 2

Note: If you are not sure about OSPF, please read our OSPF Tutorial.

Question 1

Why R1 can't establish an OSPF neighbor relationship with R3 according to the following graphic? (Choose two)

A – Configure EIGRP on these routers with a lower administrative distance
B – All routers should be configured for backbone Area 1
C – R1 and R3 have been configured in different areas
D – The hello and dead interval timers are not configured the same values on R1 and R3

Answer: C D

Explanation

A is not correct because configure EIGRP on these routers (with a lower administrative distance) will force these routers to run EIGRP, not OSPF.

B is not correct because the backbone area of OSPF is always Area 0.

C and D are correct because these entries must match on neighboring routers:

– **Hello and dead intervals**
– **Area ID** (Area 0 in this case)
– Authentication password
– Stub area flag

Question 2

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

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

Answer: B

Explanation

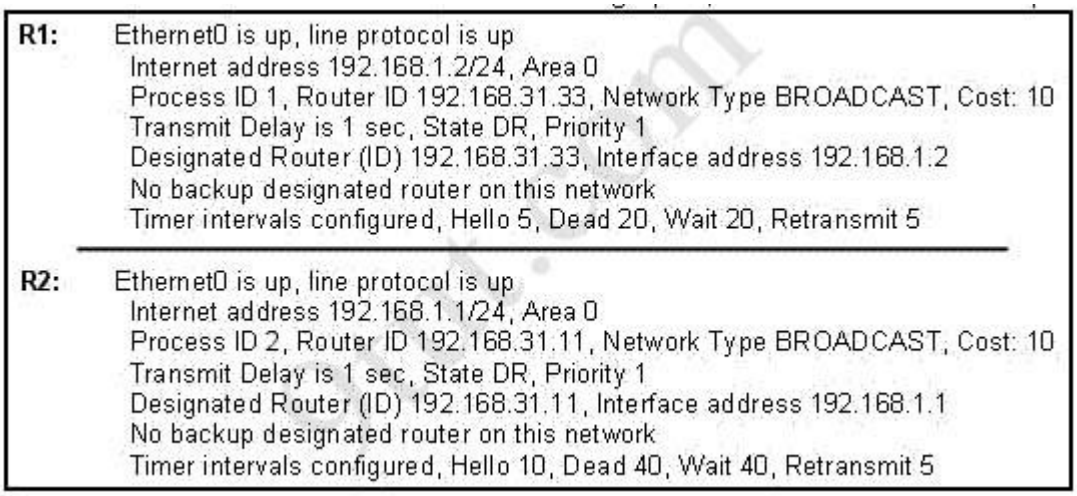
The well-known formula to calculate OSPF cost is

Cost = 10^8 / Bandwidth

so B is the correct answer.

Question 3

A network administrator is troubleshooting the OSPF configuration of routers R1 and R2. The routers cannot establish an adjacency relationship on their common Ethernet link. The graphic shows the output of the show ip ospf interface e0 command for routers R1 and R2. Based on the information in the graphic, what is the cause of this problem?



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

Answer: D

Explanation

D is correct because these entries must match on neighboring routers:

– **Hello and dead intervals**
– **Area ID** (Area 0 in this case)
– Authentication password
– Stub area flag

In this case Ethernet0 of R1 has Hello and Dead Intervals of 5 and 20 while R2 has Hello and Dead Intervals of 10 and 40 -> R1 and R2 cannot form OSPF neighbor relationship.

Question 4

What information does a router running a link-state protocol use to build and maintain its topological database? (Choose two)

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

Answer: A C

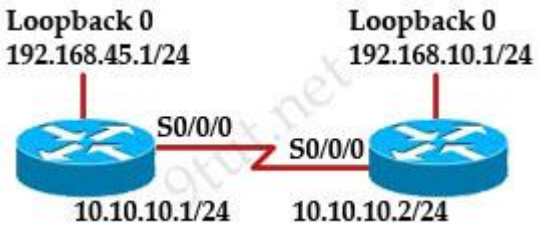
Question 5

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

Question 6

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

Answer: B

Explanation

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

Question 7

Which is true about OSPF router-id? (Choose two)

A. It is used for type 1 router LSA
B. Highest IP address of the loopback is used
C. router-id needs to be matched on ospf neighbors
D. router-id is 16 bit

Answer: A B

Explanation

OSPF LSA Type 1 (or Router LSA) is generated by all routers in an area to describe their directly attached links. An example below shows this type of LSA:

OSPF Router with ID (1.1.1.1) (Process ID 1)

Router Link States (Area 12)

Link ID	ADV Router	Age	Seq#	Checksum	Link count
1.1.1.1	1.1.1.1	115	0x80000002	0x002233	4
2.2.2.2	2.2.2.2	116	0x80000002	0x00A3AB	3

Summary Net Link States (Area 12)

Link ID	ADV Router	Age	Seq#	Checksum
10.1.1.4	2.2.2.2	122	0x80000001	0x00FBEB
10.1.1.8	2.2.2.2	113	0x80000001	0x00564D
10.1.2.64	2.2.2.2	113	0x80000001	0x00F7CD
10.1.10.3	2.2.2.2	113	0x80000001	0x00BE1D

As you can see, the LSA Type 1 uses the router ID to advertise itself (1.1.1.1 or 2.2.2.2).

The Router ID (RID) is an IP address used to identify the router and is chosen using the following sequence:
+ The highest IP address assigned to a loopback (logical) interface.
+ If a loopback interface is not defined, the highest IP address of all active router's physical interfaces will be chosen.
+ The router ID can be manually assigned

Question 8

Which two statements about the OSPF Router ID are true? (Choose two)

A. It identifies the source of Type 1 LSA
B. It should be the same on all routers in an OSPF routing instance
C. By default, the lowest IP address on the router becomes the OSPF router ID
D. The router automatically chooses the IP address of a loopback as the OSPF Router ID
E. It is created using the MAC Address of the loopback interface

Answer: A D

Explanation

From the output of the "show ip ospf database":

OSPF Router with ID (1.1.1.1) (Process ID 1)

Router Link States (Area 12)

Link ID	ADV Router	Age	Seq#	Checksum	Link count
1.1.1.1	1.1.1.1	115	0x80000002	0x002233	4
2.2.2.2	2.2.2.2	116	0x80000002	0x00A3AB	3

Summary Net Link States (Area 12)

Link ID	ADV Router	Age	Seq#	Checksum
10.1.1.4	2.2.2.2	122	0x80000001	0x00FBEB
10.1.1.8	2.2.2.2	113	0x80000001	0x00564D
10.1.2.64	2.2.2.2	113	0x80000001	0x00F7CD
10.1.10.3	2.2.2.2	113	0x80000001	0x00BE1D

We can see OSPF Router ID will be used as source of Type 1 LSA (1.1.1.1 & 2.2.2.2). Also the router will chose the highest loopback interface as its OSPF router ID (if available).

Question 9

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

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

Answer: B C

Question 10

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

The ‘network … area …’ command under OSPF process has the following meaning: It searches all the active interfaces, if the IP address of that interface belong to the ‘network …’ configured under OSPF process then the router will run OSPF on that interface. Therefore when we configure ‘network 0.0.0.0 255.255.255.255 area 0′ command, all interfaces are matched -> OSPF is enabled on all active interfaces on the router.

CCNA – EIGRP Questions

Note: If you are not sure about EIGRP, please read our EIGRP Tutorial.

Question 1

A network administrator is troubleshooting an EIGRP problem on a router and needs to confirm the IP addresses of the devices with which the router has established adjacency. The retransmit interval and the queue counts for the adjacent routers also need to be checked. What command will display the required information?

A. Router# show ip eigrp adjacency

B. Router# show ip eigrp topology

C. Router#show ip eigrp interfaces

D. Router#show ip eigrp neighbors

Answer: D

Explanation

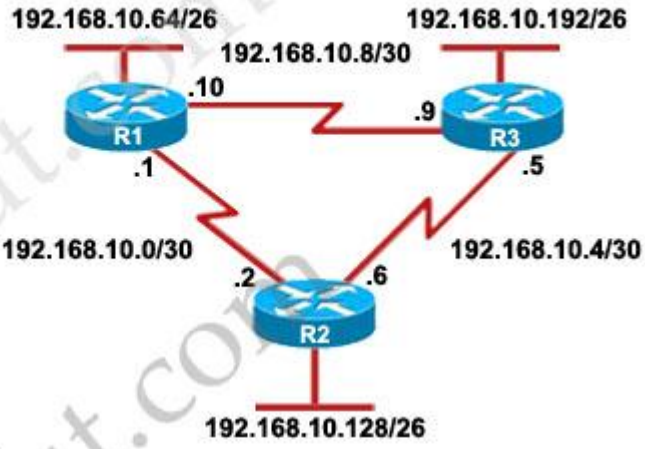
Below is an example of the **show ip eigrp neighbors** command. The retransmit interval (Smooth Round Trip Timer – SRTT) and the queue counts (Q count, which shows the number of queued EIGRP packets) for the adjacent routers are listed:

Router1# show ip eigrp neighbors

Address	Interface	Holdtime (secs)	Uptime (h:m:s)	Q Count	Seq Num	SRTT (ms)	RTO (ms)
192.168.1.2	Se0	13	01:10:20	106	636	0	30

Question 2

Refer to the exhibit. Based on the exhibited routing table, how will packets from a host within the 192.168.10.192/26 LAN be forwarded to 192.168.10.1?




```
R3# show ip route
Gateway of last resort is not set
    192.168.10.0/24 is variably subnetted, 6 subnets, 2 masks
D       192.168.10.64/26  [90/2195456] via 192.168.10.9, 00:03:31, Serial0/0
D       192.168.10.0/30  [90/2681856] via 192.168.10.9, 00:03:31, Serial0/0
                         [90/2681856] via 192.168.10.5, 00:03:31, Serial0/1
C       192.168.10.4/30 is directly connected, Serial0/1
C       192.168.10.8/30 is directly connected, Serial0/0
C       192.168.10.192/30 is directly connected, FastEthernet0/0
C       192.168.10.128/26 [90/2195456] via 192.168.10.5, 00:03:31, Serial0/1
```

A. The router will forward packets from R3 to R2 to R1

B. The router will forward packets from R3 to R1

C. The router will forward packets from R3 to R1 to R2

D. The router will forward packets from R3 to R2 to R1 AND from R3 to R1

Answer: D

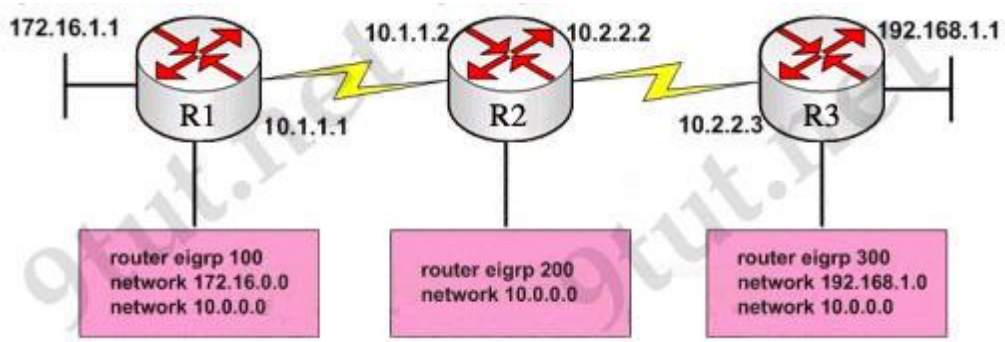
Explanation

From the routing table we learn that network 192.168.10.0/30 is learned via 2 equal-cost paths (192.168.10.9 &192.168.10.5) -> traffic to this network will be load-balancing.

Note: There is a typo in this question because R3 lists the its own IP addresses to 192.168.10.0/30. and 192.168.10.128/26 as the next-hop IP addresses. However we have to choose the best answers based on our understanding even the question output is wrong.

Question 3

Refer to the exhibit, when running EIGRP what is required for R1 to exchange routing updates with R3?



A – AS numbers must be changed to match on all the routers

B – Loopback interfaces must be configured so a DR is elected

C – The no auto-summary command is needed on R1 and R3

D – R2 needs to have two network statements, one for each connected network

Answer: A

Question 4

Which type of EIGRP route entry describes a feasible successor?

A. a primary route,stored in the routing table

B. a backup route,stored in the routing table

C. a backup route,stored in the topology table

D. a primary route,stored in the topology table

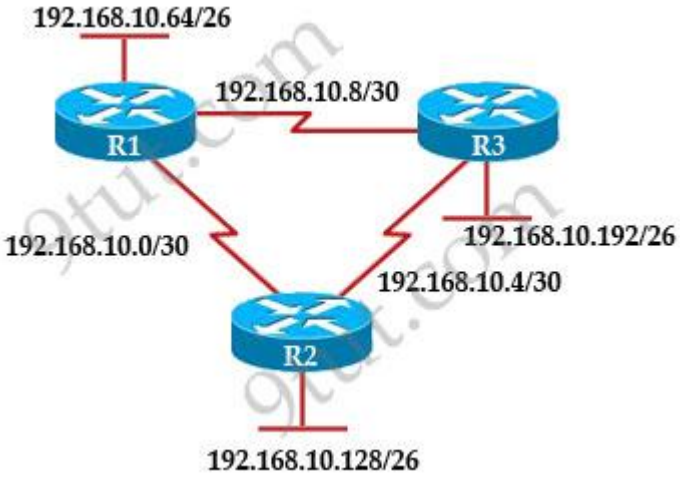
Answer: C

Explanation

Feasible successor is a route whose Advertised Distance is less than the Feasible Distance of the current best path. A feasible successor is a backup route, which is not stored in the routing table but stored in the topology table.

Question 5

Refer to the exhibit. The company uses EIGRP as the routing protocol. What path will packets take from a host on 192.168.10.192/26 network to a host on the LAN attached to router R1?



R3# show ip route

Gateway of last resort is not set

192 168.10.0/24 is variably subnetted, 6 subnets, 2 masks

D 192.168.10.64/26 [90/2195456] via 192.168.10.9, 00:03:31, Serial0/0

D 192.168.10.0/30 [90/2681856] via 192.168.10.9, 00:03:31, Serial0/0

C 192.168.10.4/30 is directly connected, Serial0/1

C 192.168.10.8/30 is directly connected, Serial0/0

C 192.168.10.192/26 is directly connected, FastEthernet0/0

D 192.168.10.128/26 [90/2195456] via 192.168.10.5,00:03:31, Serial0/1

A. The path of the packets will be R3 to R2 to R1.

B. The path of the packets will be R3 to R1 to R2.

C. The path of the packets will be both R3 to R2 to R1 and R3 to R1.

D. The path of the packets will be R3 to R1

Answer: D

Explanation

Host on the LAN attached to router R1 belongs to 192.168.10.64/26 subnet. From the output of the routing table of R3 we learn this network can be reach via 192.168.10.9, which is an IP address in

192.168.10.8/30 network (the network between R1 & R3) -> packets destined for 192.168.10.64 will be routed from R3 -> R1 -> LAN on R1.

CCNA – DHCP Questions

Note: If you are not sure about DHCP, please read our DHCP tutorial.

Question 1

When a DHCP server is configured, which two IP addresses should never be assignable to hosts? (Choose two)

A. network or subnetwork IP address
B. broadcast address on the network
C. IP address leased to the LAN
D. IP address used by the interfaces
E. manually assigned address to the clients
F. designated IP address to the DHCP server

Answer: A B

Explanation

Network or subnetwork IP address (for example 11.0.0.0/8 or 13.1.0.0/16) and broadcast address (for example 23.2.1.255/24) should never be assignable to hosts. When try to assign these addresses to hosts, you will receive an error message saying that they can't be assignable.

Question 2

Which two tasks does the Dynamic Host Configuration Protocol perform? (Choose two)

A. Set the IP gateway to be used by the network.
B. Perform host discovery used DHCPDISCOVER message.
C. Configure IP address parameters from DHCP server to a host.
D. Provide an easy management of layer 3 devices.
E. Monitor IP performance using the DHCP server.
F. Assign and renew IP address from the default pool.

Answer: C F

Question 3

Refer to the exhibit. Which rule does the DHCP server use when there is an IP address conflict?

```
Router# show ip dhcp conflict
IP address      Detection method    Detection time
172.16.1.32     Ping                Feb 16 1998 12:28 PM
172.16.1.64     Gratuitous ARP      Feb 23 1998 08:12 AM
```

A. The address is removed from the pool until the conflict is resolved.
B. The address remains in the pool until the conflict is resolved.
C. Only the IP detected by Gratuitous ARP is removed from the pool.
D. Only the IP detected by Ping is removed from the pool.
E. The IP will be shown, even after the conflict is resolved.

Answer: A

Question 4

How does a DHCP server dynamically assign IP address to host?

A. Addresses are allocated after a negotiation between the server and the host to determine the length of the agreement.
B. Addresses are assigned for a fixed period of time. At the end of period, a new quest for an address must be made, and another address is then assigned.
C. Addresses are leased to host. A host will usually keep the same address by periodically contacting the DHCP sever to renew the lease.
D. Addresses are permanently assigned so that the host uses the same address at all times.

Answer: C

Question 5

Which statement is correct regarding the operation of DHCP?

A. A DHCP client uses a ping to detect address conflicts.
B. A DHCP server uses a gratuitous ARP to detect DHCP clients.
C. A DHCP client uses a gratuitous ARP to detect a DHCP server.
D. If an address conflict is detected, the address is removed from the pool and an administrator must resolve the conflict.
E. If an address conflict is detected, the address is removed from the pool for an amount of time configurable by the administrator.
F. If an address conflict is detected, the address is removed from the pool and will not be reused until the server is rebooted.

Answer: D

Explanation

An address conflict occurs when two hosts use the same IP address. During address assignment, DHCP checks for conflicts using ping and gratuitous ARP. If a conflict is detected, the address is removed from the pool. The address will not be assigned until the administrator resolves the conflict.

(Reference: http://www.cisco.com/en/US/docs/ios/12_1/iproute/configuration/guide/1cddhcp.html)

CCNA – HSRP VRRP GLBP

Note: If you are not sure about HSRP and GLBP, please read our HSRP tutorial and GLBP tutorial.

Question 1

Which one of these is a valid HSRP Virtual Mac Address?

A. 0000.0C07.AC01
B. 0000.5E00.0110
C. 0007.B400.1203
D. 0000.C007.0201

Answer: A

Explanation

With HSRP, two or more devices support a virtual router with a fictitious MAC address and unique IP address. There are two version of HSRP.

+ With HSRP version 1, the virtual router's MAC address is 0000.0c07.ACxx , in which xx is the HSRP group.
+ With HSRP version 2, the virtual MAC address if 0000.0C9F.Fxxx, in which xxx is the HSRP group.

Note: Another case is HSRP for IPv6, in which the MAC address range from 0005.73A0.0000 through 0005.73A0.0FFF.

-> A is correct.

(Good resource for HSRP: http://www.cisco.com/en/US/docs/switches/datacenter/sw/5_x/nx-os/unicast/configuration/guide/l3_hsrp.html)

Question 2

Which three statements about HSRP operation are true? (Choose three)

A. The virtual IP address and virtual MAC address are active on the HSRP Master router.
B. The HSRP default timers are a 3 second hello interval and a 10 second dead interval.

C. HSRP supports only clear-text authentication.
D. The HSRP virtual IP address must be on a different subnet than the routers' interfaces on the same LAN.
E. The HSRP virtual IP address must be the same as one of the router's interface addresses on the LAN.
F. HSRP supports up to 255 groups per interface, enabling an administrative form of load balancing.

Answer: A B F

Explanation

The virtual MAC address of HSRP version 1 is **0000.0C07.ACxx**, where **xx** is the HSRP group number in hexadecimal based on the respective interface. For example, HSRP group 10 uses the HSRP virtual MAC address of 0000.0C07.AC0A. HSRP version 2 uses a virtual MAC address of 0000.0C9F.F**XXX** (XXX: HSRP group in hexadecimal)

For more information about HSRP operation, please read our HSRP tutorial.

Question 3

Which statement describes VRRP object tracking?

A. It monitors traffic flow and link utilization.
B. It ensures the best VRRP router is the virtual router master for the group.
C. It causes traffic to dynamically move to higher bandwidth links
D. It thwarts man-in-the-middle attacks.

Answer: B

Explanation

Object tracking is the process of tracking the state of a configured object and uses that state to determine the priority of the VRRP router in a VRRP group -> B is correct.

(Reference: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/unicast/configuration/guide/l3_cli_nxos/l3_vrrp.html#wp1074871)

Note: Unlike HSRP which can track interface status directly, VRRP can only track interface status through a tracked object.

Question 4

In GLBP, which router will respond to client ARP requests?

A. The active virtual gateway will reply with one of four possible virtual MAC addresses.
B. All GLBP member routers will reply in round-robin fashion.

C. The active virtual gateway will reply with its own hardware MAC address.
D. The GLBP member routers will reply with one of four possible burned in hardware addresses.

Answer: A

Explanation

One disadvantage of HSRP and VRRP is that only one router is in use, other routers must wait for the primary to fail because they can be used. However, Gateway Load Balancing Protocol (GLBP) can use of up to four routers simultaneously. In GLBP, there is still only one virtual IP address but each router has a different virtual MAC address. First a GLBP group must elect an Active Virtual Gateway (AVG). The AVG is responsible for replying ARP requests from hosts/clients. It replies with different virtual MAC addresses that correspond to different routers (known as Active Virtual Forwarders – AVFs) so that clients can send traffic to different routers in that GLBP group (load sharing).

Question 5

In a GLBP network, who is responsible for the arp request?

A. AVF
B. AVG
C. Active Router
D. Standby Router

Answer: B

Question 6

What are three benefits of GLBP? (Choose three)

A. GLBP supports up to eight virtual forwarders per GLBP group.
B. GLBP supports clear text and MD5 password authentication between GLBP group members.
C. GLBP is an open source standardized protocol that can be used with multiple vendors.
D. GLBP supports up to 1024 virtual routers.
E. GLBP can load share traffic across a maximum of four routers.
F. GLBP elects two AVGs and two standby AVGs for redundancy.

Answer: B D E

CCNA – SNMP Questions

Note: If you are not sure about SNMP, please read our SNMP tutorial.

Question 1

Which three are the components of SNMP? (Choose three)

A. MIB
B. SNMP Manager
C. SysLog Server
D. SNMP Agent

Answer: A B D

Explanation

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network.
The SNMP framework has three parts:

+ An SNMP manager
+ An SNMP agent
+ A Management Information Base (MIB)

The SNMP manager is the system used to control and monitor the activities of network hosts using SNMP. The most common managing system is called a Network Management System (NMS). The term NMS can be applied to either a dedicated device used for network management, or the applications used on such a device. A variety of network management applications are available for use with SNMP. These features range from simple command-line applications to feature-rich graphical user interfaces (such as the CiscoWorks2000 line of products).

The SNMP agent is the software component within the managed device that maintains the data for the device and reports these data, as needed, to managing systems. The agent and MIB reside on the routing device (router, access server, or switch). To enable the SNMP agent on a Cisco routing device, you must define the relationship between the manager and the agent.

The Management Information Base (MIB) is a virtual information storage area for network management information, which consists of collections of managed objects.

(Reference:
http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf014.html#wp1017597)

Question 2

Which protocol can cause overload on a CPU of a managed device?

A. Netflow
B. WCCP
C. IP SLA
D. SNMP

Answer: D

Explanation

Sometimes, messages like this might appear in the router console:

%SNMP-3-CPUHOG: Processing [chars] of [chars]

They mean that the SNMP agent on the device has taken too much time to process a request.

You can determine the cause of high CPU use in a router by using the output of the **show process cpu** command.

Note: A managed device is a part of the network that requires some form of monitoring and management (routers, switches, servers, workstations, printers…).

(Reference: http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a00800948e6.shtml)

Question 3

What is the alert message generated by SNMP agents called ?

A. TRAP
B. INFORM
C. GET
D. SET

Answer: A B

Explanation

A TRAP is a SNMP message sent from one application to another (which is typically on a remote host). Their purpose is merely to notify the other application that something has happened, has been noticed, etc. The big problem with TRAPs is that they're unacknowledged so you don't actually know if the remote application received your oh-so-important message to it. SNMPv2 PDUs fixed this by introducing the notion of an INFORM, which is nothing more than an acknowledged TRAP.

Question 4

Which three features are added in SNMPv3 over SNMPv2?

A. Message Integrity
B. Compression
C. Authentication
D. Encryption
E. Error Detection

Answer: A C D

Explanation

Cisco IOS software supports the following versions of SNMP:

+ SNMPv1 – The Simple Network Management Protocol: A Full Internet Standard, defined in RFC 1157. (RFC 1157 replaces the earlier versions that were published as RFC 1067 and RFC 1098.) Security is based on community strings.

+ SNMPv2c – The community-string based Administrative Framework for SNMPv2. SNMPv2c (the "c" stands for "community") is an Experimental Internet Protocol defined in RFC 1901, RFC 1905, and RFC 1906. SNMPv2c is an update of the protocol operations and data types of SNMPv2p (SNMPv2 Classic), and uses the community-based security model of SNMPv1.

+ SNMPv3 – Version 3 of SNMP. SNMPv3 is an interoperable standards-based protocol defined in RFCs 2273 to 2275. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network. The security features provided in SNMPv3 are as follows:

– Message integrity: Ensuring that a packet has not been tampered with in transit.
– Authentication: Determining that the message is from a valid source.
– Encryption: Scrambling the contents of a packet prevent it from being learned by an unauthorized source.

(Reference: http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf014.html#wp1010901)

Question 5

What is SNMPv3 authentication protocol?

Answer: HMAC-MD5 or HMAC-SHA (Maybe either of them will appear in the exam)

Question 6

Which three statements about the features of SNMPv2 and SNMPv3 are true? (Choose three)

A. SNMPv3 enhanced SNMPv2 security features
B. SNMPv3 added the Inform protocol message to SNMP.
C. SNMPv2 added the Inform protocol message to SNMP.
D. SNMPv3 added the GetBulk protocol messages to SNMP.

E. SNMPv2 added the GetBulk protocol message to SNMP.
F. SNMPv2 added the GetNext protocol message to SNMP.

Answer: A C E

Explanation

SNMPv1/v2 can neither authenticate the source of a management message nor provide encryption. Without authentication, it is possible for nonauthorized users to exercise SNMP network management functions. It is also possible for nonauthorized users to eavesdrop on management information as it passes from managed systems to the management system. Because of these deficiencies, many SNMPv1/v2 implementations are limited to simply a read-only capability, reducing their utility to that of a network monitor; no network control applications can be supported. To correct the security deficiencies of SNMPv1/v2, SNMPv3 was issued as a set of Proposed Standards in January 1998. -> A is correct.

(Reference: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_1-3/snmpv3.html)

The two additional messages are added in SNMP2 (compared to SNMPv1)

GetBulkRequest The GetBulkRequest message enables an SNMP manager to access large chunks of data. GetBulkRequest allows an agent to respond with as much information as will fit in the response PDU. Agents that cannot provide values for all variables in a list will send partial information. -> E is correct.

InformRequest The InformRequest message allows NMS stations to share trap information. (Traps are issued by SNMP agents when a device change occurs.) InformRequest messages are generally used between NMS stations, not between NMS stations and agents. -> C is correct.

Note: These two messages are carried over SNMPv3.

Question 7

What authentication type is used by SNMPv2?

A. HMAC-MD5
B. HMAC-SHA
C. CBC-DES
D. community strings

Answer: D

CCNA – NetFlow Questions

Question 1

What are the benefit of using Netflow? (Choose three)

A. Network, Application & User Monitoring
B. Network Planning
C. Security Analysis
D. Accounting/Billing

Answer: A C D

Explanation

NetFlow traditionally enables several key customer applications including:

+ **Network Monitoring** – NetFlow data enables extensive near real time network monitoring capabilities. Flow-based analysis techniques may be utilized to visualize traffic patterns associated with individual routers and switches as well as on a network-wide basis (providing aggregate traffic or application based views) to provide proactive problem detection, efficient troubleshooting, and rapid problem resolution.

+ **Application Monitoring and Profiling** – NetFlow data enables network managers to gain a detailed, time-based, view of application usage over the network. This information is used to plan, understand new services, and allocate network and application resources (e.g. Web server sizing and VoIP deployment) to responsively meet customer demands.

+ **User Monitoring and Profiling** – NetFlow data enables network engineers to gain detailed understanding of customer/user utilization of network and application resources. This information may then be utilized to efficiently plan and allocate access, backbone and application resources as well as to detect and resolve potential security and policy violations.

+ **Network Planning** – NetFlow can be used to capture data over a long period of time producing the opportunity to track and anticipate network growth and plan upgrades to increase the number of routing devices, ports, or higher- bandwidth interfaces. NetFlow services data optimizes network planning including peering, backbone upgrade planning, and routing policy planning. NetFlow helps to minimize the total cost of network operations while maximizing network performance, capacity, and reliability. NetFlow detects unwanted WAN traffic, validates bandwidth and Quality of Service (QOS) and allows the analysis of new network applications. NetFlow will give you valuable information to reduce the cost of operating your network.

+ **Security Analysis** – NetFlow identifies and classifies DDOS attacks, viruses and worms in real-time. Changes in network behavior indicate anomalies that are clearly demonstrated in NetFlow data. The data is also a valuable forensic tool to understand and replay the history of security incidents.

+ **Accounting/Billing** – NetFlow data provides fine-grained metering (e.g. flow data includes details such as IP addresses, packet and byte counts, timestamps, type-of-service and application ports, etc.) for highly flexible and detailed resource utilization accounting. Service providers may utilize the information for billing based on time-of-day, bandwidth usage, application usage, quality of service, etc. Enterprise customers may utilize the information for departmental charge-back or cost allocation for resource utilization.

(Reference: http://www.cisco.com/en/US/products/sw/netmgtsw/ps1964/products_implementation_design_guide09186a00800d6a11.html#wp1030045)

Question 2

What are the three things that the NetFlow uses to consider the traffic to be in a same flow?

A. IP address
B. Interface name
C. Port numbers
D. L3 protocol type
E. MAC address

Answer: A C D

Explanation

What is an IP Flow?
Each packet that is forwarded within a router or switch is examined for a set of IP packet attributes. These attributes are the IP packet identity or fingerprint of the packet and determine if the packet is unique or similar to other packets.
Traditionally, an IP Flow is based on a set of 5 and up to 7 IP packet attributes.
IP Packet attributes used by NetFlow:
+ **IP source address**
+ **IP destination address**
+ **Source port**
+ **Destination port**
+ **Layer 3 protocol type**
+ Class of Service
+ Router or switch interface

(Reference: http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html)

Question 3

What NetFlow component can be applied to an interface to track IPv4 traffic?

A. flow monitor
B. flow record

C. flow sampler
D. flow exporter

Answer: A

Explanation

Flow monitors are the Flexible NetFlow component that is applied to interfaces to perform network traffic monitoring. Flow monitors consist of a record and a cache. You add the record to the flow monitor after you create the flow monitor. The flow monitor cache is automatically created at the time the flow monitor is applied to the first interface. Flow data is collected from the network traffic during the monitoring process based on the key and nonkey fields in the record, which is configured for the flow monitor and stored in the flow monitor cache.
For example, the following example creates a flow monitor named FLOW-MONITOR-1 and enters Flexible NetFlow flow monitor configuration mode:
Router(config)# flow monitor FLOW-MONITOR-1
Router(config-flow-monitor)#

(Reference: http://www.cisco.com/c/en/us/td/docs/ios/fnetflow/command/reference/fnf_book/fnf_01.html#wp1314030)

Question 4

What command visualizes the general NetFlow data on the command line?

A. show ip flow export
B. show ip flow top-talkers
C. show ip cache flow
D. show mls sampling
E. show mls netflow ip

Answer: C

Explanation

The “show ip cache flow” command displays a summary of the NetFlow accounting statistics.

```
GATEWAY#show ip cache flow
IP packet size distribution (1149 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .134 .475 .100 .010 .006 .037 .043 .005 .001 .004 .001 .002 .001 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .003 .000 .001 .020 .147 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  13 active, 4083 inactive, 378 added
  7046 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  13 active, 1011 inactive, 378 added, 378 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-WWW             32      0.0         8   989      0.1       3.8       8.1
TCP-other           24      0.0         2    57      0.0       2.2      14.4
UDP-other          309      0.1         2   105      0.3       2.4      15.4
Total:             365      0.1         3   318      0.4       2.5      14.7

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Fa0/0         10.0.0.23       Null          10.255.255.255  11 0089 0089     9
Fa0/0         10.0.0.30       Null          10.255.255.255  11 008A 008A     1
```

Question 5

What are three reasons to collect NetFlow data on a company network? (Choose three)

A. To identify applications causing congestion.
B. To authorize user network access.
C. To report and alert link up / down instances.
D. To diagnose slow network performance, bandwidth hogs, and bandwidth utilization.
E. To detect suboptimal routing in the network.
F. To confirm the appropriate amount of bandwidth that has been allocated to each Class of Service.

Answer: A D F

Explanation

NetFlow facilitates solutions to many common problems encountered by IT professionals.
+ **Analyze new applications and their network impact**
Identify new application network loads such as VoIP or remote site additions.
+ **Reduction in peak WAN traffic**
Use NetFlow statistics to measure WAN traffic improvement from application-policy changes; understand who is utilizing the network and the network top talkers.
+ **Troubleshooting and understanding network pain points**

Diagnose slow network performance, bandwidth hogs and bandwidth utilization quickly with command line interface or reporting tools. -> D is correct.
+ **Detection of unauthorized WAN traffic**
Avoid costly upgrades by identifying the applications causing congestion. -> A is correct.
+ **Security and anomaly detection**
NetFlow can be used for anomaly detection and worm diagnosis along with applications such as Cisco CS-Mars.
+ **Validation of QoS parameters**
Confirm that appropriate bandwidth has been allocated to each Class of Service (CoS) and that no CoS is over- or under-subscribed.-> F is correct.

(Reference: http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html)

Question 6

What are three factors a network administrator must consider before implementing Netflow in the network? (Choose three)

A. CPU utilization
B. where Netflow data will be sent
C. number of devices exporting Netflow data
D. port availability
E. SNMP version
F. WAN encapsulation

Answer: A B C

Question 7

What Cisco IOS feature can be enabled to pinpoint an application that is causing slow network performance?

A. SNMP
B. Netflow
C. WCCP
D. IP SLA

Answer: B

CCNA – Syslog Questions

If you are not sure about Syslog, please read our Syslog tutorial.

Question 1

What are the popular destinations for Syslog messages to be saved?

A. Flash
B. The logging buffer RAM
C. The console terminal
D. Other terminals
E. Syslog server

Answer: B C E

Explanation

By default, switches send the output from system messages and debug privileged EXEC commands to a logging process. The logging process controls the distribution of logging messages to various destinations, such as the **logging buffer** (on RAM), **terminal lines** (console terminal), or a UNIX **syslog server**, depending on your configuration. The process also sends messages to the console.

(Reference: http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_9_ea1/configuration/guide/swlog.html#wp1024032)

Note: Syslog messages can be written to a file in Flash memory although it is not a popular place to use. We can configure this feature with the command **logging file flash:*filename***.

Question 2

Syslog was configured with a level 3 trap. Which 3 types of logs would be generated (choose four)

A. Emergencies
B. Alerts
C. Errors
D. Warnings
E. Critical

Answer: A B C E

Explanation

The Message Logging is divided into 8 levels as listed below:

Level	Keyword	Description
0	emergencies	System is unusable
1	alerts	Immediate action is needed
2	critical	Critical conditions exist
3	errors	Error conditions exist
4	warnings	Warning conditions exist
5	notification	Normal, but significant, conditions exist
6	informational	Informational messages
7	debugging	Debugging messages

The highest level is level 0 (emergencies). The lowest level is level 7. If you specify a level with the "logging console *level*" command, that level and all the higher levels will be displayed. For example, by using the "logging console warnings" command, all the logging of emergencies, alerts, critical, errors, warnings will be displayed.

In this question level 3 trap is configured so Emergencies, Alerts, critical and Errors messages are displayed. Although this question only requires to choose 3 correct answers but maybe something is missing here.

Question 3

Which three statements about Syslog utilization are true? (Choose three)

A. Utilizing Syslog improves network performance.
B. The Syslog server automatically notifies the network administrator of network problems.
C. A Syslog server provides the storage space necessary to store log files without using router disk space.
D. There are more Syslog messages available within Cisco IOS than there are comparable SNMP trap messages.
E. Enabling Syslog on a router automatically enables NTP for accurate time stamping.
F. A Syslog server helps in aggregation of logs and alerts.

Answer: C D F

Question 4

What command instructs the device to timestamp Syslog debug messages in milliseconds?

A. service timestamps log datetime localtime
B. service timestamps debug datetime msec
C. service timestamps debug datetime localtime
D. service timestamps log datetime msec

Answer: B

Explanation

The "service timestamps debug" command configures the system to apply a time stamp to debugging messages. The time-stamp format for **datetime** is **MMM DD HH:MM:SS**, where **MMM** is the month, **DD** is the date, **HH** is the hour (in 24-hour notation), **MM** is the minute, and **SS** is the second. With the additional keyword **msec**, the system includes milliseconds in the time stamp, in the format HH:DD:MM:SS.mmm, where .mmm is milliseconds

(Reference: http://www.cisco.com/c/en/us/td/docs/ios/fundamentals/command/reference/cf_book/cf_r1.html#wp1030116)

Question 5

What is the default Syslog facility level?

A. local4
B. local5
C. local6
D. local7

Answer: D

Question 6

What levels will be trapped if the administrator executes the command

router(config)# logging trap 4

A. Emergency
B. Notice
C. Alert
D. Error
E. Warning

Answer: A C D E

Explanation

The Message Logging is divided into 8 levels as listed below:

Level	Keyword	Description
0	emergencies	System is unusable
1	alerts	Immediate action is needed
2	critical	Critical conditions exist
3	errors	Error conditions exist
4	warnings	Warning conditions exist
5	notification	Normal, but significant, conditions exist
6	informational	Informational messages
7	debugging	Debugging messages

If you specify a level with the "logging *trap level*" command, that level and all the higher levels will be logged. For example, by using the "logging trap 4″ command, all the logging of emergencies, alerts, critical, errors, warnings will be logged.

Question 7

A network administrator enters the following command on a router: logging trap 3. What are three message types that will be sent to the Syslog server? (Choose three)

A. informational
B. emergency
C. warning
D. critical
E. debug
F. error

Answer: B D F

CCNA – Security Questions

Question 1

Which Cisco Catalyst feature automatically disables the port in an operational PortFast upon receipt of a BPDU?

A. BackboneFast
B. UplinkFast
C. Root Guard
D. BPDU Guard
E. BPDU Filter

Answer: D

Explanation

We only enable PortFast feature on access ports (ports connected to end stations). But if someone does not know he can accidentally plug that port to another switch and a loop may occur when BPDUs are being transmitted and received on these ports.

With BPDU Guard, when a PortFast receives a BPDU, it will be shut down to prevent a loop -> D is correct.

Question 2

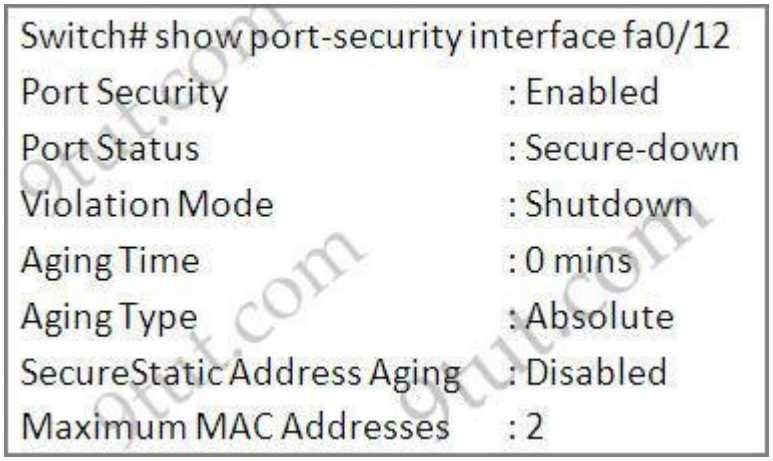
Which two commands correctly verily whether port security has been configured on port FastEthernet 0/12 on a switch? (Choose two)

A. SW1# show switchport port-security interface FastEthernet 0/12
B. SW1# show switchport port-secure interface FastEthernet 0/12
C. SW1# show port-security interface FastEthernet 0/12
D. SW1# show running-config

Answer: C D

Explanation

We can verify whether port security has been configured by using the “show running-config” or “show port-security interface ” for more detail. An example of the output of “show port-security interface ” command is shown below:



Question 3

Select the action that results from executing these commands:

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

A. A dynamically learned MAC address is saved in the startup-configuration file.
B. A dynamically learned MAC address is saved in the running-configuration file.
C. A dynamically learned MAC address is saved in the VLAN database.
D. Statically configured MAC addresses are saved in the startup-configuration file if frames from that address are received.
E. Statically configured MAC addresses are saved in the running-configuration file if frames from that address are received.

Answer: B

Explanation

The full syntax of the second command is:

switchport port-security mac-address sticky [MAC]

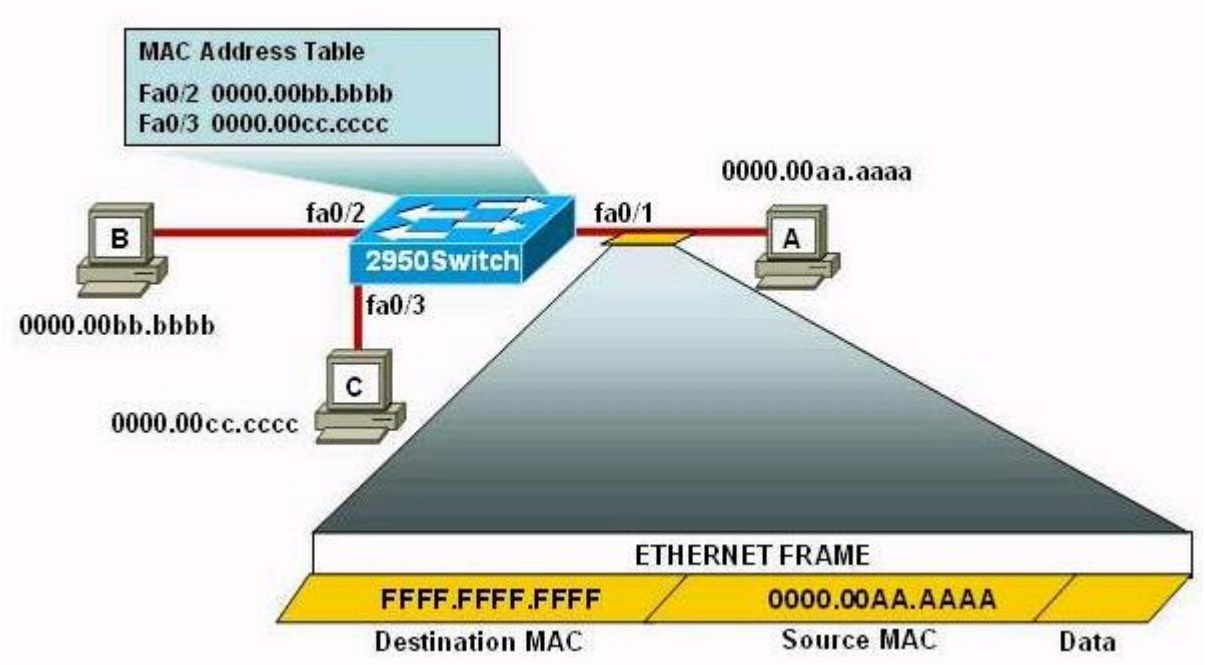
If we don't specify the MAC address (like in this question) then the switch will dynamically learn the attached MAC Address and place it into your running-configuration -> B is correct.

Question 4

Refer to the exhibit. The following commands are executed on interface fa0/1 of 2950Switch.

2950Switch(config-if)#switchport port-security
2950Switch(config-if)#switchport port-security mac-address sticky
2950Switch(config-if)#switchport port-security maximum 1

The Ethernet frame that is shown arrives on interface fa0/1. What two functions will occur when this frame is received by 2950Switch? (Choose two)



A. The MAC address table will now have an additional entry of fa0/1 FFFF.FFFF.FFFF.
B. Only host A will be allowed to transmit frames on fa0/1.
C. This frame will be discarded when it is received by 2950Switch.
D. All frames arriving on 2950Switch with a destination of 0000.00aa.aaaa will be forwarded out fa0/1.
E. Hosts B and C may forward frames out fa0/1 but frames arriving from other switches will not be forwarded out fa0/1.
F. Only frames from source 0000.00bb.bbbb, the first learned MAC address of 2950Switch, will be forwarded out fa0/1.

Answer: B D

Explanation

Please read the **Explanation** at http://www.9tut.net/icnd2/icnd2-operations

Question 5

Which set of commands is recommended to prevent the use of a hub in the access layer?

A.
switch(config-if)#switchport mode trunk
switch(config-if)#switchport port-security maximum 1

B.
switch(config-if)#switchport mode trunk
switch(config-if)#switchport port-security mac-address 1

C.
switch(config-if)#switchport mode access
switch(config-if)#switchport port-security maximum 1

D.
switch(config-if)#switchport mode access
switch(config-if)#switchport port-security mac-address 1

Answer: C

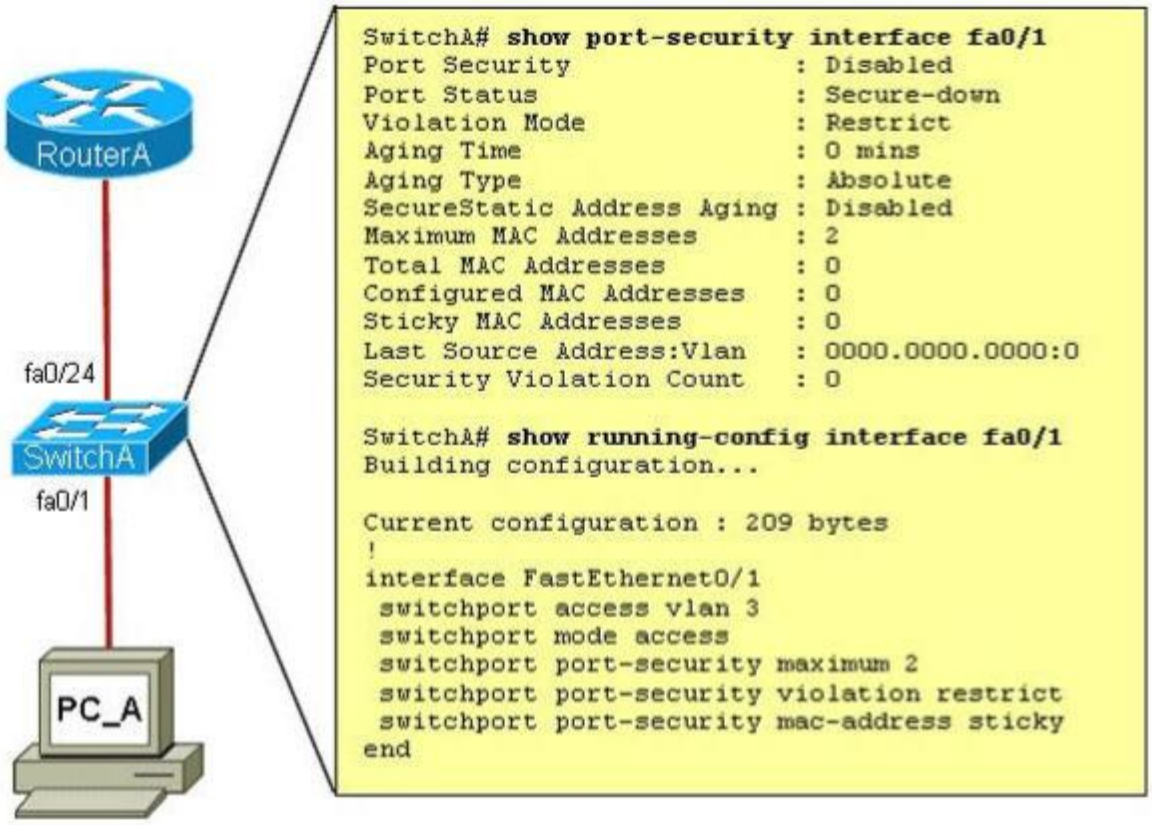
Explanation

Port security is only used on access port (which connects to hosts) so we need to set that port to "access" mode, then we need to specify the maximum number of hosts which are allowed to connect to this port -> C is correct.

Note: If we want to allow a fixed MAC address to connect, use the "switchport port-security mac-address " command.

Question 6

Refer to the exhibit. A junior network administrator was given the task of configuring port security on SwitchA to allow only PC_A to access the switched network through port fa0/1. If any other device is detected, the port is to drop frames from this device. The administrator configured the interface and tested it with successful pings from PC_A to RouterA, and then observes the output from these two show commands.



Which two of these changes are necessary for SwitchA to meet the requirements? (Choose two)

A. Port security needs to be globally enabled.
B. Port security needs to be enabled on the interface.
C. Port security needs to be configured to shut down the interface in the event of a violation.
D. Port security needs to be configured to allow only one learned MAC address.
E. Port security interface counters need to be cleared before using the show command.
F. The port security configuration needs to be saved to NVRAM before it can become active.

Answer: B D

Explanation

As we see in the output, the “Port Security” is in “Disabled” state (line 2 in the output). To enable Port security feature, we must enable it on that interface first with the command:

SwitchA(config-if)#switchport port-security

-> B is correct.

Also from the output, we learn that the switch is allowing 2 devices to connect to it (switchport port-security maximum 2) but the question requires allowing only PC_A to access the network so we need to reduce the maximum number to 1 -> D is correct.

Question 7

A network administrator needs to configure port security on a switch. Which two statements are true? (Choose two)

A. The network administrator can apply port security to dynamic access ports
B. The network administrator can configure static secure or sticky secure mac addresses in the voice vlan.
C. The sticky learning feature allows the addition of dynamically learned addresses to the running configuration.
D. The network administrator can apply port security to EtherChannels.
E. When dynamic mac address learning is enabled on an interface, the switch can learn new addresses up to the maximum defined.

Answer: C E

Explanation

Follow these guidelines when configuring port security:
+ **Port security can only be configured on static access ports, trunk ports, or 802.1Q tunnel ports**. -> A is not correct.
+ A secure port cannot be a dynamic access port.
+ A secure port cannot be a destination port for Switched Port Analyzer (SPAN).
+ A secure port cannot belong to a Fast EtherChannel or Gigabit EtherChannel port group. -> D is not correct
+ **You cannot configure static secure or sticky secure MAC addresses on a voice VLAN**. -> B is not correct.
+ When you enable port security on an interface that is also configured with a voice VLAN, you must set the maximum allowed secure addresses on the port to at least two.
+ If any type of port security is enabled on the access VLAN, dynamic port security is automatically enabled on the voice VLAN.
+ When a voice VLAN is configured on a secure port that is also configured as a sticky secure port, all addresses seen on the voice VLAN are learned as dynamic secure addresses, and all addresses seen on the access VLAN (to which the port belongs) are learned as sticky secure addresses.
+ The switch does not support port security aging of sticky secure MAC addresses.
+ The protect and restrict options cannot be simultaneously enabled on an interface.

(Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3550/software/release/12-1_19_ea1/configuration/guide/3550scg/swtrafc.html#wp1038546)

Note: Dynamic access port or Dynamic port VLAN membership must be connected to an end station. This type of port can be configured with the “switchport access vlan dynamic” command in the interface configuration mode. Please read more about Dynamic access port here: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3550/software/release/12-1_19_ea1/configuration/guide/3550scg/swvlan.html#wp1103064

Question 8

Which protocol is an open standard protocol framework that is commonly used in VPNs to provide secure end-to-end connections?

A. PPTP
B. IPsec
C. RSA
D. L2TP

Answer: B

Explanation

One of the most widely deployed network security technologies today is IPsec over VPNs. It provides high levels of security through encryption and authentication, protecting data from unauthorized access.

CCNA – Operation Questions

Question 1

Which command would you use on a Cisco router to verify the Layer 3 path to a host?
A. traced address
B. traceroute address
C. telnet address
D. ssh address

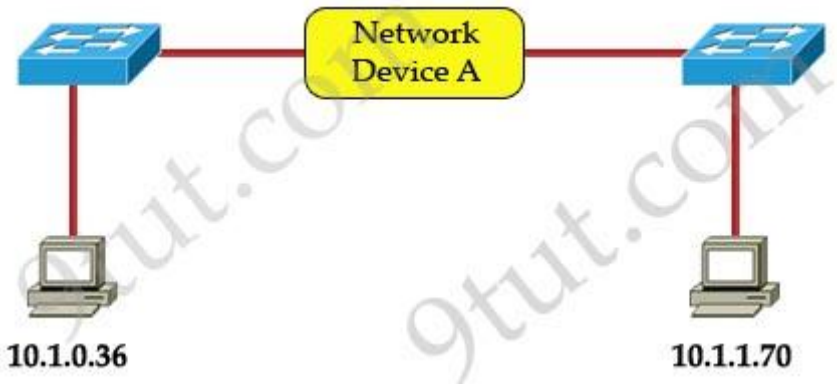
Answer: B

Explanation

To check the connectivity between a host and a destination (through some networks) we can use both “tracert” and “ping” commands. But the difference between these 2 commands is the “tracert” command can display a list of near-side router interfaces in the path between the source and the destination. The “traceroute” command has the same function of the “tracert” command but it is used on Cisco routers only, not on a PC -> B is correct.

Question 2

Refer to the exhibit:



Which three statements correctly describe Network Device A? (Choose three)

A. With a network wide mask of 255.255.255.128, each interface does not require an IP address.
B. With a network wide mask of 255.255.255.128, each interface does require an IP address on a unique IP subnet.
C. With a network wide mask of 255.255.255.0, must be a Layer 2 device for the PCs to communicate with each other.
D. With a network wide mask of 255.255.255.0, must be a Layer 3 device for the PCs to communicate with each other.
E. With a network wide mask of 255.255.254.0, each interface does not require an IP address.

Answer: B D E

Explanation

The principle here is if the subnet mask makes two IP addresses 10.1.0.36 and 10.1.1.70 in the same subnet then the Network device A does not need to have IP addresses on its interfaces (and we don't need a Layer 3 device here).

A quick way to find out the correct answers is notice that all 255.255.255.x subnet masks will separate these two IP addresses into two separate subnets so we need a Layer 3 device here and each interface must require an IP address on a unique IP subnet -> A, C are not correct while B, D are correct.

With 255.255.254.0 subnet mask, the increment here is 2 in the third octet -> the first subnet is from 10.1.0.0 to 10.1.1.255, in which two above IP addresses belong to -> each interface of Network device A does not require an IP address -> E is correct.

Question 3

What are three reasons that an organization with multiple branch offices and roaming users might implement a Cisco VPN solution instead of point-to-point WAN links? (Choose three)

A. reduced cost
B. better throughput
C. broadband incompatibility

D. increased security
E. scalability
F. reduced latency

Answer: A D E

Question 4

What two things will a router do when running a distance vector routing protocol? (Choose two)

A. Send periodic updates regardless of topology changes.
B. Send entire routing table to all routers in the routing domain.
C. Use the shortest-path algorithm to the determine best path.
D. Update the routing table based on updates from their neighbors.
E. Maintain the topology of the entire network in its database.

Answer: A D

Question 5

What is the purpose of the inverse ARP?

A. to map a known DLCI to an IP address
B. to map a known IP address to a MAC address
C. to map known SPID to a MACaddress
D. to map a known DLCI to a MAC address
E. to map a known IP address to a SPID.
F. to map a known MAC address to an IP address

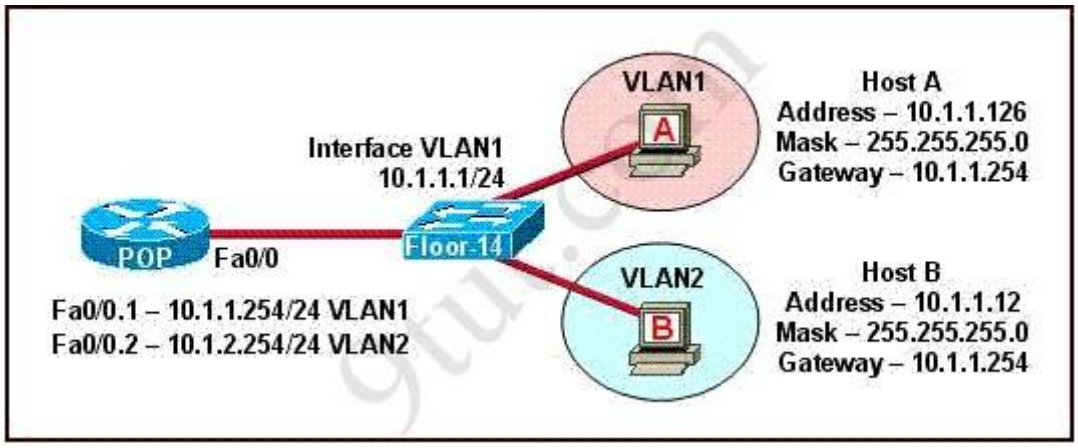
Answer: A

Explanation

For more information about Inverse ARP, please read my Frame Relay tutorial.

Question 6

The network shown in the diagram is experiencing connectivity problems. Which of the following will correct the problems? (Choose two.)



A. Configure the gateway on Host A as 10.1.1.1.
B. Configure the gateway on Host B as 10.1.2.254.
C. Configure the IP address of Host A as 10.1.2.2.
D. Configure the IP address of Host B as 10.1.2.2.
E. Configure the masks on both hosts to be 255.255.255.224.
F. Configure the masks on both hosts to be 255.255.255.240.

Answer: B D

Question 7

Refer to the exhibit. For what two reasons has the router loaded its IOS image from the location that is shown? (Choose two)

```
Router1> show version
Cisco Internetwork Operating System Software
IOS ™ 7200 Software (C7200-J-M), Experimental Version 11.3tl997091S:1647S2)
[hampton-nitro-baseline 249]
Copyright (c) 1986-1997 by cisco Systems, Inc.
Compiled Wed 08-0ct-97 06:39 by hampton
Image text-base: 0×60008900, data-base: 0x60B98000

ROM: System Bootstrap, Version 11.1(11855) [beta 2], INTERIM SOFTWARE
BOOTPLASH: 7200 Software (C7200-BOOT-M), Version 11.1(472), RELEASE SOFTWARE (fcl)

Router1 uptime is 23 hours, 33 minutes
System restarted by abort at PC 0x6022322C at 10:50:SS PDT Tue Oct 21 1997
System image file is "tftp://112.16.1.129/hampton/nitro/c7200-j-mz"

cisco 7206 (NPE150) processor with 57344K/8192K bytes of memory.



Configuration register is 0×2102
```

A. Router1 has specific boot system command that instruct it to load IOS from TFTP server.
B. Router1 is acting as a TFTP server for other routers.
C. Router1 cannot locate a valid IOS image in flash memory.
D. Router1 defaulted to ROMMON mode and loaded the IOS image from a TFTP server.
E. Cisco routers will first attempt to load a image from TFTP for management purposes.

Answer: A C

Explanation

When powered on, the router first checks its hardware via Power-On Self Test (POST). Then it checks the configuration register to identify where to load the IOS image from. In the output above we learn that the Configuration register value is 0×2102 so the router will try to boot the system image from Flash memory first.

But we also see a line "System image file is "tftp://112.16.1.129/hampton/nitro/c7200-j-mz". Please notice that this line tells us the image file that the device last started. In this case it is from a TFTP server. Therefore we can deduce that the router could not load the IOS image from the flash and the IOS image has been loaded from TFTP server.

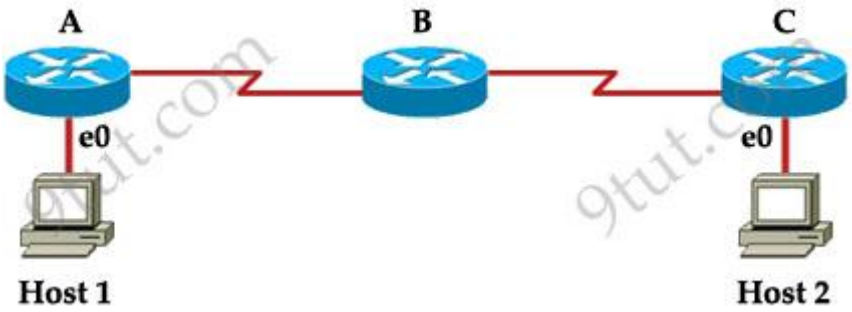
Note:

If the startup-config file is missing or does not specify a location, it will check the following locations for the IOS image:

+ Flash (the default location)
+ TFTP server
+ ROM (used if no other source is found)

Question 8

Host 1 is trying to communicate with Host 2. The e0 interface on Router C is down. Which of the following are true? (Choose two)



A. Router C will use ICMP to inform Host 1 that Host 2 cannot be reached.
B. Router C will use ICMP to inform Router B that Host 2 cannot be reached.
C. Router C will use ICMP to inform Host 1, Router A, and Router B that Host 2 cannot be reached.
D. Router C will send a Destination Unreachable message type.

E. Router C will send a Router Selection message type.
F. Router C will send a Source Quench message type.

Answer: A D

Explanation

The last known good router will try to inform you that the destination cannot be reached (with a Destination Unreachable message type) so from that information you can learn how far your packets can travel to and where the problem is.

Question 9

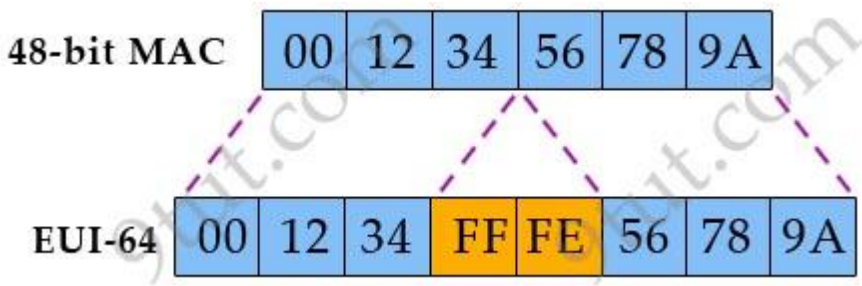
How is an EUI-64 format interface ID created from a 48-bit MAC address?

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

Answer: D

Explanation

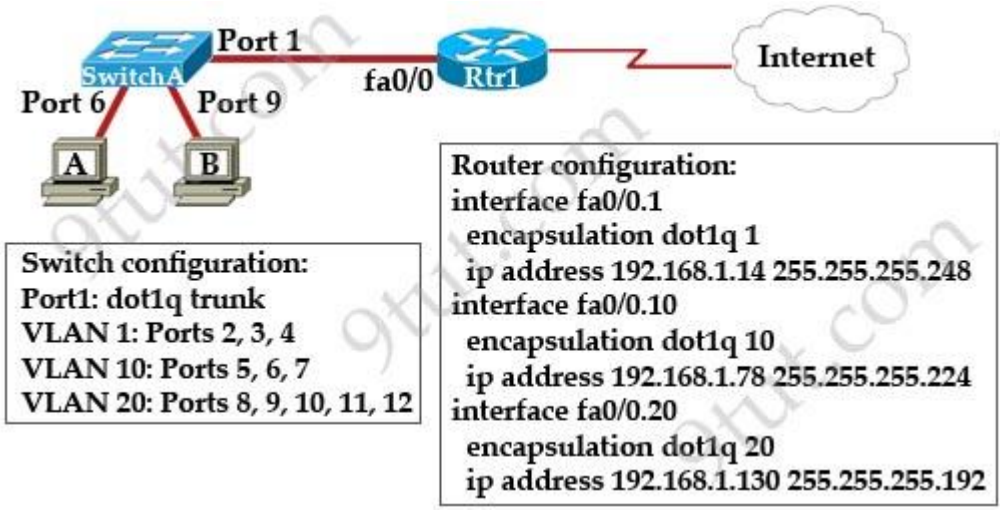
We convert a 48-bit MAC address (IEEE 802) to a 64-bit value by breaking the MAC address into its two 24-bit halves. The first part is the Organizationally Unique Identifier (OUI) and the next part is the NIC specific part. Then the 16-bit hex value 0xFFFE is inserted between them to create a 64-bit value.



Just for your information, to obtain an IPv6 interface identifier from EUI-64 address, we have to complement the U/L bit (the seventh bit of the first byte and is used to determine whether the address is universally or locally administered). This means if it is a 1, it is set to 0; and if it is a 0, it is set to 1. In the above example, the U/L bit is 0 (from 00 = 0000 00**0**0). Therefore we have to set this bit to 1 to create an IPv6 interface address.

Question 10

Refer to the exhibit:



A network administrator is adding two new hosts to SwitchA. Which three values could be used for the configuration of these hosts? (Choose three)

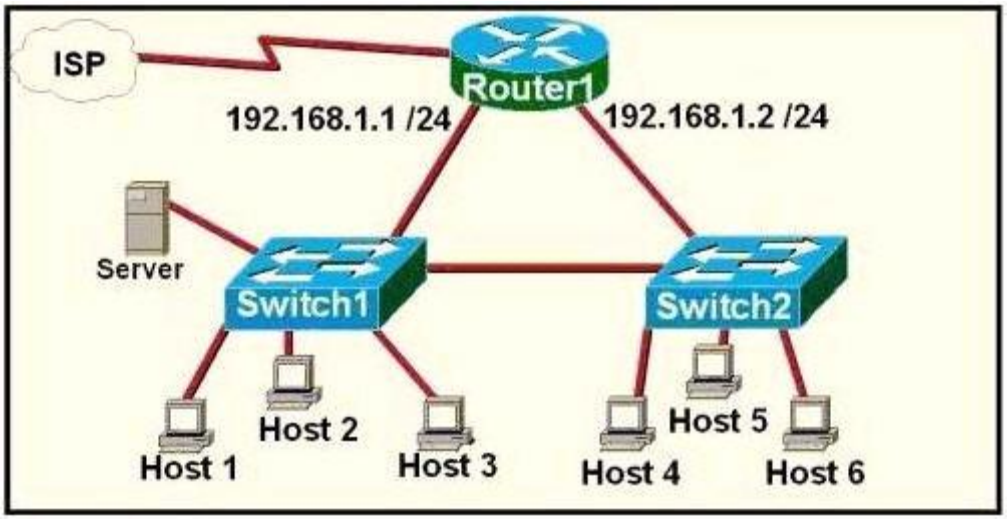
A. host A IP address: 192.168.1.79
B. host A IP address: 192.168.1.64
C. host A default gateway: 192.168.1.78
D. host B IP address: 192.168.1.128
E. host B default gateway: 192.168.1.129
F. host B IP address: 192.168.1.190

Answer: A C F

CCNA – Operation 2

Question 1

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. The 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

Each interface on a router must be in a different network. If two interfaces are in the same network, the router will not accept it and show error when the administrator assigns it.

Question 2

Refer to the exhibit. What can be determined about the router from the console output?

```
1 FastEthernet/IEEE 802.3 interface(s)
125K bytes of non-volatile configuration memory.
65536K bytes of ATA PCMCIA card at slot 0 (Sector size 512 bytes) .
8192K bytes of Flash internal SIMM (Sector size 256K).

————-System Configuration Dialog ————-
```

```
Would you like to enter the initial configuration dialog? [yes/no]:
```

A. No configuration file was found in NVRAM.
B. No configuration file was found in flash.
C. No configuration file was found in the PCMCIA card.
D. Configuration file is normal and will load in 15 seconds.

Answer: A

Explanation

When no startup configuration file is found in NVRAM, the System Configuration Dialog will appear to ask if we want to enter the initial configuration dialog or not.

Question 3

Which command displays CPU utilization?

A. show protocols
B. show process
C. show system
D. show version

Answer: B

Explanation

The “show process” (in fact, the full command is “show processes”) command gives us lots of information about each process but in fact it is not easy to read. Below shows the output of this command (some next pages are omitted)

```
Router#show process
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
 PID QTy       PC Runtime (ms)     Invoked   uSecs    Stacks TTY Process
   1 Cwe 6048DB4C           0           1       0 5604/6000   0 Chunk Manager
   2 Csp 604BCD68           0          15       0 2632/3000   0 Load Meter
   3 M*         0          28          20  140010724/12000  0 Exec
   5 Mwe 61496B84           0           1       023460/24000  0 EDDRI_MAIN
   6 Lst 6049C5E4          88          10    8800 5632/6000   0 Check heaps
   7 Cwe 604A2754           0           1       0 5592/6000   0 Pool Manager
   8 Mst 603D219C           0           2       0 5580/6000   0 Timers
   9 Mwe 600245DC           0           2       0 5584/6000   0 Serial Backgroun
  10 Mwe 602D6BB4           0           2       0 5680/6000   0 IPC Dynamic Cach
  11 Mwe 602CEF94           0           1       0 5636/6000   0 IPC Zone Manager
  12 Mwe 602CECF4           0          75       0 5708/6000   0 IPC Periodic Tim
  13 Mwe 602CEC3C           4          77      51 5624/6000   0 IPC Deferred Por
  14 Mwe 602CEDA8           4           1    4000 5596/6000   0 IPC Seat Manager
  15 Mwe 603A4900           0           2       0 5576/6000   0 AAA high-capacit
  16 Mwe 60547C2C           0           1       011604/12000  0 OIR Handler
  17 Msi 60572C2C           0           4       0 5600/6000   0 Environmental mo
  19 Mwe 6057B190           4           5     800 5588/6000   0 ARP Input
  20 Mwe 6079D838           0          19       0 5660/6000   0 HC Counter Timer
  21 Mwe 6081D4A0           0           2       0 5576/6000   0 DDR Timers
  22 Lwe 60A9AE28           0           3       0 5532/6000   0 Entity MIB API
  23 Mwe 613B56A0           0           2       0 5584/6000   0 ATM Idle Timer
```

A more friendly way to check the CPU utilization is the command “show processes cpu history”, in which the total CPU usage on the router over a period of time: one minute, one hour, and 72 hours are clearly shown:

+ The Y-axis of the graph is the CPU utilization.
+ The X-axis of the graph is the increment within the period displayed in the graph

For example, from the last graph (last 72 hours) we learn that the highest CPU utilization within 72 hours is 37% about six hours ago.

Question 4

Refer to the exhibit:

Router1# **show ip arp**

Protocol	Address	Age(min)	Hardware Adddr	Type	Interface
Internet	192.168.20.5	9	0000.0c07.f892	ARPA	FastEthernet0/0
Internet	192.168.60.5	8	0000.0c07.ac00	ARPA	FastEthernet0/1
Internet	192.168.20.1	-	0000.0c63.ae45	ARPA	FastEthernet0/0
Internet	192.168.40.5	9	0000.0c07.4320	ARPA	FastEthernet0/2
Internet	192.168.60.1	-	0000.0c63.1300	ARPA	FastEthernet0/1
Internet	192.168.40.1	-	0000.0c36.6965	ARPA	FastEthernet0/2

Data Frame:

Source MAC	Source IP	Destination MAC	Destination IP
0000.0c07.f892	192.168.20.5	0000.0c63.ae45	192.168.40.5

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

A. Router1 will strip off the source MAC address and replace it with the MAC address 0000.0c36.6965.
B. Router1 will strip off the source IP address and replace it with the IP address 192.168.40.1.
C. Router1 will strip off the destination MAC address and replace it with the MAC address 0000.0c07.4320.
D. Router1 will strip off the destination IP address and replace it with the IP address of 192.168.40.1.
E. Router1 will forward the data packet out interface FastEthernet0/1.
F. Router1 will forward the data packet out interface FastEthernet0/2.

Answer: A C F

Explanation

The “Age” field in the “show ip arp” command is the age in minutes of the cache entry. A hyphen (-) means the address is local so in this case 192.168.20.1, 192.168.40.1 & 192.168.60.1 are local to this router.

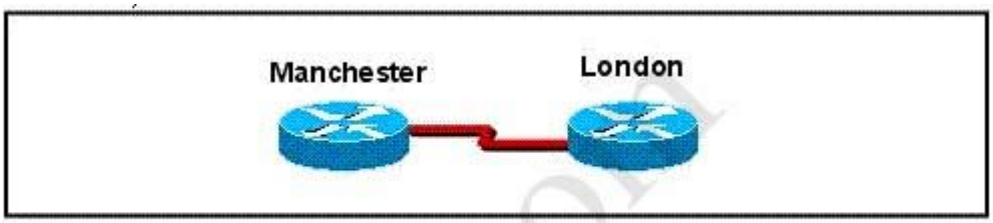
From the “Data Frame”, we learn that a packet is sent to Router1 and Router1 needs to forward it to the Destination IP 192.168.40.5. Therefore this router will:

+ Strip off the source MAC address and replace it with the MAC address 0000.0c36.6965 (because the IP address of this interface – 192.168.40.1 is in the same subnet with the Destination IP 192.138.40.5).
+ Strip off the destination MAC address and replace it with the MAC address 0000.0c07.4320, which is the MAC of Destination host.
+ Forward the data packet out interface FastEthemet0/2 because this interface has the IP address of 192.168.40.1.

CCNA – Show commands

Question 1

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

Answer: A C E

Explanation

From the output, we learn that the IP address of the neighbor router is 10.1.1.2 and the question stated that the subnet mask of the network between two router is 255.255.255.252. Therefore there are only 2 available hosts in this network ($2^2 – 2 = 2$). So we can deduce the ip address (of the serial interface) of Manchester router is 10.1.1.1 -> A is correct

The platform of the neighbor router is cisco 2610, as shown in the output -> C is correct

Maybe the most difficult choice of this question is the answer E or F. Please notice that “Interface” refers to the local port on the local router, in this case it is the port of Manchester router, and “Port ID (outgoing port)” refers to the port on the neighbor router -> E is correct.

Question 2

Which command reveals the last method used to powercycle a router?

A. show reload
B. show boot
C. show running-config
D. show version

Answer: D

Explanation

The “show version” command can be used to show the last method to powercycle (reset) a router

```
Router>show version
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-IK9S-M), Version 12.2(40a), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2007 by cisco Systems, Inc.
Compiled Sat 10-Mar-07 21:57 by pwade
Image text-base: 0x60008930, data-base: 0x612A2000

ROM: ROMMON Emulation Microcode
ROM: 3600 Software (C3640-IK9S-M), Version 12.2(40a), RELEASE SOFTWARE (fc1)

Router uptime is 3 minutes
System returned to ROM by unknown reload cause - suspect boot_data[BOOT_COUNT] 0x0
System image file is "tftp://255.255.255.255/unknown"


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

cisco 3640 (R4700) processor (revision 0xFF) with 126976K/4096K bytes of memory.
Processor board ID 00000000
R4700 CPU at 100Mhz, Implementation 33, Rev 1.2
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
1 FastEthernet/IEEE 802.3 interface(s)
4 Serial network interface(s)
DRAM configuration is 64 bits wide with parity enabled.
125K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)

Configuration register is 0x2142

Router>
```


Question 3

When you are troubleshooting an ACL issue on a router, which command would you use to verify which interfaces are affected by the ACL?

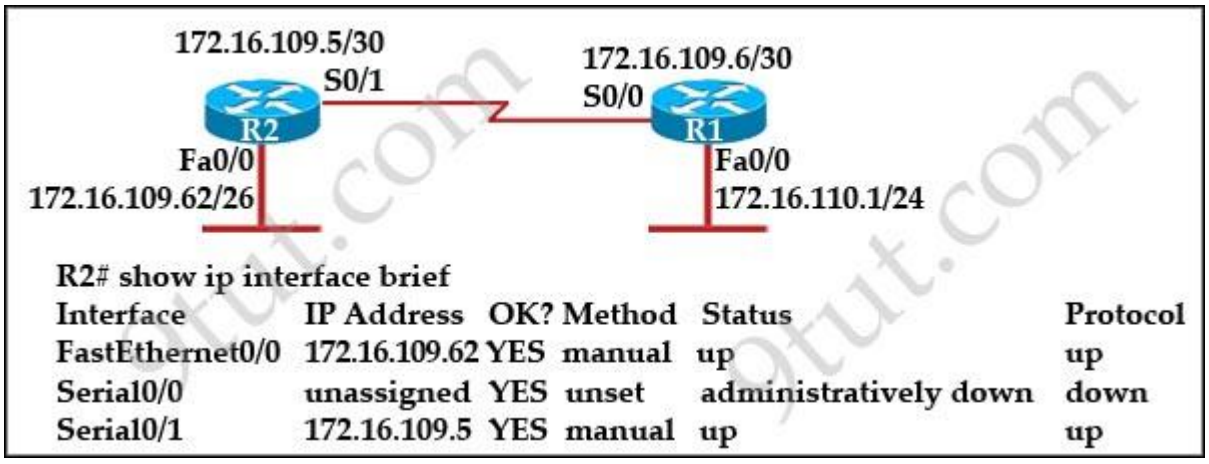
A. show ip access-lists
B. show access-lists
C. show interface
D. show ip interface
E. list ip interface

Answer: D

CCNA – Troubleshooting

Question 1

Refer to the exhibit:



Assuming that the entire network topology is shown, what is the operational status of the interfaces of R2 as indicated by the command output shown?

A. One interface has a problem.
B. Two interfaces have problems.
C. The interfaces are functioning correctly.
D. The operational status of the interfaces cannot be determined from the output shown.

Answer: C

Explanation

The subnet of Fa0/0 of R2 is 172.16.109.0/26 (range from 172.16.109.0 to 172.16.109.63) which covers the subnet of S0/1 interface 172.16.109.4/30 so in fact the answer C is not correct. But from the output of the "show ip interface brief" command we see both Fa0/0 and S0/1 interfaces' statuses are 'up/up' -> they are working normally. So we think there is a typo in the subnet mask of Fa0/0. It should not be '/26′ but longer one, '/28′, for example. So you should still choose answer C in this question.

Question 2

Refer to the exhibit:

```
ALSwitch1# show interfaces fastethernet0/24 switchport
Name: Fa0/24
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operatfonal Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Operafional private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false

Voice VLAN: none (Inactive)
Appliance trust: none
```

Switch port FastEthernet 0/24 on AlSwitch1 will be used to create an IEEE 802.1Q-complaint trunk to another switch. Based on the output shown, What is the reason the trunk does not form, even thought the proper cabling has been attached?

A. VLANs have not been created yet.
B. An IP address must be configured for the port.
C. The port is currently configured for access mode.
D. The correct encapsulation type has not been configured.
E. The no shutdown command has not been entered for the port.

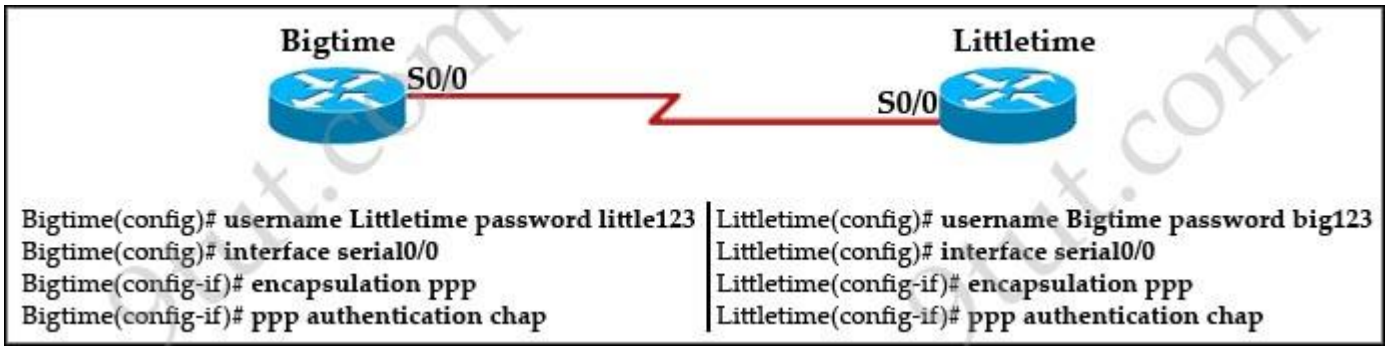
Answer: C

Explanation

The “Operational Mode” is “static access” so this port is currently in access mode.

Question 3

Refer to the exhibit:



The Bigtime router is unable to authenticate to the Littletime router. What is the cause of the problem?

A. The usernames are incorrectly configured on the two routers.
B. The passwords do not match on the two routers.
C. CHAP authentication cannot be used on a serial interface.
D. The routers cannot be connected from interface S0/0 to interface S0/0.
E. With CHAP authentication, one router must authenticate to another router. The routers cannot be configured to authenticate to each other.

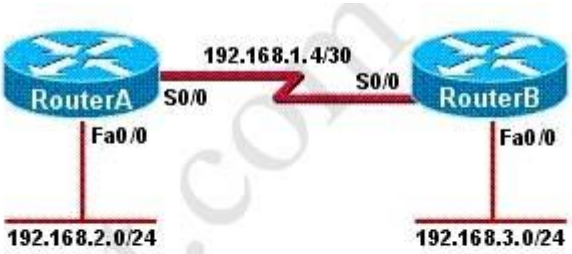
Answer: B

Explanation

Both routers must use the same password for CHAP to authentication.

Question 4

Refer to the exhibit. Hosts in network 192.168.2.0 are unable to reach hosts in network 192.168.3.0. Based on the output from RouterA, what are two possible reasons for the failure? (Choose two)




```
RouterA# show ip interface brief
Interface          IP-Address      OK? Method Status                Protocol
FastEthernet0/0    192.168.2.1     YES manual up                    up
Serial0/0          192.168.1.5     YES manual up                    down
Serial0/1          unassigned      YES manual administratively down down
```

A. The cable that is connected to S0/0 on RouterA is faulty.
B. Interface S0/0 on RouterB is administratively down.
C. Interface S0/0 on RouterA is configured with an incorrect subnet mask.

D. The IP address that is configured on S0/0 of RouterB is not in the correct subnet.
E. Interface S0/0 on RouterA is not receiving a clock signal from the CSU/DSU.
F. The encapsulation that is configured on S0/0 of RouterB does not match the encapsulation that is configured on S0/0 of RouterA.

Answer: E F

Explanation

From the output we see the Serial0/0 of RouterA is in "status up/protocol down" state which indicates a Layer 2 problem so the problem can be:

+ Keepalives mismatch
+ Encapsulation mismatch
+ Clocking problem

Question 5

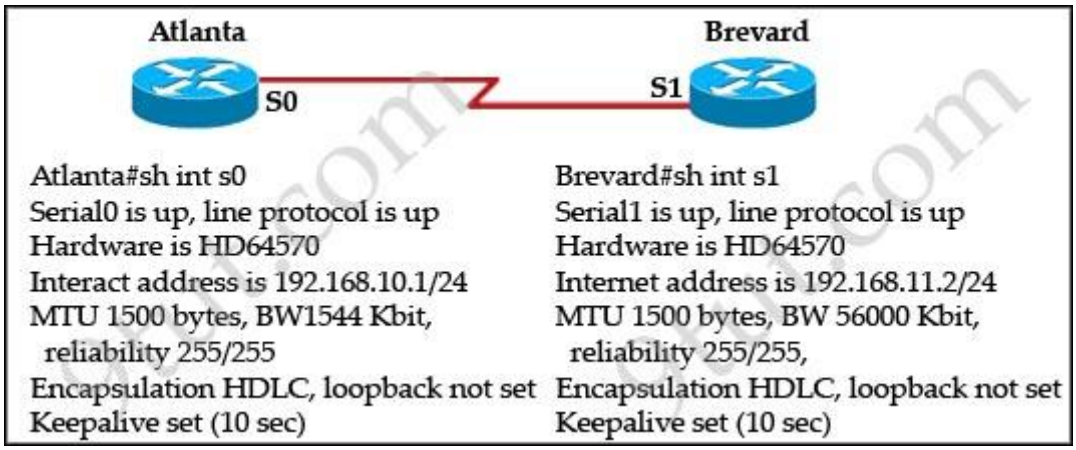
Which command can be used from a PC to verify the connectivity between hosts that connect through a switch in the same LAN?

A. pingaddress
B. tracertaddress
C. tracerouteaddress
D. arpaddress

Answer: A

Question 6

Two routers named Atlanta and Brevard are connected by their serial interfaces as illustrated, but there is no connectivity between them. The Atlanta router is known to have a correct configuration. Given the partial configurations, identify the problem on the Brevard router that is causing the lack of connectivity.

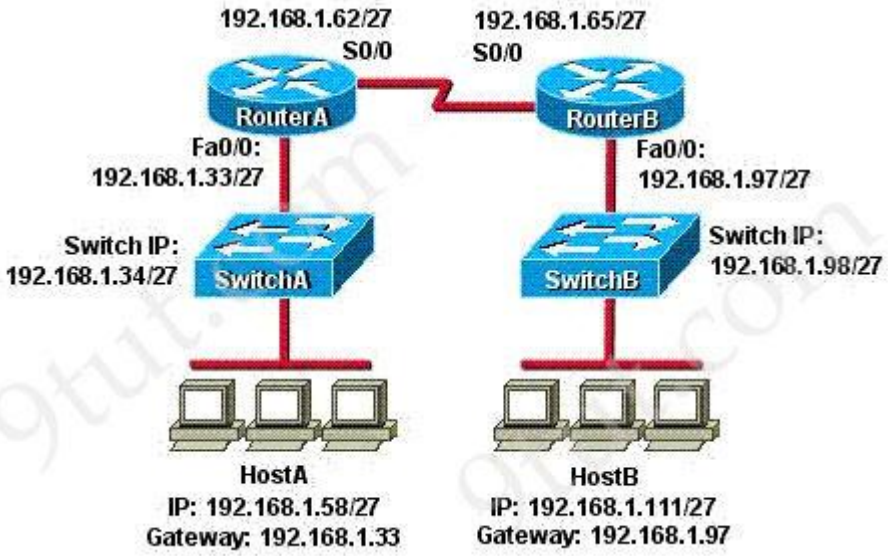


A. transmission unit size too large
B. no loopback set
C. an incorrect subnet mask
D. incompatible encapsulation at each end
E. an incorrect IP address
F. incompatible bandwidth between routers

Answer: E

Question 7

Refer to the exhibit. HostA cannot ping HostB. Assuming routing is properly configured, what could be the cause of this problem?



A. HostA is not on the same subnet as its default gateway.
B. The address of SwitchA is a subnet address.
C. The Fa0/0 interface on RouterA is on a subnet that can't be used.
D. The serial interfaces of the routers are not on the same subnet.
E. The Fa0/0 interface on RouterB is using a broadcast address.

Answer: D

Explanation

Now let's find out the range of the networks on serial link:

For the network 192.168.1.62/27:

Increment: 32
Network address: 192.168.1.32
Broadcast address: 192.168.1.63

For the network 192.168.1.65/27:

Increment: 32
Network address: 192.168.1.64
Broadcast address: 192.168.1.95

-> These two IP addresses don't belong to the same network and they can't see each other -> D is the correct answer.

Question 8

```
Router# show interface s0/0
Serial 0/0/0 is administratively down, line protocol is down
```

What is the reason that the interface status is "administratively down, line protocol down"?

A. There is no encapsulation type configured.
B. There is a mismatch in encapsulation types.
C. The interface is not receiving any keepalives.
D. The interface has been configured with the shutdown command.
E. The interface needs to be configured as a DTE device.
F. The wrong type of cable is connected to the interface.

Answer: D

Question 9

Refer to the exhibit. A network administrator configures a new router and enters the copy startup-config running-config on the router. The network administrator powers down the router and sets it up at a remote location. When the router starts, it enter the system configuration dialog as shown. What is the cause of the problem?

```
— System Configuration Dialog —
Would you like to enter the initial configuration dialog? [yes/no]: % Please answer yes' or 'no'.
```

```
Would you like to enter the initial configuration dialog? [yes/ho]: n

Would you like to terminate autoinstall? [yes]:

Press RETURN to get started!
```

A. The network administrator failed to save the configuration.
B. The configuration register is set to 0×2100.
C. The boot system flash command is missing from the configuration.
D. The configuration register is set to 0×2102.
E. The router is configured with the boot system startup command.

Answer: A

Explanation

The “System Configuration Dialog” appears only when no startup configuration file is found. The network administrator has made a mistake because the command “copy startup-config running-config” will copy the startup config (which is empty) over the running config (which is configured by the administrator). So everything configured was deleted.

Note: We can tell the router to ignore the start-up configuration on the next reload by setting the register to 0×2142. This will make the “System Configuration Dialog” appear at the next reload.

CCNA – IPv6

Note: If you are not sure about IPv6, please read our IPv6 tutorial.

Question 1

Which IPv6 address is valid?

A. 2031:0:130F::9C0:876A:130B
B. 2001:0DB8:0000:130F:0000:0000:08GC:140B
C. 2001:0DB8:0:130H::87C:140B
D. 2031::130F::9C0:876A:130B

Answer: A

Explanation

Answer B is not correct because it has a letter "G".

Answer C is not correct because it has a letter "H".

Answer D is not correct because it has two "::".

Question 2

Which IPv6 address is the equivalent of the IPv4 interface loopback address 127.0.0.1?

A. ::1
B. ::
C. 2000::/3
D. 0::/10

Answer: A

Question 3

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

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

Answer: D

Question 4

Which IPv6 address is the all-router multicast group?

A. FF02::1
B. FF02::2
C. FF02::3
D. FF02::4

Answer: B

Question 5

Which three are characteristics of an IPv6 anycast address? (Choose three)

A. one-to-many communication model
B. one-to-nearest communication model
C. any-to-many communication model
D. a unique IPv6 address for each device in the group
E. the same address for multiple devices in the group
F. delivery of packets to the group interface that is closest to the sending device

Answer: B E F

Question 6

Which two are features of IPv6? (Choose two)

A. multicast
B. broadcast
C. allcast
D. podcast
E. anycast

Answer: A E

Explanation

Anycast IPv6 addresses are 128-bit identifiers for interfaces and sets of interfaces. A packet sent to an anycast address is delivered to one of the interfaces identified by that address (the “nearest” one, according to the routing protocols’ measure of distance)

Question 7

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

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

Answer: B D F

Question 8

Which of these represents an IPv6 link-local address?

A. FE08::280e:611:a:f14f.3d69
B. FE81::280f.512b:e14f:3d69
C. FE80::380e:611a:e14f:3d69
D. FEFE:0345:5f1b::e14d:3d69

Answer: C

Explanation

The range of IPv6 link-local address (similar to the Windows auto-configuration IP address of 169.254.x.x.) is FE80::/10. For more information about IPv6, please read my IPv6 tutorial.

Question 9

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

An example of configuring RIPng (similar to RIPv2 but is used for IPv6) is shown below:

Router(config)#**ipv6 unicast-routing** (Enables the forwarding of IPv6 unicast datagrams globally on the router)
Router(config)#**interface fa0/0**
Router(config-if)#**ipv6 rip 9tut enable** (9tut is the process name of this RIPng)

Question 10

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

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

Answer: A D

Explanation

Below is the list of common kinds of IPv6 addresses:

Loopback address	::1
Link-local address	FE80::/10
Site-local address	FEC0::/10
Global address	2000::/3
Multicast address	FF00::/8

From the above table, we learn that A and D are correct while B and C are incorrect. Notice that the IPv6 unicast loopback address is equivalent to the IPv4 loopback address, 127.0.0.1. The IPv6 loopback address is 0:0:0:0:0:0:0:1, or ::1.

E is not correct because of anycast addresses which are indistinguishable from normal unicast addresses. You can think of anycast addresses like this: “send it to nearest one which have this address”. An anycast address can be assigned to many interfaces and the first interface receives the packet destined for this anycast address will proceed the packet. A benefit of anycast addressing is the capability to share load to multiple hosts. An example of this benefit is if you are a Television provider with multiple servers and you want your users to use the nearest server to them then you can use anycast addressing for your servers. When the user initiates a connection to the anycast address, the packet will be routed to the nearest server (the user does not have to specify which server they want to use).

CCNA – IPv6 Questions 2

Note: If you are not sure about IPv6, please read our IPv6 tutorial.

Question 1

What are three features of the IPv6 protocol? (Choose three)
A. optional IPsec
B. autoconfiguration
C. no broadcasts
D. complicated header
E. plug-and-play
F. checksums

Answer: B C E

Question 2

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

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

Answer: B C

Explanation

Leading zeros in IPv6 are optional do that 05C7 equals 5C7 and 0000 equals 0 -> D is not correct.

Question 3

Which option is a valid IPv6 address?

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

Answer: D

Question 4

What is the alternative notation for the IPV6 address
B514:82C3:0000:0000:0029:EC7A:0000:EC72?

A. B514:82C3:0029::EC7A:0000:EC72
B. B514:82C3:0029:EC7A:EC72
C. B514:82C3::0029:EC7A:0:EC72
D. B514:82C3::0029:EC7A:EC72

Answer: C

Question 5

Which switch would STP choose to become the root bridge in the selection process?

A. 32768: 11-22-33-44-55-66
B. 32768: 22-33-44-55-66-77
C. 32769: 11-22-33-44-55-65
D. 32769: 22-33-44-55-66-78

Answer: A

Question 6

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

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

Answer: D

Explanation

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

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

Question 7

What is known as “one-to-nearest” addressing in IPv6?

A. global unicast
B. anycast
C. multicast
D. unspecified address

Answer: B

Question 8

The network administrator has been asked to give reasons for moving from IPv4 to IPv6. What are two valid reasons for adopting IPv6 over IPv4? (Choose two)

A. telnet access does not require a password
B. nat
C. no broadcast
D. change of destination address in the IPv6 header
E. change of source address in the IPv6 header
F. autoconfiguration

Answer: C F

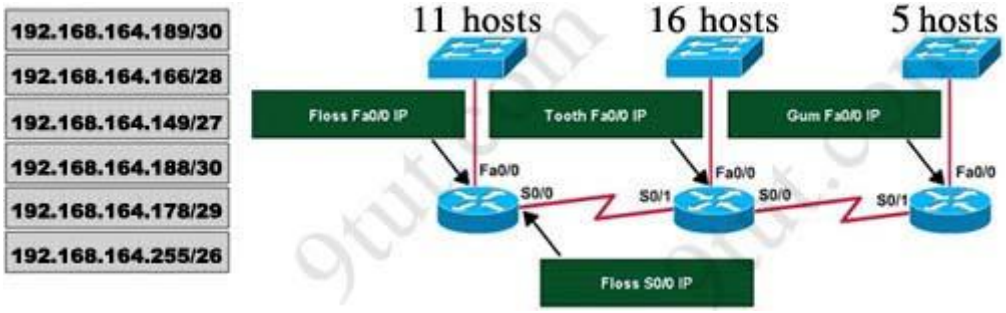
Explanation

With IPv6, devices can build a link-local address automatically. But notice this address is only used for communications within the local subnetwork, routers do not forward these addresses.

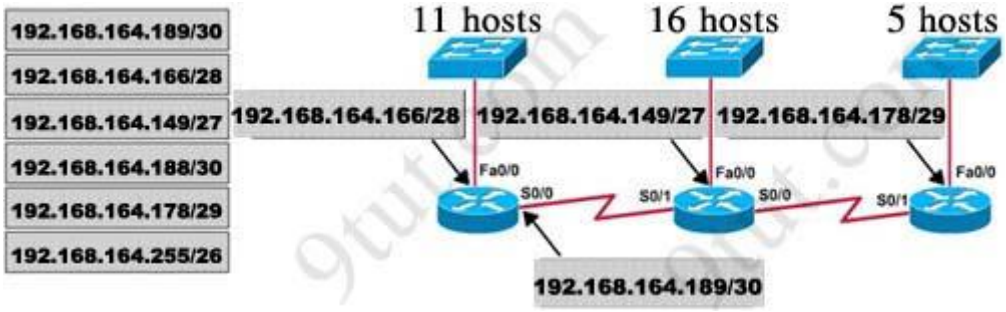
CCNA – Drag and Drop 1

Question 1

A dental firm is redesigning the network that connects its three locations. The administrator gave the networking team 192.168.164.0 to use for addressing the entire netwok. After subnetting the address, the team is ready to assign the addresses. The administrator plans to configure ip subnet-zero and use RIP v2 as the routing protocol. As a member of the networking team, you must address the network and at the same time conserver unused addresses for future growth. With those goals in mind, drag the host addresses on the left to the correct router interface. Once of the routers is partially configured. Move your mouse over a router to view its configuration. Not all of the host addresses on the left are necessary.



Answer:



Explanation

In short, we should start calculating from the biggest network (with 16 hosts) to the smallest one using the formula $2^n - 2$ (n is the number of bits we need to borrow).Therefore:

16 hosts < $2^5 - 2$ (we need to borrow 5 bits -> /27)

11 hosts < $2^4 - 2$ (borrow 4 bits -> /28)

5 hosts < $2^3 - 2$ (borrow 3 bits -> /29)

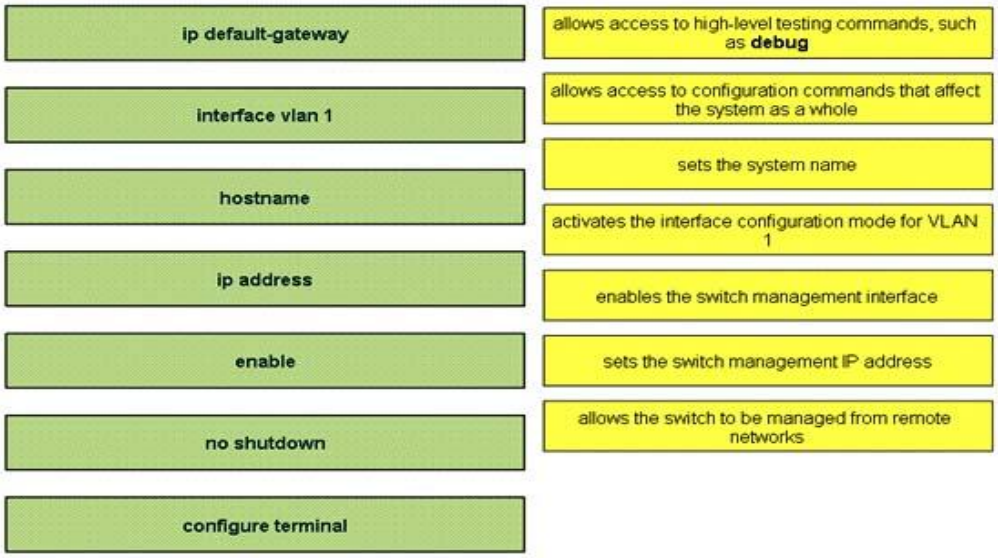
From the available ip addresses, we see that each of them has only one suitable solution (they are 192.168.164.149/27,192.168.164.166/28 and 192.168.164.178/29)

The smallest network is the Floss S0/0 which only requires 2 hosts = $2^2 - 2$ (need to borrow 2 bits ->/30). There are 2 suitable answers: 192.168.164.189/30 and 192.168.164.188/30 but notice that 192.168.164.188/30 is the network address so we can not use it (because 188 = 4 * 47) -> we have to choose 192.168.164.189 as the correct solution.

In fact, it is not the formal way to solve a VLSM question so I recommend you to review your CCNA book if you haven't grasped it well yet.

Question 2

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



Answer:

1) enable

2) configure terminal

3) hostname

4) Interface vlan 1

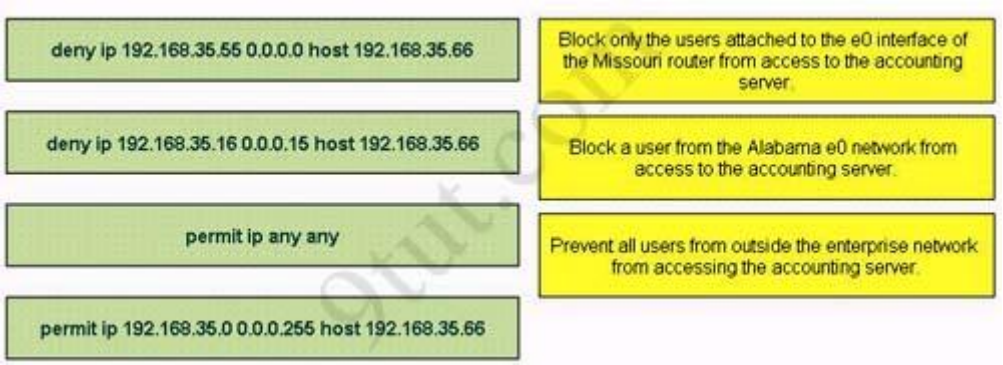
5) no shutdown

6) ip address

7) ip default-gateway

Question 3

The Missouri branch office router is connected through its s0 interface to the Alabama Headquarters router s1 interface. The Alabama router has two LANs. Missouri users obtain Internet access through the Headquarters router. The network interfaces in the topology are addressed as follows: **Missouri**: **e0 – 192.168.35.17/28**; **s0 – 192.168.35.33/28**; **Alabama**: **e0 – 192.168.35.49/28**; **e1 – 192.168.35.65/28**; **s1 – 192.168.35.34/28**. The accounting server has the address of **192.168.35.66/28**. Match the access list conditions on the left with the goals on the right. (Not all options on the left are used.)



Answer:

1) deny ip 192.168.35.16 0.0.0.15 host 192.168.35.66

2) deny ip 192.168.35.55 0.0.0.0 host 192.168.35.66

3) permit ip 192.168.35.0 0.0.0.255 host 192.168.35.66

Explanation

1) The wildcard mask of the command "deny ip 192.168.35.16 0.0.0.15 host 192.16.35.66″ is 0.0.0.15, which is equal to network mask of 255.255.255.240 = /28. So the access list will deny all traffic from network 192.168.35.16/28 from accessing host 192.16.35.66, which is the IP address of accounting server.

2) The command "deny ip 192.168.35.55 0.0.0.0 host 192.168.35.66″ will deny host 192.168.35.55, which is a user and belongs to interface e0 of Alabama router (192.168.35.49/28) from accessing accounting server.

3) Because there is an implicit "deny all" command at the end of each access list so the command "permit ip 192.168.35.0 0.0.0.255 host 192.168.35.66″ will only let network 192.168.35.0/24 access accounting server whilst prevent traffic from other networks.

Question 4

A host with the address of 192.168.125.34/27 needs to be denied access to all hosts outside its own subnet. To accomplish this, complete the command in brackets, **[access-list 100 deny *protocol address mask* any]**, by dragging the appropriate options on the left to their correct placeholders on the right.

Answer:

1) ip

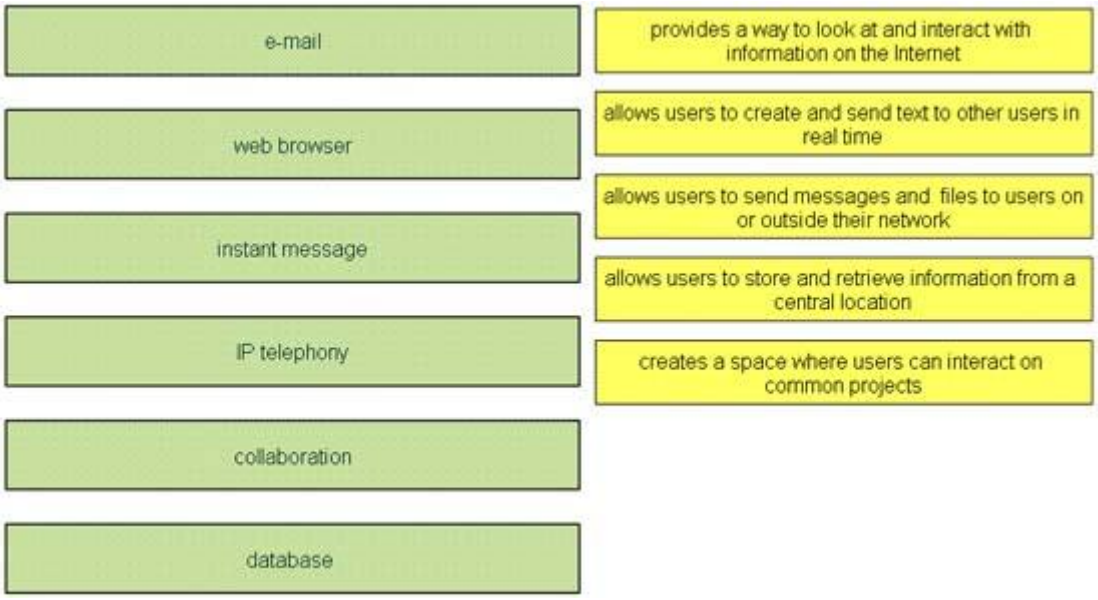
2) 192.168.125.34

3) 0.0.0.0

Full command: access-list 100 deny ip 192.168.125.34 0.0.0.0

Question 5

Drag and drop the network user application to the appropriate description of its primary use (not all options are used)



Answer:

1) web browser

2) instant message

3) e-mail

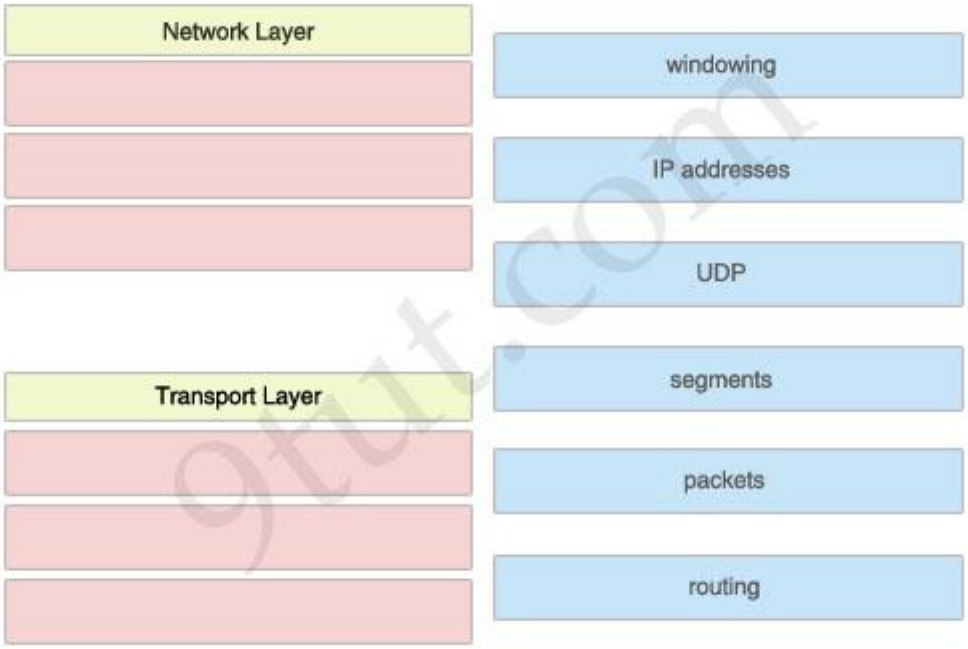
4) database

5) collaboration

CCNA – Drag and Drop 2

Question 1

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



Answer:

Network Layer:

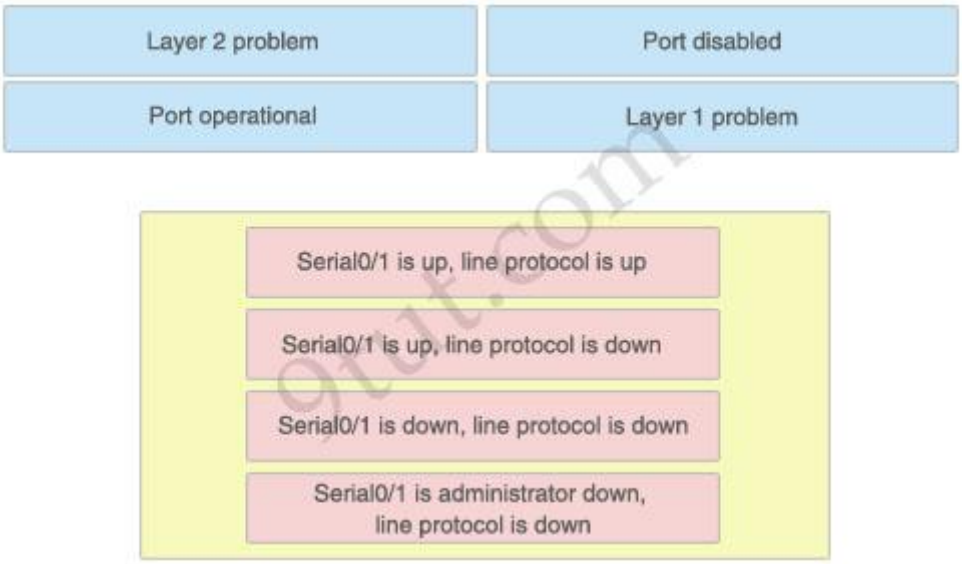
1) IP addresses
2) packets
3) routing

Transport Layer:

1) windowing
2) UDP
3) segments

Question 2

The above describes some categories, while the below provides their corresponding router output lines. Drag the above items to the proper locations.



Answer:

1) Port operational: Serial0/1 is up, line protocol is up
2) Layer 2 problem: Serial0/1 is up, line protocol is down
3) Layer 1 problem: Serial0/1 is down, line protocol is down
4) Port disabled: Serial0/1 is administrator down, line protocol is down

Explanation:

A simple way to find out which layer is having problem is to remember this rule: "the first statement is for Layer 1, the last statement is for Layer 2 and if Layer 1 is down then surely Layer 2 will be down too", so you have to check Layer 1 before checking Layer 2. For example, from the output "Serial0/1 is up, line protocol is down" we know that it is a layer 2 problem because the first statement (Serial0/1 is up) is good while the last statement (line protocol is down) is bad. For the statement "Serial0/1 is down, line protocol is down", both layers are down so the problem belongs to Layer 1.

There is only one special case with the statement "…. is administrator down, line protocol is down". In this case, we know that the port is currently disabled and shut down by the administrators.

Question 3

A user is unable to connect to the Internet. Based on the layered approach to troubleshooting and beginning with the lowest layer. Follow the guide and drag the contents to relevant modules.

Answer:

1) Verify Ethernet cable connection: Step 1
2) Verify NIC operation: Step 2
3) Verify IP configuration: Step 3
4) Verify URL: Step 4

Explanation

The question asks us to "begin with the lowest layer" so we have to begin with Layer 1: verify physical connection; in this case an Ethernet cable connection. For your information, "verify Ethernet cable connection" means that we check if the type of connection (crossover, straight-through, rollover…) is correct, the RJ45 headers are plugged in, the signal on the cable is acceptable…

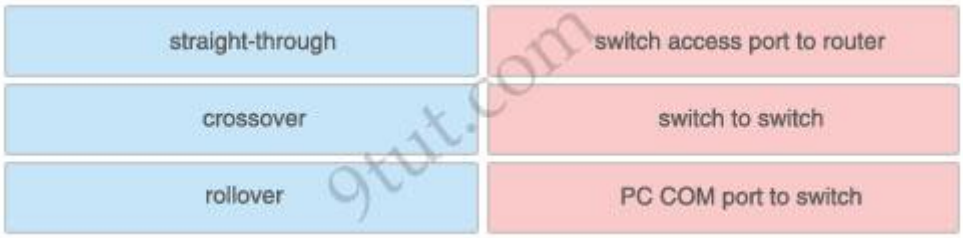
Next we "verify NIC operation". We do this by simply making a ping to the loopback interface 127.0.0.1. If it works then the NIC card (layer 1,2) and TCP/IP stack (layer 3) are working properly.

Verify IP configuration belongs to layer 3. For example, checking if the IP can be assignable for host, the PC's IP is in the same network with the gateway…

Verifying the URL by typing in your browser some popular websites like google.com, microsoft.com to assure that the far end server is not down (it sometimes make we think we can't access to the Internet). We are using a URL so this step belongs to layer 7 of the OSI model.

Question 4

The left describes the types of cables, while the right describes the purposes of the cables. Drag the items on the left to the proper locations. (Not all items can be used).



Answer:

1) straight-through: switch access port to router
2) crossover: switch to switch
3) rollover: PC COM port to switch

Explanation:

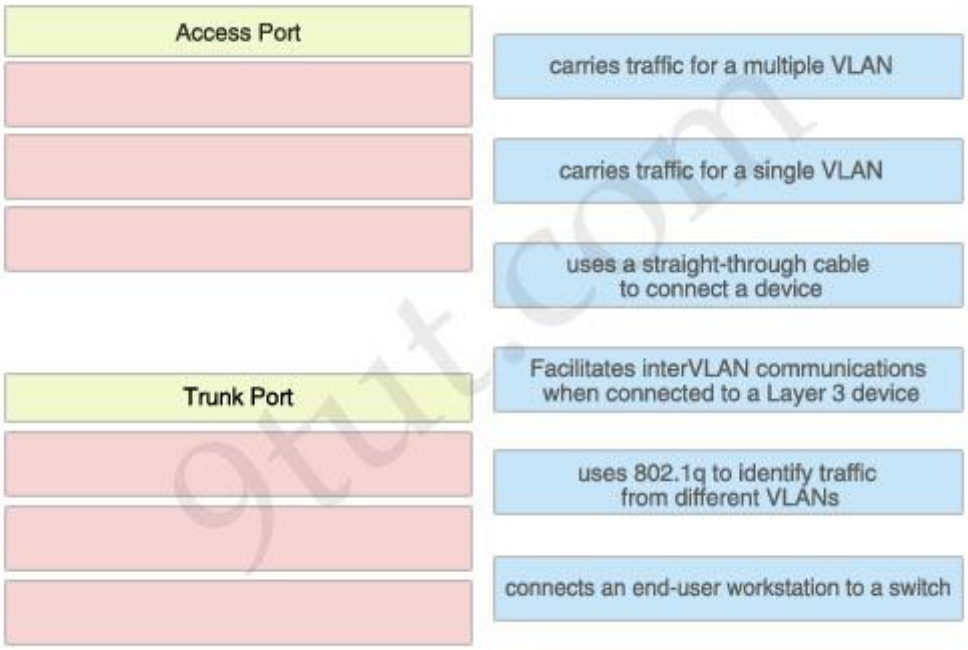
To remember which type of cable you should use, follow these tips:

– 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…)

Question 5

The left describes the types of switch ports, while the right describes the features. Drag the options on the right to the proper locations.



Answer:

Access Port:

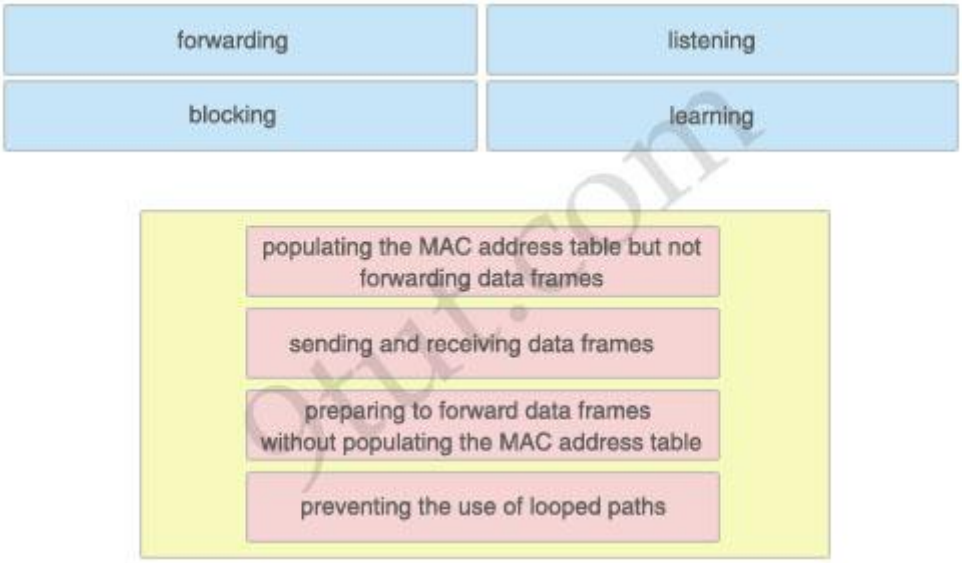
– Carries traffic for a single VLAN
– Uses a straight-through cable to connect a device
– Connects an end-user workstation to a switch

Trunk Port:

– Carries traffic for a multiple VLAN
– Uses 802.1q to identify traffic from different VLANs
– Facilitates interVLAN communications when connected to a Layer 3 device

Question 6

The above describes the Spanning-Tree Protocol port states, while the below describes their functions. Drag the above items to the proper locations.



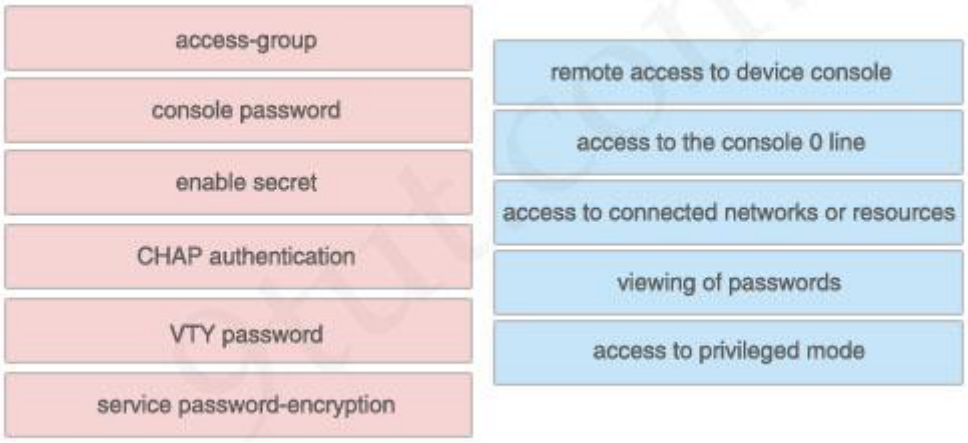
Answer:

– Learning: populating the MAC address table but not forwarding data frames
– Forwarding: sending and receiving data frames
– Listening: preparing to forward data frames without populating the MAC address table
– Blocking: preventing the use of looped paths

CCNA – Drag and Drop 3

Question 1

Drag the security features on the left to the specific security risks they help protect against on the right. (Not all options are used)



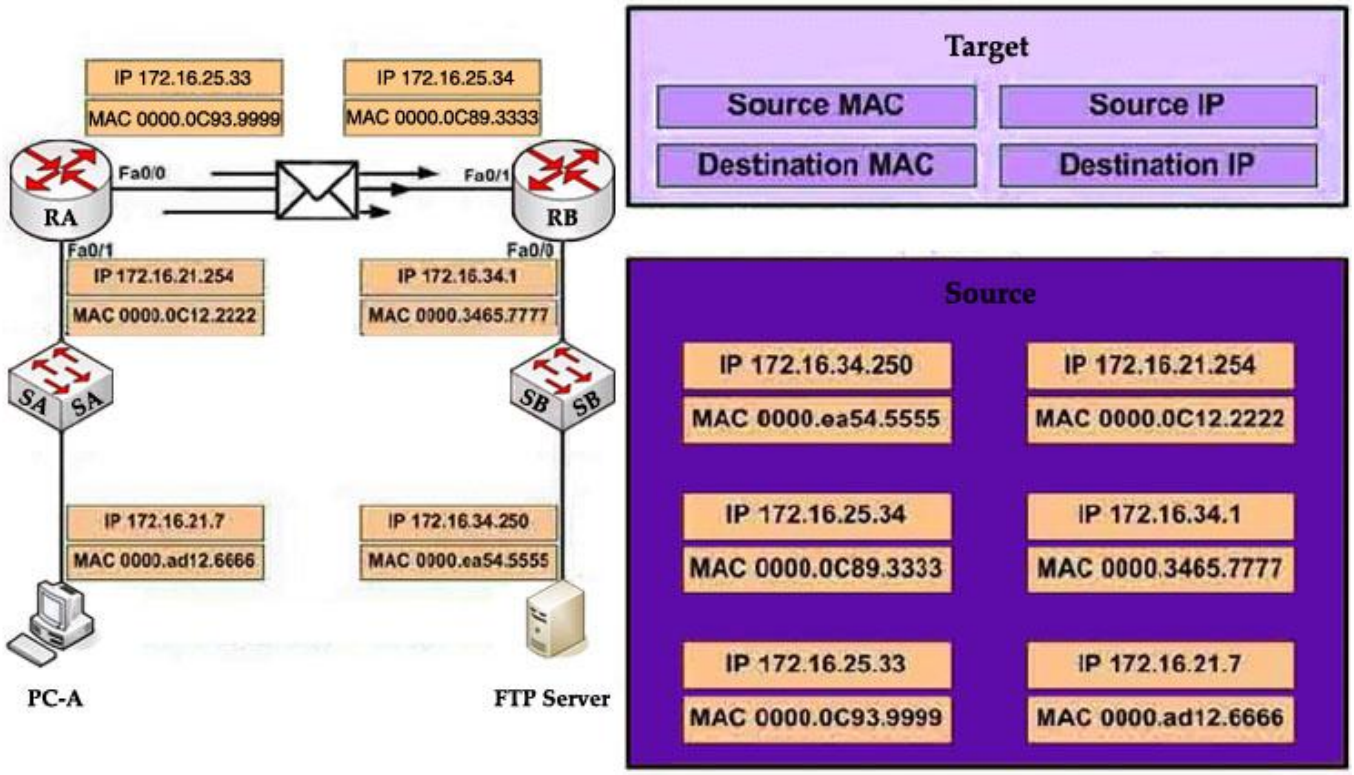
Answer:

1) VTY password: remote access to device console
2) console password: access to the console 0 line
3) access-group: access to connected networks or resources
4) service password-encryption: viewing of passwords
5) enable secret: access to privileged mode

The unselected left-box – CHAP – is used to verify the identity of the peer by means of a three-way handshake.

Question 2

Refer to the exhibit. PC-A is sending packets to the FTP server. Consider the packets as they leave RA interface Fa0/0 forwards RB. Drag the correct frame and packet address to their places in the table.



Answer:

Source MAC: 0000.0C93.9999
Destination MAC: 0000.0C89.3333
Source IP: 172.16.21.7
Destination IP: 172.16.34.250

Explanation

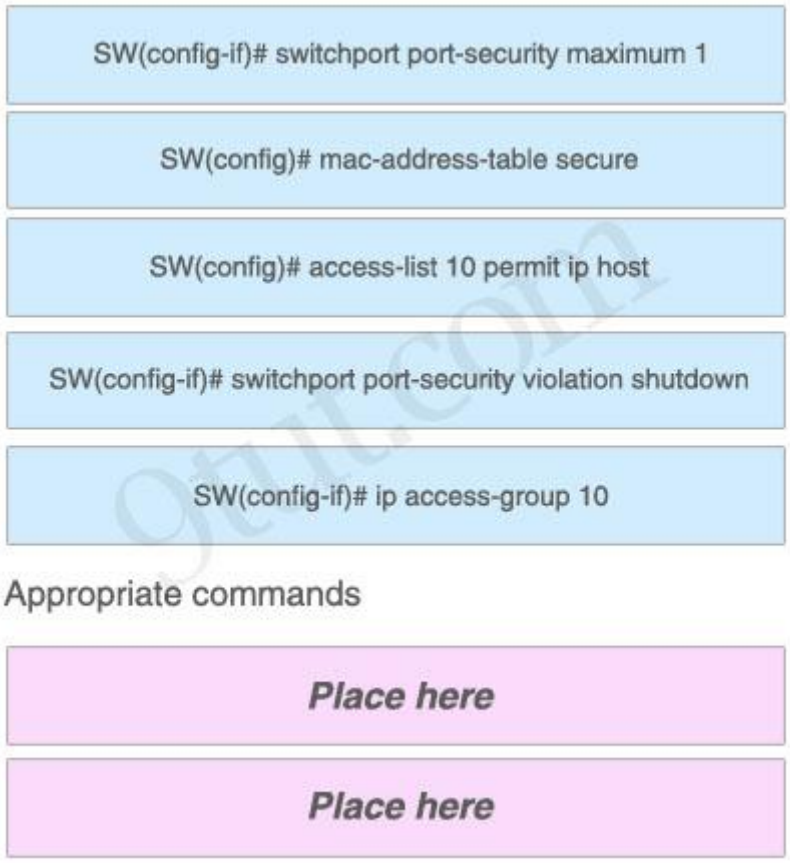
Remember these rules:

The IP addresses (of source and destination) of a packet never change during the transportation through the network. For example if PC-A wants to send a packet to PC-Z then the source and destination IP addresses of the packet will be the IP addresses of PC-A and PC-Z no matter how many devices they go through.

The MAC addresses, conversely, will change while passing the devices. The source MAC address is the address of the last sender and the destination MAC address is the address of the next device.

Question 3

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



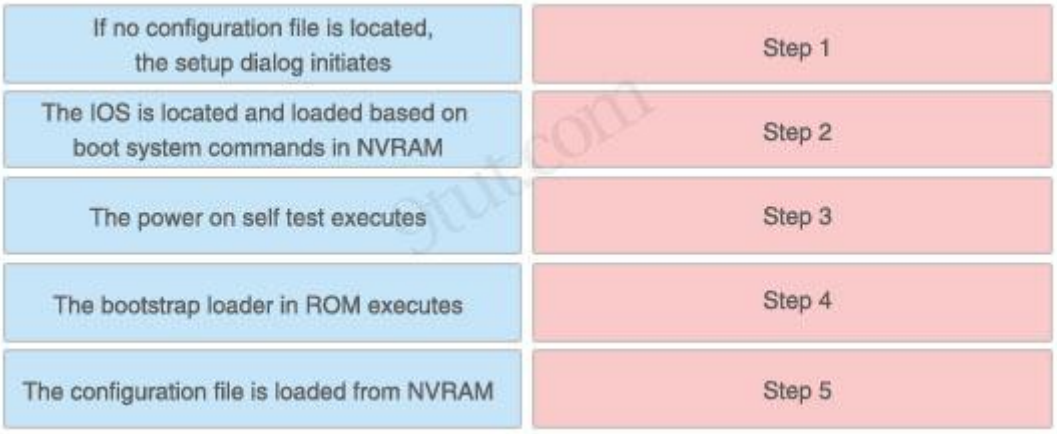
Answer:

Appropriate commands:

SW(config-if)# switchport port-security maximum 1
SW(config-if)# switchport port-security violation shutdown

Question 4

The left describes boot sequence, while the right describes the orders. Drag the items on the left to the proper locations.



Answer:

1) Step 1: The power on self test executes.
2) Step 2: The bootstrap loader in ROM executes.
3) Step 3: The IOS is located and loaded based on boot system commands in NVRAM.
4) Step 4: The configuration file is loaded from NVRAM.
5) Step 5: If no configuration file is located, the setup dialog initiates.

Explanation

When a router boots up, it performs a series of steps, called the boot sequence, to test the hardware and load the necessary software. The boot sequence consists of the following steps:

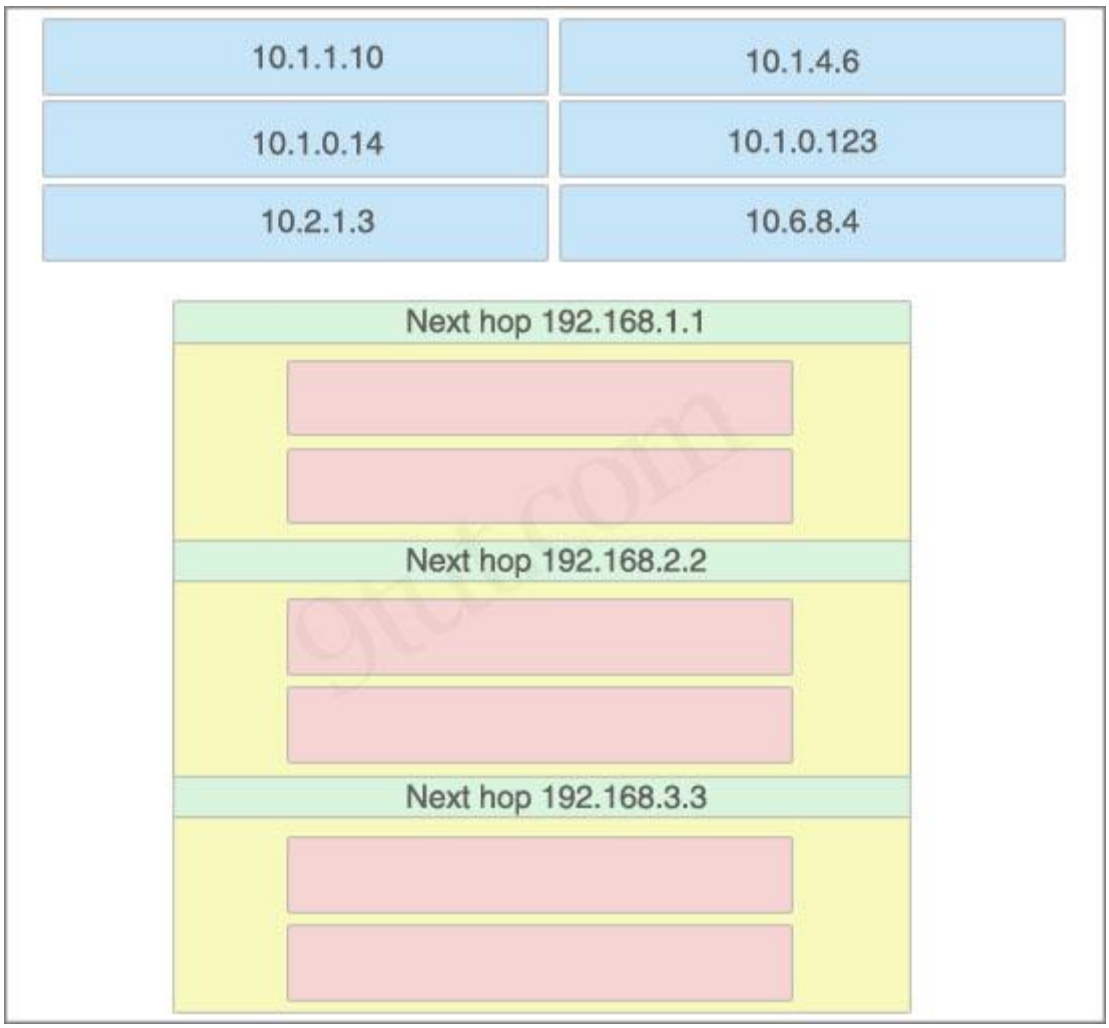
1) Power on self test (POST): tests the hardware to verify that all components of the device are operational and present.
2) The bootstrap loader in ROM executes: The bootstrap loader is a program in ROM that is used to find where a valid Cisco IOS image is located.
3) If a valid Cisco IOS image is located, it is loaded.
4) IOS loads configuration file. Once the IOS image is loaded, it will search for a valid startup configuration in NVRAM.
5) If a valid startup configuration file cannot be found, the router will load the System Configuration Dialog (sometimes called setup mode). This mode allows you to perform the initial configuration of the router.

Question 5

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

Routing has been configured on the local router with these commands:
Local(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.1
Local(config)# ip route 10.1.0.0 255.255.255.0 192.168.2.2
Local(config)# ip route 10.1.0.0 255.255.0.0 192.168.3.3

Drag each destination IP address on the top to its correct next hop address at the bottom.



Answer:

Next hop 192.168.1.1:
+ 10.2.1.3
+ 10.6.8.4

Next hop 192.168.2.2:
+ 10.1.0.14
+ 10.1.0.123

Next hop 192.168.3.3:
+ 10.1.1.10
+ 10.1.4.6

Explanation

If we have many entries matching for next hop ip address then the router will choose the one with most specific path to send the packet. This is called the "longest match" rule, the route with the most bits in the mask set to "1" will be chosen to route packet.

For example, the destination IP address of 10.1.0.14 will match two "ip route" commands:

ip route 10.1.0.0 255.255.255.0 192.168.2.2
ip route 10.1.0.0 255.255.0.0 192.168.3.3

But the first command is more specific (10.1.0.0/24 is more specific than 10.1.0.0/16) so the packet will be routed to 192.168.2.2.

Note: The IP address 10.1.1.10 only matches the second command "ip route 10.1.0.0 255.255.0.0 192.168.3.3″. It does not match the command "ip route 10.1.0.0 255.255.255.0 192.168.2.2″ because the third octet is different (10.1.**1**.10 is different from 10.1.**0**.0/24).

Question 6

If a Cisco router has learned about network 10.1.1.0 from multiple sources, the router will select and install only one entry into the routing table. Indicate the order of preference that the router will use by dragging the routes on the left to the order of preference category on the right.

Answer:

1) **First preference:** S 10.1.1.0 is directly connected, Serial1
2) **Second preference**: S 10.1 1.0/24 [1/0] via 10.1.2.2
3) **Third preference:** D 10.1.1.0/24 [90/2172416] via 10.1.5.5, Serial0
4) **Fourth preference:** O 10.1.1.0/24 [110/789] via 10.1.3.1, Serial0
5) **Fifth preference:** R 10.1.1.0/24 [120/3] via 10.1.3.1, Serial0

Explanation

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. It is a measure of the trustworthiness of the source of the routing information. The smaller the administrative distance value, the more reliable the protocol.

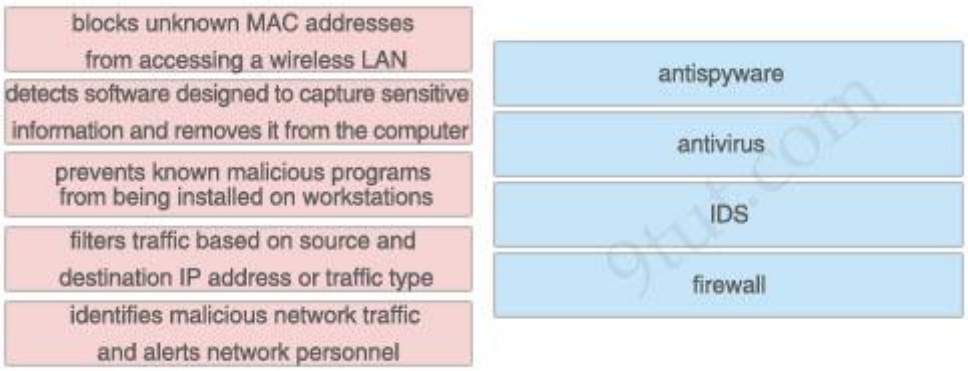
In this question, notice that the destination of all routes is 10.1.1.0/24 so we need to use Administrative distance of each routing protocol to specify the priority of each route. Below lists the Administrative Distance default values of popular routing protocols:

+ Directly connected: 0
+ Static route: 1
+ EIGRP (symbolize by "D"): 90
+ OSPF (symbolize by "O"): 110
+ RIP (symbolize by "R"): 120

CCNA – Drag and Drop 4

Question 1

Drag the function on the left to the matching security appliance or application on the right. (Not all functions are used)

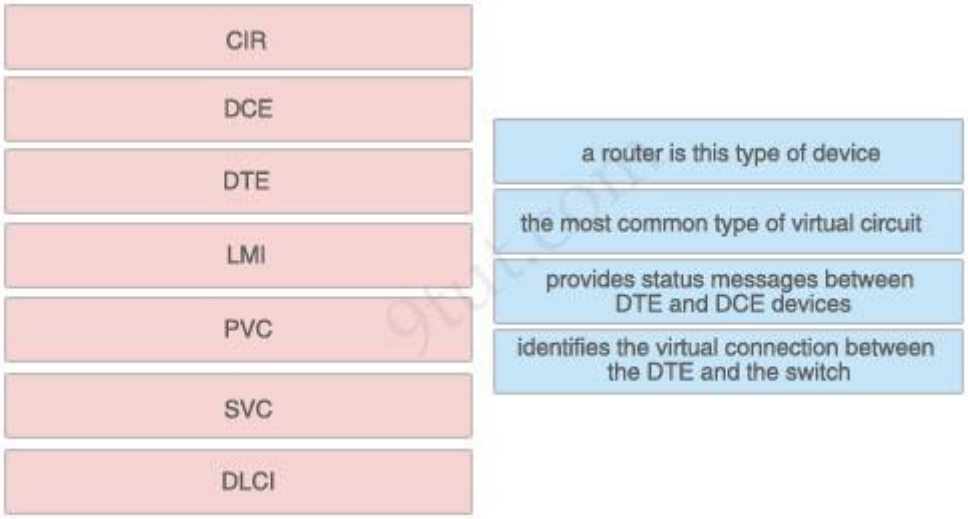


Answer:

1) antispyware: detects software designed to capture sensitive information and removes it from the computer
2) antivirus: prevents known malicious programs from being installed on workstations
3) IDS: identifies malicious network traffic and alerts network personnel
4) firewall: filters traffic based on source and destination IP address or traffic type

Question 2

Drag the Frame Relay acronym on the left to match its definition on the right. (Not all acronyms are used)

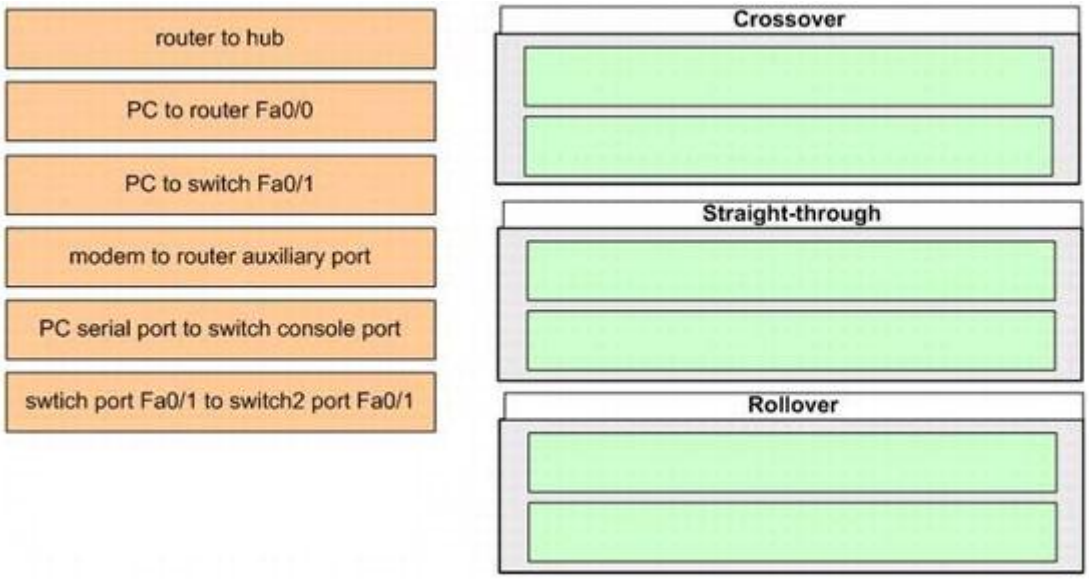


Answer:

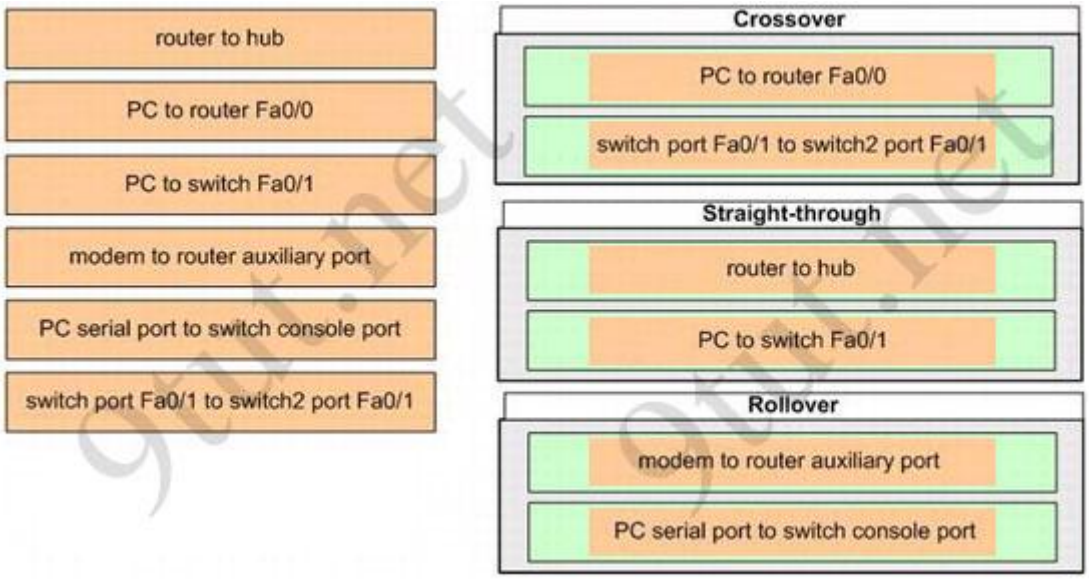
1) a router is this type of device: DTE
2) the most common type of virtual circuit: PVC
3) provides status messages between DTE and DCE devices: LMI
4) identifies the virtual connection between the DTE and the switch: DLCI

Question 3

The left describes some types of connections while the right describes some types of cables. Drag the items on the left to the proper locations.



Answer:



Explanation:

To specify when we use crossover cable or straight-through cable, we should remember:
Group 1: Router, Host(PC), 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**

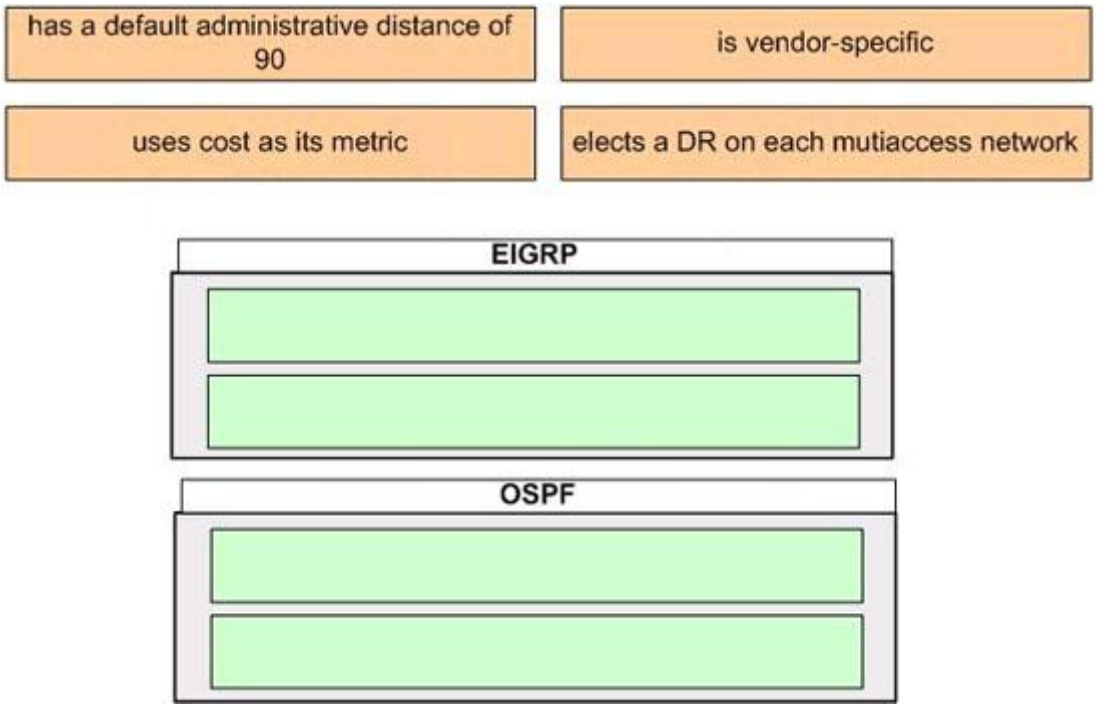
For example: we use straight-through cable to connect switch to router, switch to host, hub to host, hub to server… and we use crossover cable to connect switch to switch, switch to hub, router to router, host to host…).

+ We can connect a modem to router auxiliary port using a rollover cable. Recall that the purpose of the router's auxiliary port is for connecting to a modem and most Cisco routers have a second port on the back called the auxiliary port. We can use this port in case of a far-away router goes down, the administrator can have someone in the area go to the router, plug in a modem and access to the router remotely (if using the console port, we have to go to the site to work with that router).

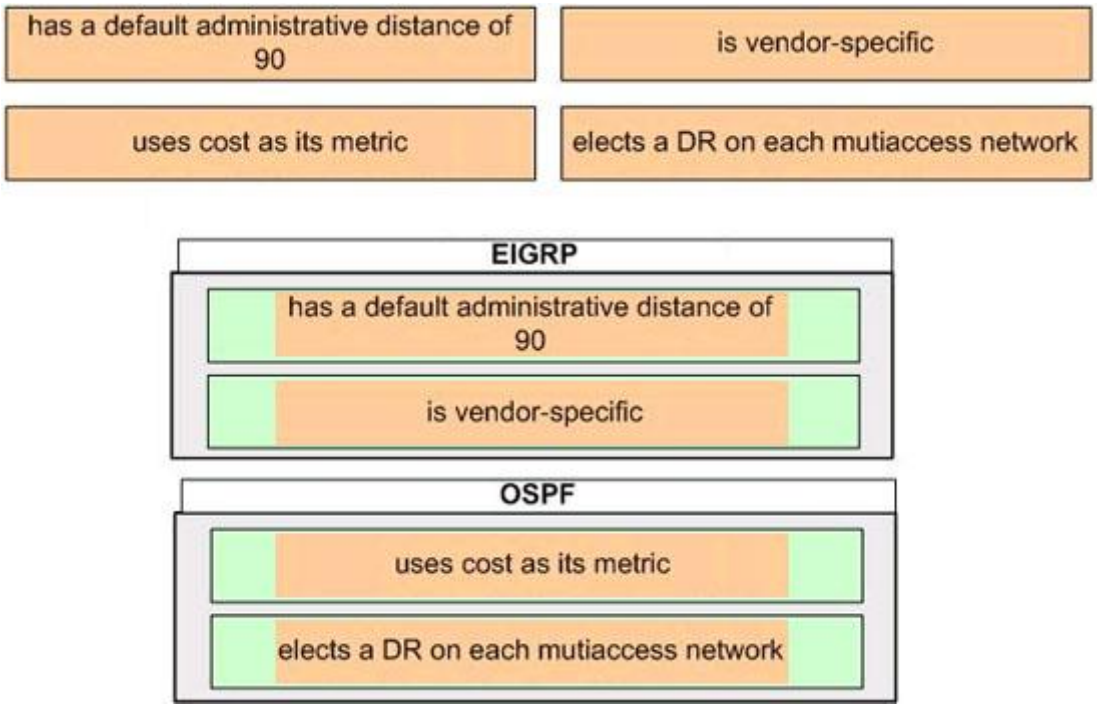
+ We can connect a PC serial port to a switch/router console port through the RJ-45 to DB-9 or RJ-45 to DB-25 adapter (at the PC end), depending on the computer.

Question 4

The above provides some descriptions, while the below provides some routing protocols. Drag the above items to the proper locations.



Answer:



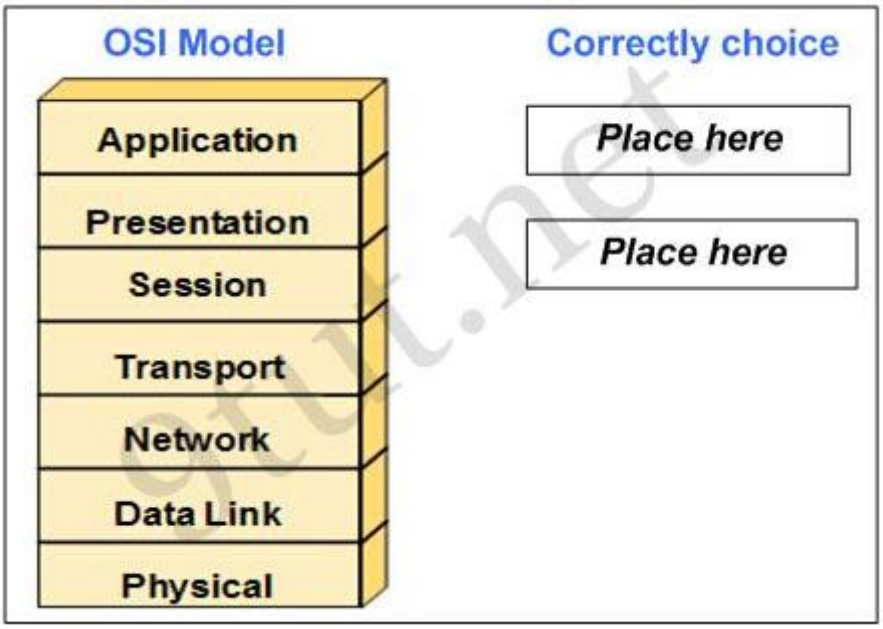
Explanation:

Enhanced Interior Gateway Routing Protocol (EIGRP) is a Cisco proprietary routing protocol, so it is vendor-specific. By default, EIGRP internal routes have an administrative distance value of 90.

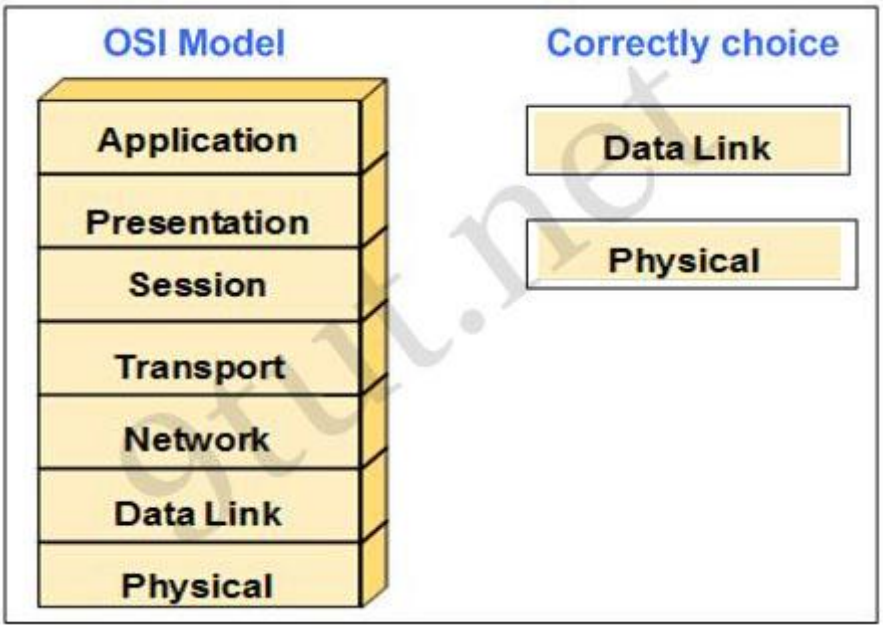
OSPF uses cost as its metric. By default, the cost of an interface is calculated based on bandwidth with the formula cost= 10000 0000/bandwith (in bps). OSPF elects a DR on each broadcast and nonbroadcast multiaccess networks (like Ethernet and Frame Relay environments, respectively). It doesn't elect a DR on point-to-point link (like a serial WAN).

Question 5

As a CCNA candidate, you are required to have a firm understanding of the OSI model. At which layers of the OSI model do Wide Area Networks operate in? Please drag the items to the proper locations.



Answer:



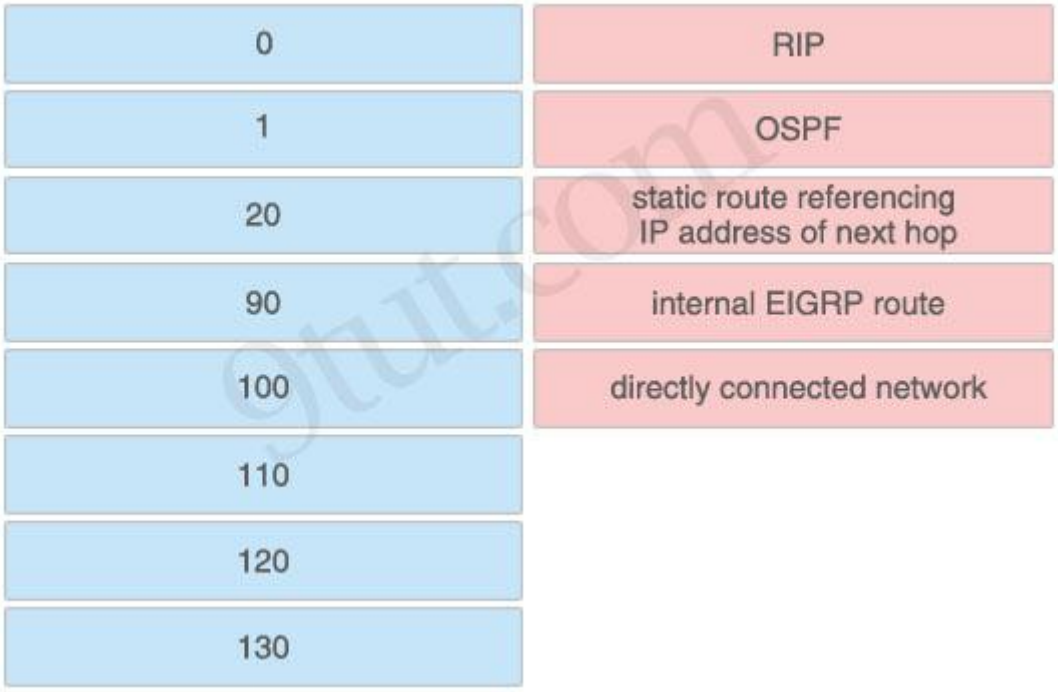
Explanation

WAN operates in the two lowest layers which are Data Link and Physical layers.

CCNA – Drag and Drop 5

Question 1

Drag the Cisco default administrative distance to the appropriate routing protocol or route (Not all options are used)

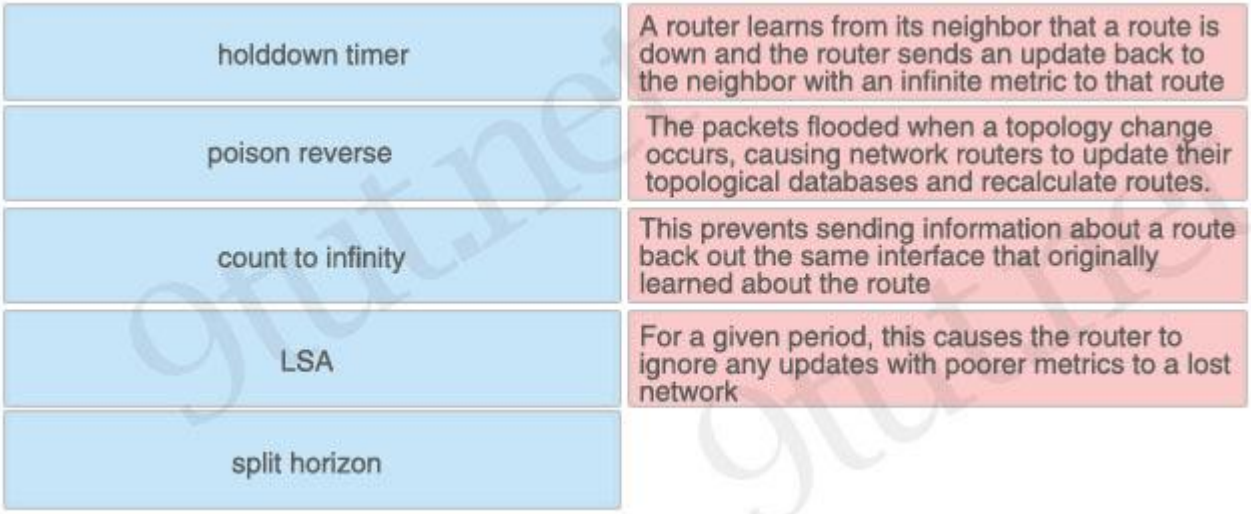


Answer:

+ RIP: 120
+ OSPF: 110
+ static route referencing IP address of next hop: 1
+ internal EIGRP route: 90
+ directly connected network: 0

Question 2

Drag the term on the left to its definition on the right (not all options are used)



Answer:

+ **poison reverse**: A router learns from its neighbor that a route is down and the router sends an update back to the neighbor with an infinite metric to that route
+ **LSA**: The packets flooded when a topology change occurs, causing network routers to update their topological databases and recalculate routes
+ **split horizon**: This prevents sending information about a routeback out the same interface that originally learned about the route
+ **holddown timer**: For a given period, this causes the router to ignore any updates with poorer metrics to a lost network

Question 3

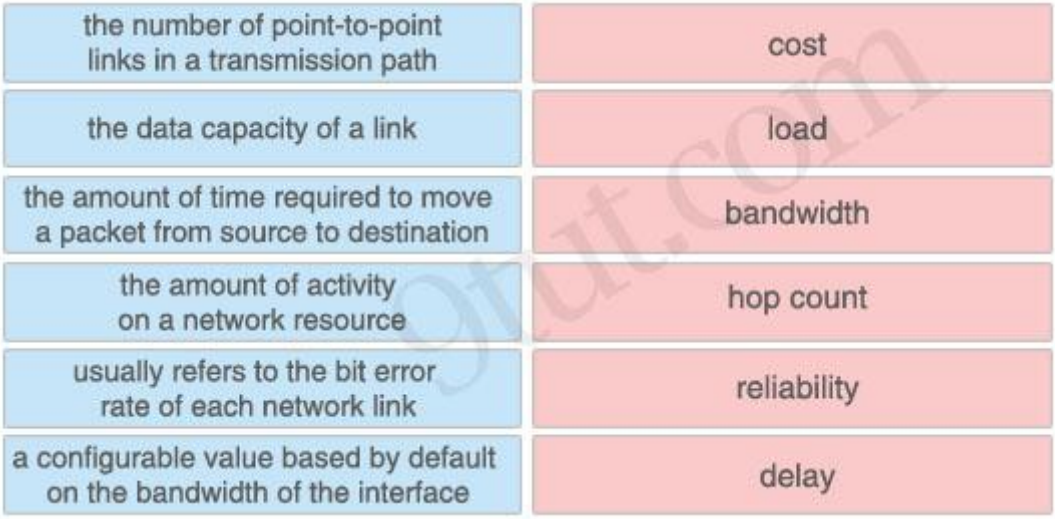
Drag the description on the left to the correct router mode on the right

Answer:

+ user EXEC mode: limited to basic monitoring commands
+ privileged EXEC mode: provide access to all other router commands
+ global configuration mode: commands that affect the entire system
+ specific configuration mode: commands that affect interfaces/processes only
+ setup mode: interactive configuration dialog

Question 4

Drag each definition on the left to the matching term on the right

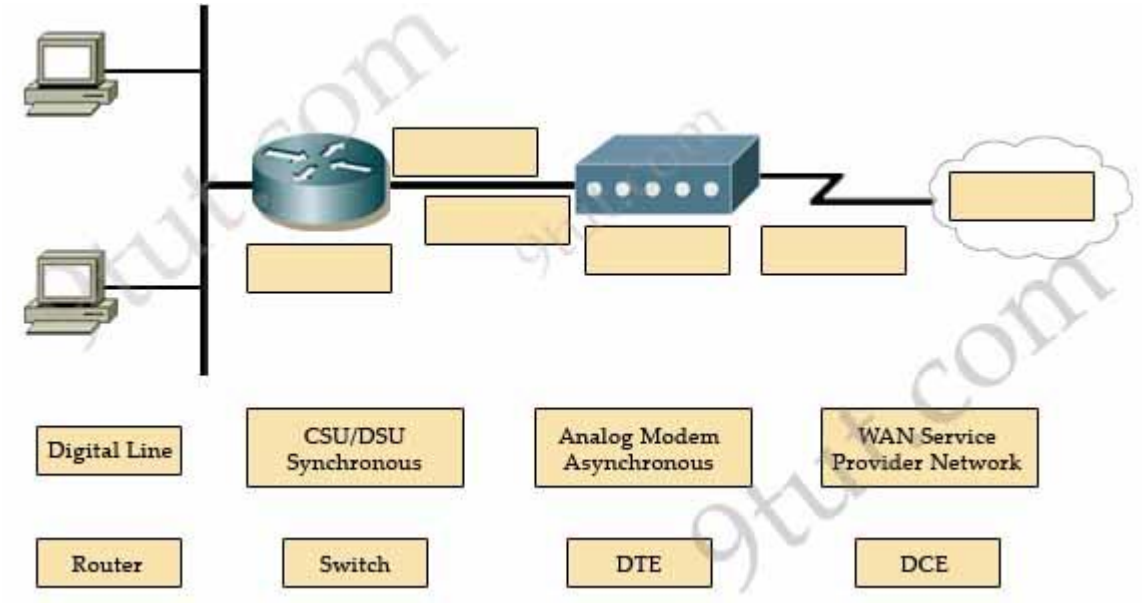


Answer:

+ cost: a configurable value based by default on the bandwidth of the interface
+ load: the amount of activity on a network resource
+ bandwidth: the data capacity of a link
+ hop count: the number of point-to-point links in a transmission path
+ reliability: usually refers to the bit error rate of each network link
+ delay: the amount of time required to move a packet from source to destination

Question 5

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



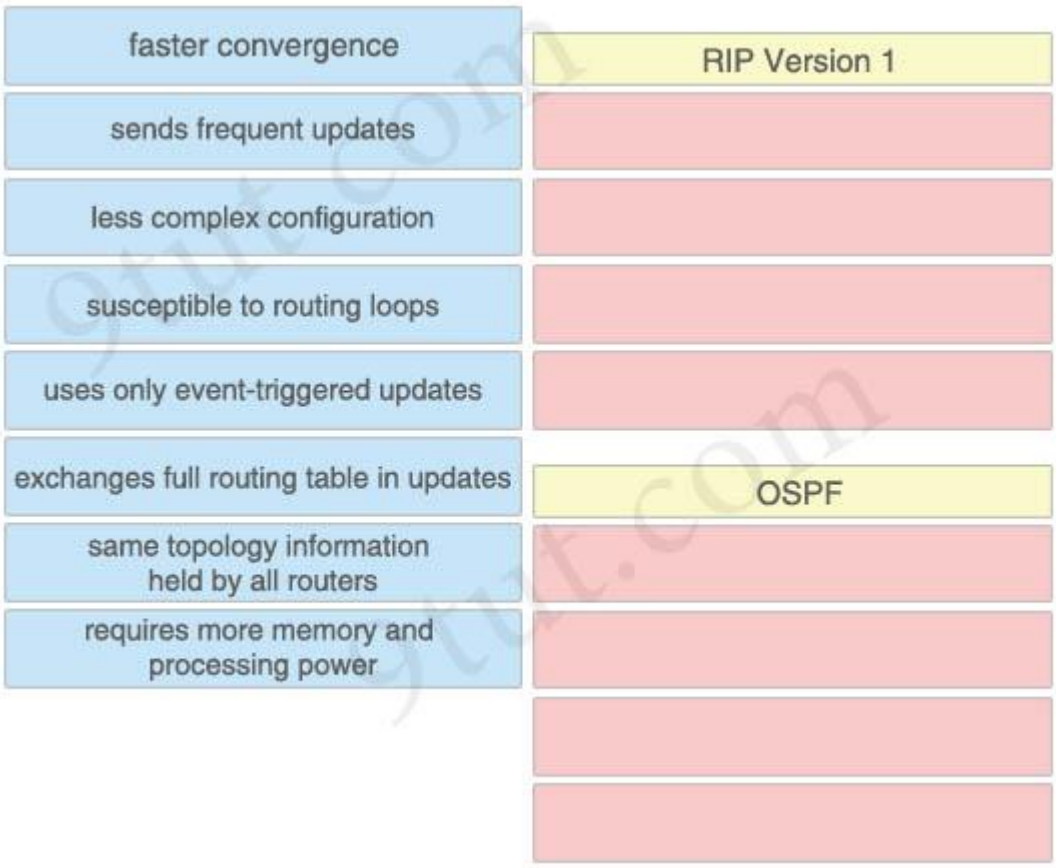
Answer:

From left to right:

Router, DTE, DCE, CSU/DSU Synchronous, Digital Line, WAN Service Provider Network.

Question 6

Drag each feature on the left to the appropriate routing protocol on the right.



Answer:

RIP version 1

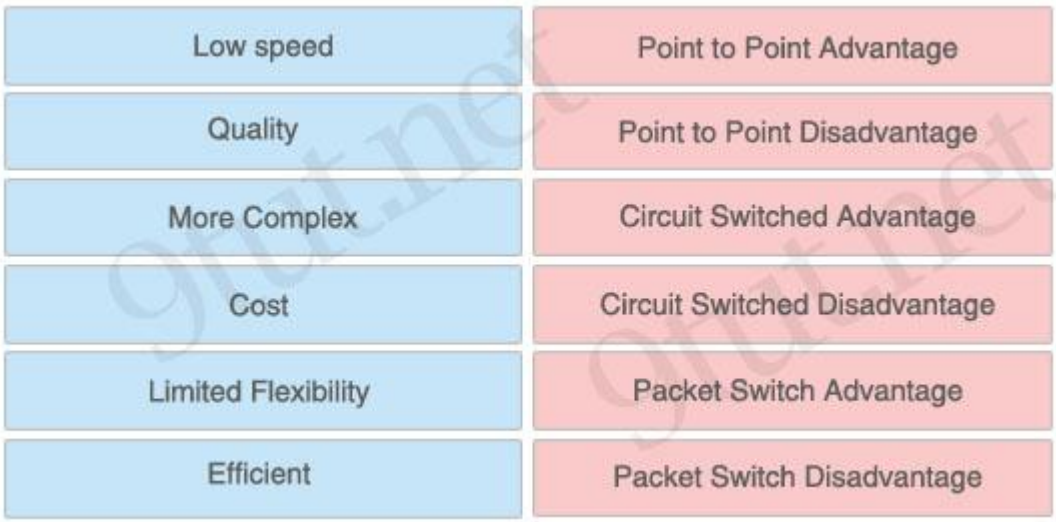
+ sends frequent updates
+ less complex configuration
+ susceptible to routing loops
+ exchanges full routing table in updates

OSPF:

+ faster convergence
+ uses only event-triggered updates
+ same topology information held by all routers
+ requires more memory and processing power

Question 7

Drag item on left to match item on right



Answer:

+ Point to Point Advantage: Quality
+ Point to Point Disadvantage: Limited Flexibility
+ Circuit Switched Advantage: Cost
+ Circuit Switched Disadvantage: Low speed
+ Packet Switch Advantage: Efficient
+ Packet Switch Disadvantage: More Complex

Question 8

All hosts in the same subnet with 172.16.5.118/26 must be denied Telnet access to hosts outside the LAN (u need to just drag & drop) fill out the command. To complete the bracketed command, [**access-list** *list-number* **deny tcp 172.16.5.***address* **0.0.0.***mask* **any eq** *port*], drag each appropriate option on the left to its proper placeholder on the right. (Not all options are used)

Answer:

+ list-number: 128
+ address: 64
+ mask: 63
+ port: 23

Explanation

In this case we want to filter port number so we have to use extended access-list so the list-number of our access-list must be from 100 to 199 -> We can choose **128**. We need to find the range of the subnet 172.16.5.118/26:

Increment: 64 (/26 = 1111 1111. 1111 1111. 1111 11111. 1**1**00 0000)
Network address: **172.16.5.64**
The corresponding wildcard mask for /26 is 0.0.0.**63** (because 63 = 0011 1111)

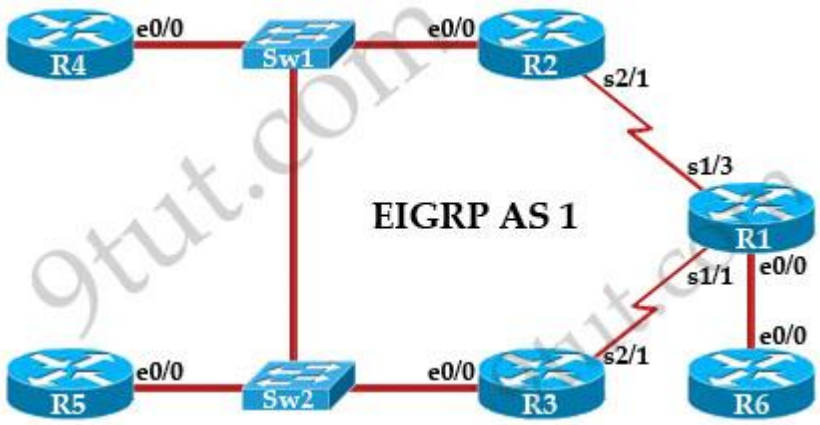
The port of Telnet access is **23** (and Telnet uses TCP). It is a well-known port that you must remember.

Therefore the full command to deny Telnet access to hosts outside the LAN 172.16.5.64 is:
access-list 128 deny tcp 172.16.5.64 0.0.0.63 any eq 23

EIGRP Troubleshooting Sim

Question

The topology below is running EIGRP. You are required to troubleshoot and resolve the EIGRP issues between the various routers. Use the appropriate show commands to troubleshoot the issues.



Instead of posting the output of "show run" commands we post here the commands entered on each router to reduce some useless lines. Also you can try solving questions by yourself before reading the answers.

R1:
int lo0
ip address 10.1.1.1
255.255.255.255
int e0/0
ip address 192.168.16.1
255.255.255.0
int s1/1
ip address 192.168.13.1
255.255.255.0
bandwidth 1000
int s1/3
ip address 192.168.12.1
255.255.255.0
!
router eigrp 1
network 192.168.12.0
network 192.168.13.0
network 192.168.16.0

R2:
int lo0
ip address 10.2.2.2
255.255.255.255
int e0/0
ip address 192.168.123.2
255.255.255.0
int s2/1
ip address 192.168.12.2
255.255.255.0
!
router eigrp 1
network 10.2.2.2 0.0.0.0
network 192.168.12.0
network 192.168.123.0

R3:
int lo0
ip address 10.3.3.3
255.255.255.255
int e0/0
ip address 192.168.123.3
255.255.255.0
int s2/1
ip address 192.168.13.3
255.255.255.0
!
router eigrp 1
network 10.3.3.3 0.0.0.0
network 192.168.13.0
network 192.168.123.0

R4:
int lo0
ip address 10.4.4.4

R5:
int lo0
ip address 10.5.5.5

R6:
int lo0
ip address 10.6.6.6

```
255.255.255.255
int lo1
ip address 10.4.4.5
255.255.255.255
int lo2
ip address 10.4.4.6
255.255.255.255
int e0/0
ip address 192.168.123.4
255.255.255.0
!
router eigrp 2
network 10.4.4.4 0.0.0.0
network 10.4.4.5 0.0.0.0
network 10.4.4.6 0.0.0.0
network 192.168.123.0
```

```
255.255.255.255
int lo1
ip address 10.5.5.55
255.255.255.255
int e0/0
ip address 192.168.123.5
255.255.255.0
!
router eigrp 1
network 10.5.5.5 0.0.0.0
network 10.5.5.55 0.0.0.0
network 10.10.10.0 0.0.0.255
network 192.168.123.0
```

```
255.255.255.255
int e0/0
ip address 192.168.16.6
255.255.255.0
!
router eigrp 1
network 10.6.6.6 0.0.0.0
```

Note: In the exam, this sim uses IOS version 15 so "no auto-summary" is the default setting of EIGRP. You don't have to type it.

You can download the pkt file to practice here:
http://www.9tut.com/download/9tut.com_CCNA_EIGRP_Troubleshooting_Sim.pkt

Question 1

After checking the routing table of R5, the administrator noticed that the two loopback interfaces on R4 (10.4.4.4/32 & 10.4.4.5/32) are not showing. Why are they missing?

A. The two loopback interfaces are shutdown.
B. By default, automatic summarization is enabled, so only the 10.0.0.0 network is shown.
C. R4 has been incorrectly configured to be in another AS, so it does not peer with R5.
D. The 'network' command is missing in the configuration of R4 so the loopback addresses haven't been advertised.

Answer: C

Explanation

On R4 we see EIGRP is configured with AS 2 (router eigrp 2) while other routers are using AS 1 (router eigrp 1). Therefore R4 cannot see other routers and vice versa.

Question 2

A user on R1 want to send data to R5. Which path are the packets sent?

A. Packets from R1 to R5 will go through R2.
B. Packets from R1 to R5 will go through R3.
C. Packets are equally load-balanced over R2 and R3.
D. Packets are unequally load-balanced over R2 and R3.

Answer: A

Explanation

For this question we have to check the routing table of R1 to find out the answer. Use the "show ip route" command on R1 we will get something like this:

```
R1#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

Gateway of last resort is not set

     10.0.0.0/32 is subnetted, 5 subnets
C       10.1.1.1 is directly connected, Loopback0
D       10.2.2.2 [90/2297856] via 192.168.12.2, 00:17:44, Serial1/3
D       10.3.3.3 [90/2298880] via 192.168.13.3, 00:00:04, Serial1/1
D       10.5.5.5 [90/2300416] via 192.168.12.2, 00:17:44, Serial1/3
D       10.5.5.55 [90/2300416] via 192.168.12.2, 00:17:44, Serial1/3
C    192.168.12.0/24 is directly connected, Serial1/3
C    192.168.13.0/24 is directly connected, Serial1/1
C    192.168.16.0/24 is directly connected, Ethernet0/0
D    192.168.123.0/24 [90/2172416] via 192.168.12.2, 00:17:44, Serial1/3
```

There are three interfaces on R5 which are Loopback0: 10.5.5.5 ; Loopback1: 10.5.5.55; Ethernet0/0: 192.168.123.5 and all of them are advertised via 192.168.12.2 so we can conclude traffic from R1 to R5 goes through R2 (192.168.12.2 is the IP address of S2/1 interface of R2).

Note: Maybe there is another version of this question in the exam in which the answer should be "The traffic is equally load-balanced over R2 and R3″. Therefore please check the "show ip route" output carefully to see if there are more than one route to the destination.

Question 3

R1 does not form EIGRP neighbor relationship with R6. What is the problem?

A. K values are mismatched.
B. The AS does not match.
C. The network command is missing.
D. The passive-interface command is enabled.

Answer: C

Explanation

From the configuration of R6 we learn that R6 is missing "network 192.168.16.0″ command (the network between R1 & R6) under EIGRP so EIGRP neighbor relationship will not be formed between them.

Question 4

Refer to the following output on R1:

```
R1#ping 10.5.5.55 source 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.5.55, timeout is 2 seconds:
Packet sent with a source address of 10.1.1.1
. . . . .
Success rate is 0 percent (0/5)
```

Why are the pings failing?

A. The network statement is missing on R5.
B. The loopback interface on R5 is shut down.
C. R1 is missing a network statement.
D. Incorrect IP address configured on the Loopback 1 interface on R5.

Answer: C

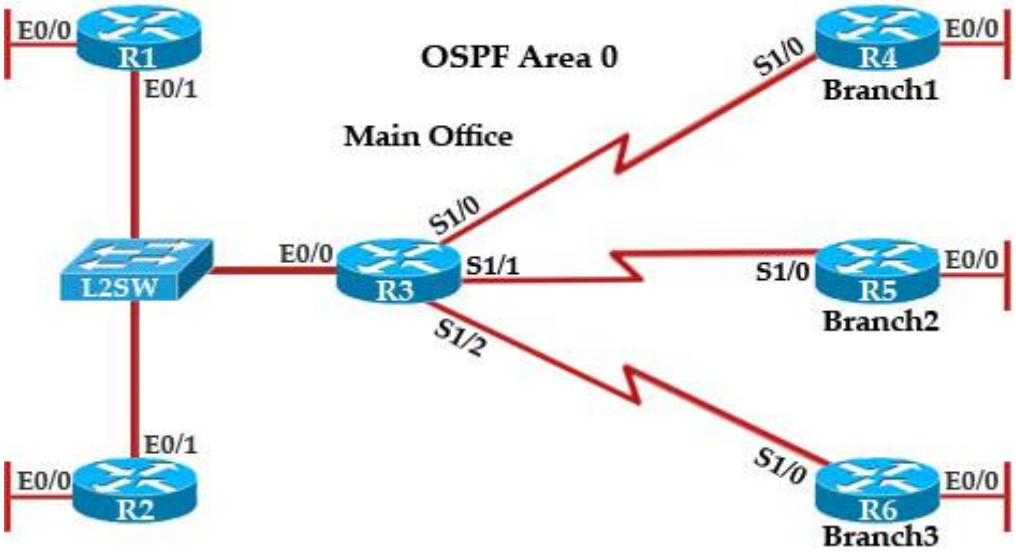
Explanation

R1 does not advertise its loopback 0 (10.1.1.1) to EIGRP therefore a ping to destination 10.5.5.55 (R5) from 10.1.1.1 will not be successful because R5 does not know how to reply to R1.

OSPF Neighbor Sim

Question

The topology below is running OSPF. You are required to troubleshoot and resolve the OSPF issues between the various routers. Use the appropriate show commands to troubleshoot the issues.



Instead of posting the output of "show run" commands we post here the commands entered on each router to reduce some useless lines. Also you can try solving questions by yourself before reading the answers.

R1	R2	R3
interface Loopback0 description ***Loopback*** ip address 192.168.1.1 255.255.255.255 ip ospf 1 area 0 ! interface Ethernet0/0 description **Connected to R1-LAN** ip address 10.10.110.1 255.255.255.0 ip ospf 1 area 0 ! interface Ethernet0/1 description **Connected to L2SW** ip address 10.10.230.1	! interface Loopback0 description **Loopback** ip address 192.168.2.2 255.255.255.255 ip ospf 2 area 0 ! interface Ethernet0/0 description **Connected to R2-LAN** ip address 10.10.120.1 255.255.255.0 ip ospf 2 area 0 ! interface Ethernet0/1 description **Connected to L2SW**	username R6 password CISCO36 ! interface Loopback0 description **Loopback** ip address 192.168.3.3 255.255.255.255 ip ospf 3 area 0 ! interface Ethernet0/0 description **Connected to L2SW** ip address 10.10.230.3 255.255.255.0 ip ospf 3 area 0 ! interface Serial1/0

255.255.255.0 ip ospf hello-interval 25 ip ospf 1 area 0 ! router ospf 1 log-adjacency-changes	ip address 10.10.230.2 255.255.255.0 ip ospf 2 area 0 ! router ospf 2 log-adjacency-changes	description **Connected to R4-Branch1 office** ip address 10.10.240.1 255.255.255.252 encapsulation ppp ip ospf 3 area 0 ! interface Serial1/1 description **Connected to R5-Branch2 office** ip address 10.10.240.5 255.255.255.252 encapsulation ppp ip ospf hello-interval 50 ip ospf 3 area 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 ! router ospf 3 router-id 192.168.3.3 !
R4 ! interface Loopback0 description **Loopback** ip address 192.168.4.4 255.255.255.255 ip ospf 4 area 2 ! interface Ethernet0/0 ip address 172.16.113.1 255.255.255.0 ip ospf 4 area 2 ! interface Serial1/0 description **Connected to R3-Main Branch office** ip address 10.10.240.2 255.255.255.252 encapsulation ppp ip ospf 4 area 2 !	R5 ! interface Loopback0 description **Loopback** ip address 192.168.5.5 255.255.255.255 ip ospf 5 area 0 ! interface Ethernet0/0 ip address 172.16.114.1 255.255.255.0 ip ospf 5 area 0 ! interface Serial1/0 description **Connected to R3-Main Branch office** ip address 10.10.240.6 255.255.255.252 encapsulation ppp ip ospf 5 area 0 !	R6 username R3 password CISCO36 ! interface Loopback0 description **Loopback** ip address 192.168.6.6 255.255.255.255 ip ospf 6 area 0 ! interface Ethernet0/0 ip address 172.16.115.1 255.255.255.0 ip ospf 6 area 0 ! interface Serial1/0 description **Connected to R3-Main Branch office** ip address 10.10.240.10 255.255.255.252 encapsulation ppp

router ospf 4 log-adjacency-changes	router ospf 5 log-adjacency-changes	ip ospf 6 area 0 ppp authentication chap ! router ospf 6 router-id 192.168.3.3 !

Note: Packet Tracer does not support enabling OSPF under interface mode (ip ospf 3 area 0). We don't know why such a popular command is not supported so we can't make a pkt file for this lab.

Question 1

R3 and R4 cannot form an OSPF neighborship. What is the problem?

A. The area IDs of R3 and R4 are mismatched
B. The Layer 2 encapsulation of the serial links is mismatched
C. The OSPF hello and dead interval are mismatched
D. The router ID of R3 is configured on R4

Answer: A

Explanation

We learned it is a OSPF problem so we should check the interfaces between them first. On both R3 and R4 use "show running-config" command to check their S1/0 interfaces

```
R3#show running-config
<<output omitted>>
!
interface Serial1/0
  description **Connected to R4-Branch1 office**
  ip address 10.10.240.1 255.255.255.252
  encapsulation ppp
  ip ospf 3 area 0
!
<<output omitted>>
```

```
R4#show running-config
<<output omitted>>
!
interface Serial1/0
  description **Connected to R3-Main Branch office**
  ip address 10.10.240.2 255.255.255.252
  encapsulation ppp
  ip ospf 4 area 2
!
<<output omitted>>
```

In the output above we see their Area IDs are mismatched; interface S1/0 of R3 is in area 0 (R3: **ip ospf 3 area 0**) while interface s1/0 of R4 is in area 2 (R4: **ip ospf 4 area 2**).

Question 2

R3 and R5 cannot form an OSPF neighborship. What is the problem?

A. The area IDs of R3 and R5 are mismatched
B. The Layer 2 encapsulation of the serial links is mismatched
C. The OSPF hello and dead interval are mismatched
D. The router ID of R3 is configured on R5

Answer: C

Explanation

Continue checking their connected interfaces with the "show running-config" command:

```
R3#show running-config
<<output omitted>>
!
interface Serial1/1
  description **Connected to R5-Branch2 office**
  ip address 10.10.240.5 255.255.255.252
  encapsulation ppp
  ip ospf hello-interval 50
  ip ospf 3 area 0
!
<<output omitted>>
```

```
R5#show running-config
<<output omitted>>
!
interface Serial1/0
  description **Connected to R3-Main Branch office**
  ip address 10.10.240.6 255.255.255.252
  encapsulation ppp
  ip ospf 5 area 0
!
<<output omitted>>
```

The only difference we can see here is the line "ip ospf hello-interval 50″ on R3. This command sets the number of seconds R3 waits before sending the next hello packet out this interface. In this case after configuring this command, R3 will send hello packets to R5 every 50 seconds. But the default value of hello-interval is 10 seconds and R5 is using it. Therefore we can think of a hello interval mismatch problem here. You can verify with the "show ip ospf interface <interface>" command on each router.

```
R3#sh ip ospf int s1/1
Serial1/1 is up, line protocol is up
  Internet Address 10.10.240.5/30, Area 0
  Process ID 3, Router ID 192.168.3.3, Network Type POINT_TO_POINT, Cost: 64
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 50, Dead 200, Wait 200, Retransmit 5
  oob-resync timeout 200
  Hello due in 00:00:28
  Supports Link-local Signaling (LLS)
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

```
R5#sh ip ospf int s1/0
Serial1/0 is up, line protocol is up
  Internet Address 10.10.240.6/30, Area 0
  Process ID 5, Router ID 10.10.240.6, Network Type POINT_TO_POINT, Cost: 64
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:04
  Supports Link-local Signaling (LLS)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

So we can see both hello and dead interval are mismatched because the dead interval always four times the value of hello interval, unless you manually configure the dead interval (with the **ip ospf dead-interval <seconds>** command).

Question 3

R1 and R2 cannot form an OSPF neighborship. What is the problem?

A. The area IDs of R1 and R2 are mismatched
B. Ethernet0/1 of R1 is configured with a non-default OSPF hello interval
C. The Layer 2 encapsulation of the serial links is mismatched
D. The OSPF hello and dead interval are mismatched

Answer: B

Explanation

Continue checking their connected interfaces with the "show running-config" command:

```
R1#show running-config
<<output omitted>>
!
interface Ethernet0/1
 description **Connected to L2SW**
 ip address 10.10.230.1 255.255.255.0
 ip ospf hello-interval 25
 ip ospf 1 area 0
!
<<output omitted>>
```

```
R2#show running-config
<<output omitted>>
!
interface Ethernet0/1
 description **Connected to L2SW**
 ip address 10.10.230.2 255.255.255.0
 ip ospf 2 area 0
!
<<output omitted>>
```

We see the hello interval on R1 is not the same as R2 (and you can verify with the "show ip ospf interface <interface> command") -> There is a hello and dead interval mismatch problem. We should configure "no ip ospf hello-interval 25″ on R1.

Note: Maybe there are some versions of this question in the exam. For example there are some reports saying that Ethernet0/1 on R1 is shutdown (and this is the correct choice in the exam). So please be careful checking the config on the routers before choosing the correct answers.

Question 4

R3 and R6 cannot form an OSPF neighborship. What is the problem?

A. The area IDs of R3 and R6 are mismatched
B. The Layer 2 encapsulation of the serial links is mismatched
C. The OSPF hello and dead interval are mismatched
D. The router ID of R3 is configured on R6

Answer: D

Explanation

```
R3#show running-config
```

```
<<output omitted>>
username R6 password CISCO36
!
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
!
<<output omitted>>
!
router ospf 3
 router-id 192.168.3.3
!
<<output omitted>>
```

```
R6#show running-config
<<output omitted>>
username R3 password CISCO36
!
interface Serial1/0
 description **Connected to R3-Main Branch office**
 ip address 10.10.240.10 255.255.255.252
 encapsulation ppp
 ip ospf 6 area 0
 ppp authentication chap
!
<<output omitted>>
!
router ospf 6
 router-id 192.168.3.3
!
<<output omitted>>
```

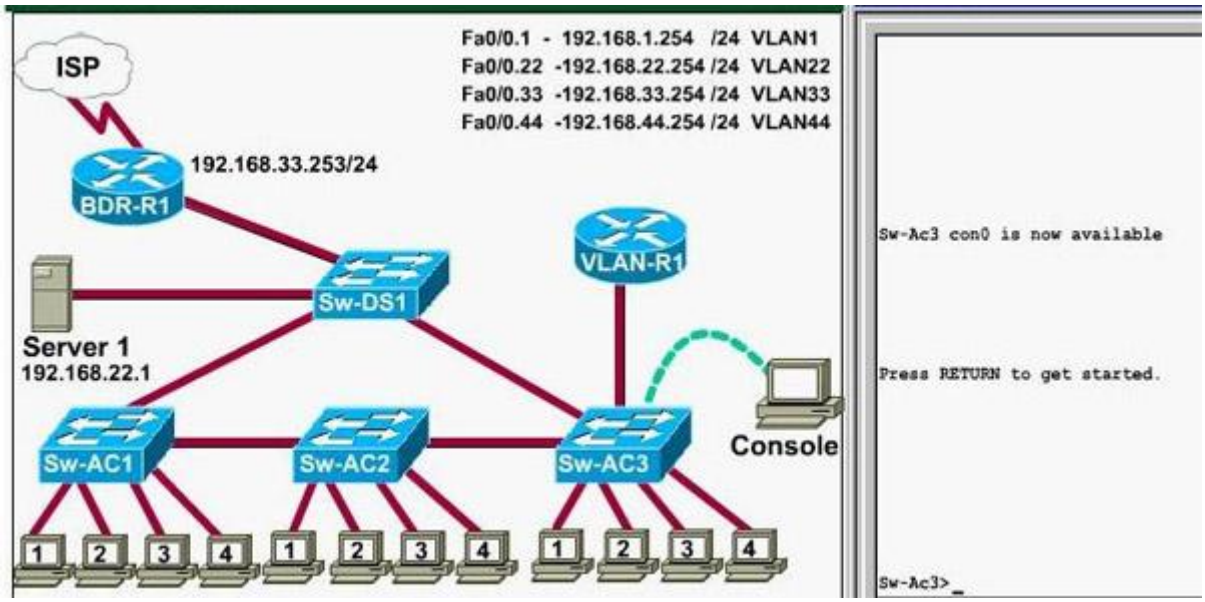
We are not sure about the configuration of ppp authentication in this case. Some reports said that only one router has the “ppp authentication chap” command but it is just a trick and is not the problem here. The real problem here is R6 uses the same router-id of R3 (192.168.3.3) so OSPF neighborship cannot be established. In real life, such configuration error will be shown in the command line interface (CLI). So please check carefully for this question.

CCNA VTP SIM Question

Question

This task requires you to use the CLI of Sw-AC3 to answer five multiple-choice questions. This does not require any configuration.

To answer the multiple-choice questions, click on the numbered boxes in the right panel.



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

Notice: All the images in this VTP LAB are used for demonstration only, you will see slightly different images in the real CCNA exam. You can download this sim to practice here (but notice that this sim is not perfect, only for practicing purpose):
http://www.9tut.com/download/9tut.com_CCNA_vtp_sim.pka

If you are not sure about VTP, please read my VTP Tutorial

Note: In this VTP sim, you have to answer 5 questions. After answering the first question, click on the number boxes to move to other questions. If you click “Next” at the first question, you will lose points for 4 remaining questions.

Question 1

What interface did Sw-AC3 associate with source MAC address 0010.5a0c.ffba ?

a) Fa0/1

b) Fa0/3

c) Fa0/6

d) Fa0/8

e) Fa0/9

f) Fa0/12

Answer: Fa 0/8

Explanation: to find out which interface associated with a given MAC address, use the show mac-address-table command. It shows the learned MAC addresses and their associated interfaces. After entering this command, you will see a MAC address table like this:

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

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    000f.2485.8900    STATIC      CPU
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0100.0cdd.dddd    STATIC      CPU
   1    0009.e8b2.c28c    DYNAMIC     Fa0/12
   1    000a.b7e9.8360    DYNAMIC     Fa0/3
   1    000f.2485.8b49    DYNAMIC     Fa0/9
  22    0009.e8b2.c28c    DYNAMIC     Fa0/12
  22    000a.b7e9.8360    DYNAMIC     Fa0/3
  22    0010.5a0c.ffba    DYNAMIC     Fa0/8
  33    0009.e8b2.c28c    DYNAMIC     Fa0/12
  33    000a.b7e9.8360    DYNAMIC     Fa0/3
  33    000c.ce8d.8860    DYNAMIC     Fa0/12
  33    0010.5a0c.fd86    DYNAMIC     Fa0/6
  33    0010.5a0c.feae    DYNAMIC     Fa0/12
  33    0010.5a0c.ff9f    DYNAMIC     Fa0/1
  44    0009.e8b2.c28c    DYNAMIC     Fa0/12
--More--
```

From this table we can figure out that the MAC address 0010.5a0c.ffba is associated with interface Fa0/8.

Note: There are some reports that the “show mac-address-table” command does not exist in the exam. So in the exam, if you cannot use the “show mac-address-table” command then try using the “show mac address-table” (without “-”) instead.

Question 2

What ports on Sw-AC3 are operating has trunks (choose three)?

a) Fa0/1

b) Fa0/3

c) Fa0/4

d) Fa0/6

e) Fa0/9

f) Fa0/12

Answer: Fa0/3, Fa0/9 and Fa0/12

Explanation: Use the show interface trunk command to determine the trunking status of a link and VLAN status. This command lists port, its mode, encapsulation and whether it is trunking. The image below shows how it works:

```
Sw-Ac3#show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/3       on           802.1q         trunking      1
Fa0/9       desirable    802.1q         trunking      1
Fa0/12      desirable    802.1q         trunking      1

Port      Vlans allowed on trunk
Fa0/9       1-4094
Fa0/12      1-4094

Port        Vlans allowed and active in management domain
Fa0/9       1
Fa0/12      1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/9       1
Fa0/12      1
Sw-Ac3#
```

(This image is used for demonstration only)

Question 3

What kind of router is VLAN-R1?

a) 1720

b) 1841

c) 2611

d) 2620

Answer: 2620

Explanation: VLAN-R1 is the router directly connected to Sw-Ac3 switch, so we can use the show cdp neighbors command to see:

1. Neighbor Device ID : The name of the neighbor device;

2. Local Interface : The interface to which this neighbor is heard

3. Capability: Capability of this neighboring device – R for router, S for switch, H for Host etc.

4. Platform: Which type of device the neighbor is

5. Port ID: The interface of the remote neighbor you receive CDP information

6. Holdtime: Decremental hold time in seconds

Sample output of *show cdp neighbors* command:

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

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

One thing I want to notice you is "Local Intrfce" in the image above refers to the local interface on the device you are running the "show cdp neighbors" command

Question 4

Which switch is the root bridge for VLAN 1?

Answer: Sw-DS1

Explanation: First we use the show spanning-tree vlan 1 to view the spanning-tree information of VLAN 1

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

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

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

From the "Cost 19″, we learn that the root switch is directly connected to the Sw-Ac3 switch over a 100Mbps Ethernet link

Notice that if you see all of the interface roles are Desg (designated) then you can confirm **Sw-Ac3** switch is the root bridge for this VLAN (VLAN 1).

If you see there is at least one Root port in the interface roles then you can confirm Sw-Ac3 is not the root bridge because root bridge does not have root port. In this case, we notice that the root port on Sw-Ac3 switch is FastEthernet0/12, so we have to figure out which switch is associated with this port -> it is the root bridge. You can verify it with the show cdp neighbors command:

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

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

The "Local Intrfce" column refers to the interface on the switch running "show cdp neighbors" command. In this case, Sw-DS1 is associated with interface FastEthernet0/12 -> **Sw-DS1** is the root bridge

Question 5

What address should be configured as the default-gateway for the host connected to interface fa 0/4 of SW-Ac3?

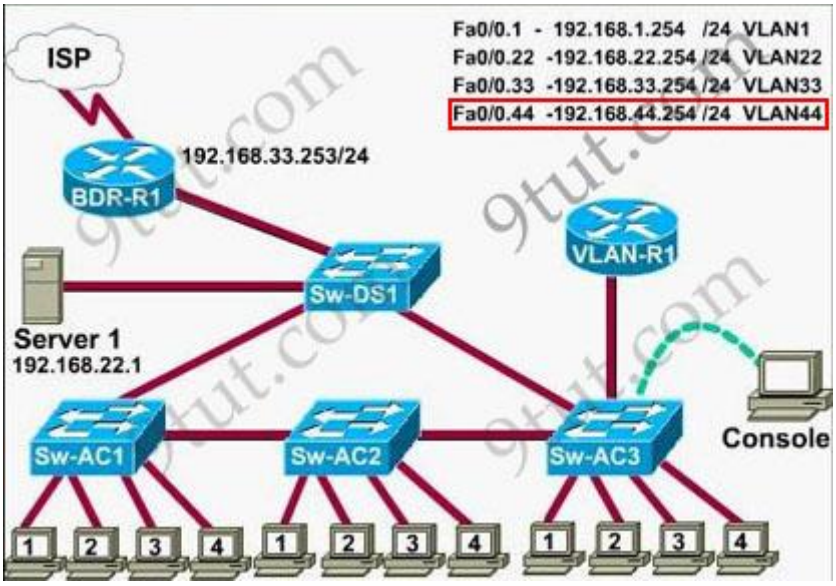
Answer: 192.168.44.254

Explanation:

First we have to identify which VLAN interface Fa0/4 belongs to by the show vlan command

```
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
```

From the exhibit we know that VLAN 44 is configured on router using sub-interface Fa0/0.44 with IP address 192.168.44.254/24



Therefore the default gateway of the host should be 192.168.44.254

Question 6

From which switch did Sw-Ac3 receive VLAN information ?

Answer: Sw-AC2

Explanation: to view the VTP configuration information, use the show vtp status command

```
Sw-Ac3#show vtp status
VTP Version : 2
Configuration Revision : 5
Maximum VLANs supported locally : 255
Number of existing VLANs : 7
VTP Operating Mode : Client
VTP Domain Name : home-office
VTP Pruning Mode : Enabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0x22 0x07 0xF2 0x3A 0xF1 0x28 0xA0 0x5D
Configuration last modified by 163.5.8.3 at 3-1-93 00:28:35
```

So we knew Sw-Ac3 received VLAN information from 163.5.8.3 (notice:the IP address may be different). Finally we use the show cdp neighbors detail to find out who 163.5.8.3 is:

```
Sw-Ac3#show cdp neighbor detail

<output omitted>
Device ID: Sw-AC2
Entry address(es):
IP address: 163.5.8.3
Platform: cisco 2950, Capabilities: Switch
Interface: FastEthernet, Port ID (outgoing port): FastEthernet Holdtime : 164 sec
Version :
<output omitted>
```

Question 7

Refer to the exibit, SwX was taken out of the production network for maintenance. It will be reconnected to the Fa 0/16 port of Sw-Ac3. What happens to the network when it is reconnected and a trunk exists between the two switches?

```
SwX#show vlan
VLAN Name  Status   Ports
---- ----- ------ -------------------------------
1    default    active  Fa0/1, Fa0/2, Fa0/3
                        Fa0/4, Fa0/5, Fa0/6
                        Fa0/7, Fa0/8, Fa0/9
                        Fa0/10, Fa0/11, Fa0/12
                        Gi0/1, Gi0/2
2    students   active
3    admin      active
4    faculty    active
```

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

A – All VLANs except the default VLAN will be removed from all switches

B – All existing switches will have the students, admin, faculty, Servers, Management, Production, and no-where VLANs

C – The VLANs Servers, Management, Production and no-where will replace the VLANs on SwX

D – The VLANs Servers, Management, Production and no-where will be removed from existing switches

Answer and **Explanation**:

First we should view the VTP configuration of switch Sw-Ac3 by using the show vtp status command on Sw-Ac3

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

Notice that its configuration revision number is **5** and VTP Domain Name is **home-office**

Next, from the exhibit we know that SwX has a revision number of 6, which is greater than that of Sw-Ac3 switch, and both of them have same VTP Domain Name called “home-office”.

```
SwX#show vlan
VLAN Name  Status   Ports
---- ----- ------ -------------------------------
1    default    active  Fa0/1, Fa0/2, Fa0/3
                        Fa0/4, Fa0/5, Fa0/6
                        Fa0/7, Fa0/8, Fa0/9
                        Fa0/10, Fa0/11, Fa0/12
                        Gi0/1, Gi0/2
2    students   active
3    admin      active
4    faculty    active
```

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

Therefore SwX will replace vlan information on other switches with its own information. We should check vlan information of Sw-Ac3 switch with show vlan command

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

So the correct answer is **D – The VLANs Servers, Management, Production and no-where will be removed from existing switches**

Please notice that in the real CCNA exam you may see a different configuration revision of Sw-Ac3 or of SwX. In general, which switch has a higher revision number it will become the updater and other switches will overwrite their current databases with the new information received from the updater (provided that they are on the same domain and that switch is not in transparent mode). In particular, **if the revision number of SwX is lower than that of Sw-Ac3, the answer should be "C – The VLANs Servers, Management, Production and no-where will replace the VLANs on SwX"**.

Also, some recent comments have said that the new switch's VTP Operating Mode is **Server** but the answer is still the same.

Note: If a switch is in client mode and has a higher Revision number, it can still update other Server switches (with lower Revision numbers).

Question 8

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

A – Fa0/8

B – Fa0/3

C – Fa0/1

D – Fa0/12

Answer: B C D

Explanation:

First we check to see which ports the source mac-address and the destination mac-address belong to by using show mac-address-table command

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

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

We notice that the source mac-address 0010.5a0c.fd86 is listed in the table and it belongs to Vlan 33 but we can't find the destination mac-address 000a.8a47.e612 in this table. In this case, the switch will flood to all ports of Vlan 33 and flood to all the trunk links, except the port it received this frame (port Fa0/6). Therefore from the output above, we can figure out it will flood this frame to **Fa0/1**, **Fa0/3** and **Fa0/12**.

Please notice that the "show mac-address-table" command just lists information that was learned by the switch, it means that there can be other ports besides Fa0/1, Fa0/3 and Fa0/12 belong to Vlan 33. You can use the show vlan command to see which ports belong to vlan 33

```
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
```

And we found other ports which belong to vlan 33, they are Fa0/2, Fa0/5 and Fa0/7. Our switch will flood the frame to these ports, too.

And we can check which trunk ports will receive this frame by the show interface trunk command

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

-> Port Fa0/9 will also receive this frame!

Note: Some reports said there is another version of this question. A reader on 9tut commented:

Another question on the VTP SIM was" What will be the destination MAC address of a packet with Source IP address 192.168.44.1 and destination IP address 192.0.2.X (doesn't really matter what will be the Dest. IP address, since it will be sent to the router).
The answer is simple:
Since the source IP address belongs to VLAN 44, the default gw of the sender is the Router's Subinterface 192.168.44.254, and this is where the packet will be sent. Thus, you need to perform a 'show cdp nei' on the Sw-AC3 in order to find the local FastEthernet port where the router is connected. Then execute a "show mac address-table" (this command was functioning) and find the mac address associated with the previous port. This is the answer.

Question 9

If one of the host connected to Sw-AC3 wants to send something for the ip 190.0.2.5 (or any ip that is not on the same subnet) what will be the destination MAC address?

Answer and **Explanation**:

Because the destination address is not on the same subnet with the switch, it will forward the packet to its default gateway. So we have to find out who is the default gateway of this switch by using the show running-config command

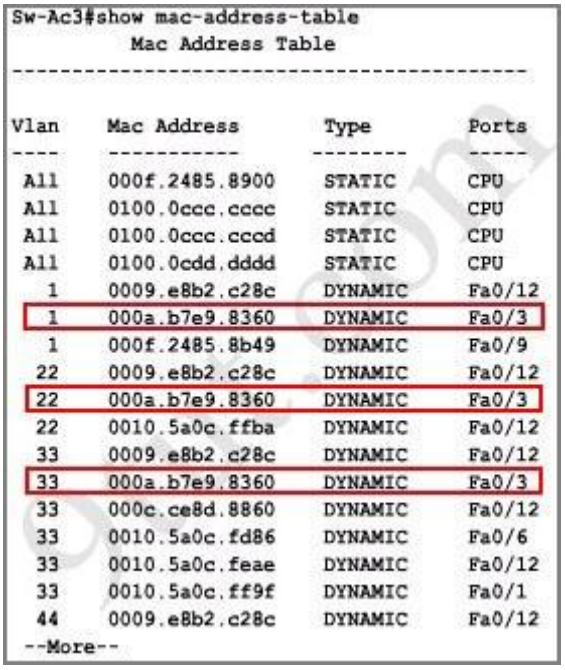
```
Sw-Ac3#show running-config
<ouput omitted>
!
ip http server
ip default-gateway 192.168.1.254
!
<output omitted>
```

From the output, we notice that its default-gateway is 192.168.1.254. In fact, we can easily guess that its default gateway should be a layer 3 device like a router; and in this case, the VLAN-R1 router. To verify our theory, use the show cdp neighbor detail command and focus on the description of VLAN-R1 router

```
Sw-Ac3#show cdp neighbor detail
<output omitted>
Device ID: VLAN-R1
Entry address(es):
IP address: 192.168.1.254
Platform: cisco 2620, Capabilities: Router
Interface: FastEthernet0/3 Port ID (outgoing port):FastEthernet0/0.1
Holdtime : 152 sec
Version :
Cisco Internetwork Operating System Software
IOS (tm) 3000 Software (IGS-J-L), Version 11.1(5),
RELEASE SOFTWARE (fc1)Copyright (c) 1986-1996 by cisco
Systems, Inc.Compiled Tue 05-Aug-03 11:48 by mkamson
```

From this output, we can confirm the switch's default gateway is VLAN-R1 router (with the IP address of 192.168.1.254). And "the interface: FastEthernet0/3″ tells us that the switch is connected to VLAN-R1 router through Fa0/3 port (Fa0/3 is the port on the switch).

Finally we just need to use the show mac-address-table command to find out which MAC address is associated with this interface



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

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

(Notice that in the real CCNA exam the MAC address or port may be different)

And we find out the corresponding MAC address is 000a.b7e9.8360. Although there are some entries of port Fa0/3 with different Vlans but they have the same MAC address

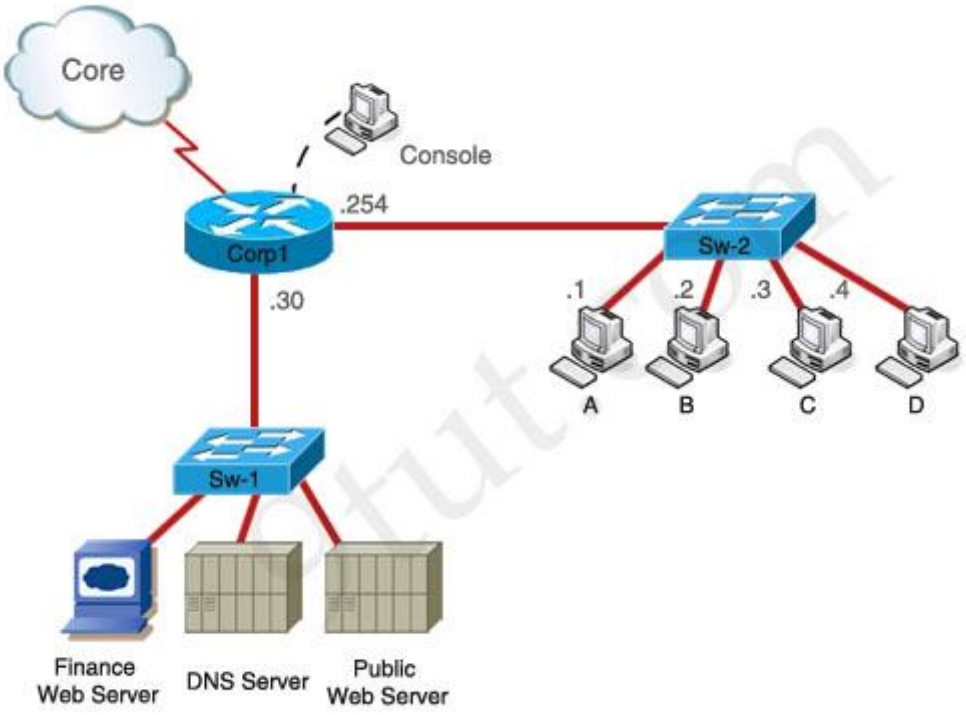
CCNA Access List Sim 2

Question

A network associate is adding security to the configuration of the Corp1 router. The user on host C should be able to use a web browser to access financial information from the Finance Web Server. No other hosts from the LAN nor the Core should be able to use a web browser to access this server. Since there are multiple resources for the corporation at this location including other resources on the Finance Web Server, all other traffic should be allowed.

The task is to create and apply a numbered access-list with no more than three statements that will allow ONLY host C web access to the Finance Web Server. No other hosts will have web access to the Finance Web Server. All other traffic is permitted.
Access to the router CLI can be gained by clicking on the appropriate host.

All passwords have been temporarily set to “cisco”.
The Core connection uses an IP address of 198.18.196.65
The computers in the Hosts LAN have been assigned addresses of 192.168.33.1 – 192.168.33.254
Host A 192.168.33.1
Host B 192.168.33.2
Host C 192.168.33.3
Host D 192.168.33.4
The servers in the Server LAN have been assigned addresses of 172.22.242.17 – 172.22.242.30
The Finance Web Server is assigned an IP address of 172.22.242.23.
The Public Web Server is assigned an IP address of 172.22.242.17



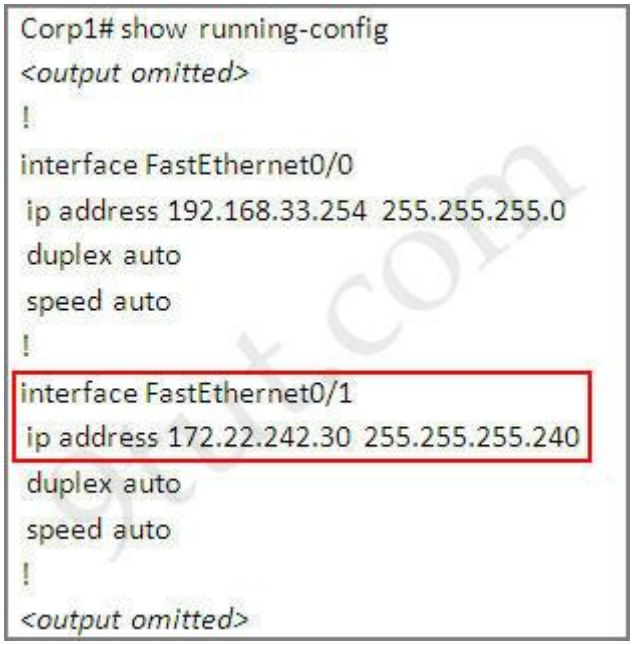
Answer and **Explanation**

(Note: If you are not sure how to use access-list, please check out my access-list tutorial at: http://www.9tut.com/access-list-tutorial, also some modifications about the access-list have been reported so you should read the "Some modifications" section at the end of this question to understand more. You can also download this sim to practice (open with Packet Tracer) here: http://www.9tut.com/download/9tut.com_Access-list_sim2.pkt

Corp1>enable (you may enter "cisco" as it passwords here)

We should create an access-list and apply it to the interface which is connected to the Server LAN because it can filter out traffic from both Sw-2 and Core networks. The Server LAN network has been assigned addresses of 172.22.242.17 – 172.22.242.30 so we can guess the interface connected to them has an IP address of 172.22.242.30 (.30 is the number shown in the figure). Use the "show running-config" command to check which interface has the IP address of 172.22.242.30.

Corp1#show running-config



We learn that interface FastEthernet0/1 is the interface connected to Server LAN network. It is the interface we will apply our access-list (for outbound direction).

Corp1#configure terminal

Our access-list needs to allow host C – 192.168.33.3 to the Finance Web Server 172.22.242.23 via web (port 80)

Corp1(config)#access-list 100 permit tcp host 192.168.33.3 host 172.22.242.23 eq 80

Deny other hosts access to the Finance Web Server via web

Corp1(config)#access-list 100 deny tcp any host 172.22.242.23 eq 80

All other traffic is permitted

Corp1(config)#access-list 100 permit ip any any

Apply this access-list to Fa0/1 interface (outbound direction)

Corp1(config)#interface fa0/1
Corp1(config-if)#ip access-group 100 out

Notice: We have to apply the access-list to Fa0/1 interface (not Fa0/0 interface) so that the access-list can filter traffic coming from both the LAN and the Core networks. If we apply access list to the inbound interface we can only filter traffic from the LAN network.

In the real exam, just click on host C and open its web browser. In the address box type http://172.22.242.23 to check if you are allowed to access Finance Web Server or not. If your configuration is correct then you can access it.

Click on other hosts (A, B and D) and check to make sure you can't access Finance Web Server from these hosts.

Finally, save the configuration

Corp1(config-if)#end
Corp1#copy running-config startup-config

(This configuration only prevents hosts from accessing Finance Web Server via web but if this server supports other traffic – like FTP, SMTP… then other hosts can access it, too.)

Notice: In the real exam, you might be asked to allow other host (A, B or D) to access the Finance Web Server so please read the requirement carefully.

Some modifications:

Modification 1:

permit host B from accessing finance server	access-list 100 permit ip host 192.168.33.2 host 172.22.242.23
deny host B from accessing other servers (not the whole network)	access-list 100 deny ip host 192.168.33.2 172.22.242.16 0.0.0.15
permit everything else	access-list 100 permit ip any any

Modification 2:

Only allow Host C to to access the financial server	access-list 100 permit ip host 192.168.33.3 host 172.22.242.23
Not allow anyone else in any way communicate with the financial server	access-list 100 deny ip any host 172.22.242.23
Allow all other traffic	access-list 100 permit ip any any

Modification 3:

- Host C should be able to use a web browser(HTTP)to access the Finance Web Server	access-list 100 permit tcp host 192.168.33.3 host 172.22.242.23 eq 80
- Other types of access from host C to the Finance Web Server should be blocked - All access from hosts in the Core or	access-list 100 deny ip any host 172.22.242.23 (because the requirement says we can not use more than 3 statements so we have to use "any" here for the

local LAN to the Finance Web Server should be blocked	hosts in the Core and hosts in local LAN)
- All hosts in the Core and local LAN should be able to access the Public Web Server *	access-list 100 permit ip any host (If the question asks this, surely it has to give you the IP of Public Web Server) but in the exam you should use "access-list 100 permit ip any any"

Modification 4:

Host C should be able to use a web browser to access the financial web server	access-list 100 permit tcp host 192.168.33.3 host 172.22.242.23 eq 80
Other types of access from host C to the finance web server should be blocked	access-list 100 deny ip host 192.168.33.3 host 172.22.242.23
All hosts in the core and on the local LAN should be able to access the Public web server *	access-list 100 permit ip any host (The IP of Public Web Server will surely be given in this question) but in the exam you should use "access-list 100 permit ip any any"

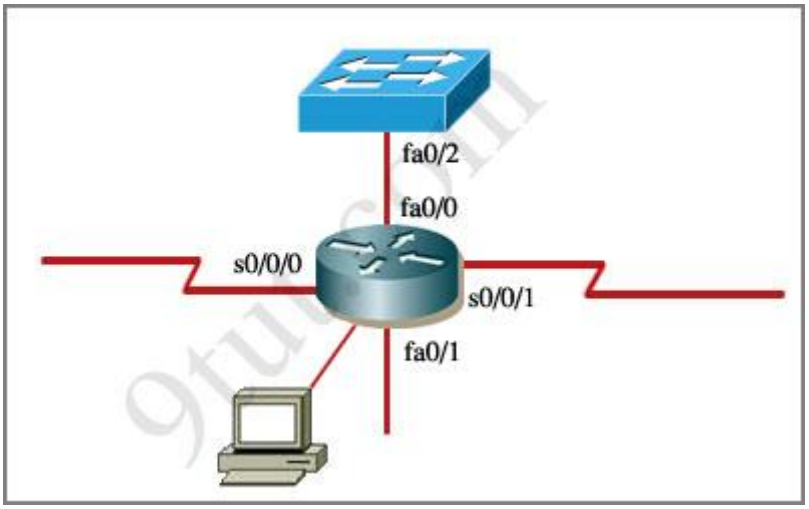
* There are some reports about the command of "All hosts in the core and on the local LAN should be able to access the Public web server" saying that the correct command should be "access-list 100 permit ip any any", not "access-list 100 permit ip any host (IP of Public Web Server)". Although I believe the second command is better but maybe you should use the first command "access-list 100 permit ip any any" instead as some reports said they got 100% when using this command (even if the question gives you the IP address of Public Web Server). It is a bug in this sim.

(Note: Don't forget to apply this access list to the suitable interface or you will lose points
interface fa0/1
ip access-group 100 out

And in the exam, they may slightly change the requirements, for example host A, host B instead of host C… so make sure you read the requirement carefully and use the access-list correctly)

CCNA Access List Sim

Question



An administrator is trying to ping and telnet from Switch to Router with the results shown below:

Switch>
Switch> ping 10.4.4.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.4.4.3,timeout is 2 seconds:
.U.U.U
Success rate is 0 percent (0/5)
Switch>
Switch> telnet 10.4.4.3
Trying 10.4.4.3 …
% Destination unreachable; gateway or host down
Switch>

Click the console connected to Router and issue the appropriate commands to answer the questions.

Answer and **Explanation**

Note: If you are not sure about Access-list, please read my Access-list tutorial. You can also download this sim to practice (open with Packet Tracer) here:
http://www.9tut.com/download/9tut.com_CCNA_Access_List_Sim.pkt

For this question we only need to use the show running-config command to answer all the questions below

Router>enable
Router#show running-config

```
<output omitted>

interface Loopback1
 ip address 172.16.4.1 255.255.255.0
!
interface Loopback2
 ip address 10.145.145.1 255.255.255.0
 ipv6 address 2001:410:2:3::/64 eui-64
!
interface FastEthernet0/0
 ip address 10.4.4.3 255.255.255.0
 ip access-group 106 in
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 bandwidth 64
 no ip address
 ip access-group 102 out
 encapsulation frame-relay
 ip ospf authentication
 ip ospf authentication-key san-fran
!
interface Serial0/0/0.1 point-to-point
 ip address 10.140.3.2 255.255.255.0
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 icndchain
 frame-relay interface-dlci 120
!
interface Serial0/0/1
 bandwidth 64
 ip address 10.45.45.1 255.255.255.0
 ip access-group 102 in
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 icndchain
 ip ospf authentication
 ip ospf authentication-key san-fran
 ipv6 address 2001:410:2:10::/64 eui-64
!
```

```
router eigrp 100
 network 10.0.0.0
 network 172.16.0.0
 network 192.168.2.0
 no auto-summary
!
router ospf 100
 log-adjacency-changes
 network 10.4.4.3 0.0.0.0 area 0
 network 10.45.45.1 0.0.0.0 area 0
 network 10.140.3.2 0.0.0.0 area 0
 network 192.168.2.62 0.0.0.0 area 0
!
router rip
 version 2
 network 10.0.0.0
 network 172.16.0.0
!
ip default-gateway 10.1.1.2
!
!
ip http server
no ip http secure-server
!
```

```
access-list 102 permit tcp any any eq ftp
access-list 102 permit tcp any any eq ftp-data
access-list 102 deny tcp any any eq telnet
access-list 102 deny icmp any any echo-reply
access-list 102 permit ip any any

access-list 104 permit tcp any any eq ftp
access-list 104 permit tcp any any eq ftp-data
access-list 104 deny tcp any any eq telnet
access-list 104 permit icmp any any echo
access-list 104 deny icmp any any echo-reply
access-list 104 permit ip any any

access-list 106 permit tcp any any eq ftp
access-list 106 permit tcp any any eq ftp-data
access-list 106 deny tcp any any eq telnet
access-list 106 permit icmp any any echo-reply
access-list 110 permit udp any any eq domain
access-list 110 permit udp any eq domain any
access-list 110 permit tcp any any eq domain
access-list 110 permit tcp any eq domain any
access-list 110 permit tcp any any

access-list 114 permit ip 10.4.4.0 0.0.0.255 any

access-list 115 permit ip 0.0.0.0 255.255.255.0 any

access-list 122 deny tcp any any
access-list 122 deny Imp any any echo-reply
access-list 122 permit ip any any
!
<output omitted>
```

Question 1:

Which will fix the issue and allow ONLY ping to work while keeping telnet disabled?

A – Correctly assign an IP address to interface fa0/1
B – Change the ip access-group command on fa0/0 from “in” to “out”
C – Remove *access-group 106 in* from interface fa0/0 and add access-group 115 in.
D – Remove access-group 102 out from interface s0/0/0 and add access-group 114 in
E – Remove access-group 106 in from interface fa0/0 and add access-group 104 in

Answer: E

Explanation:

Let's have a look at the access list 104:

```
access-list 104 permit tcp any any eq ftp
access-list 104 permit tcp any any eq ftp-data
access-list 104 deny tcp any any eq telnet
access-list 104 permit icmp any any echo
access-list 104 deny icmp any any echo-reply
access-list 104 permit ip any any
```

The question does not ask about ftp traffic so we don't care about the two first lines. The 3rd line denies all telnet traffic and the 4th line allows icmp traffic to be sent (ping). Remember that the access list 104 is applied on the inbound direction so the 5th line "access-list 104 deny icmp any any echo-reply" will not affect our icmp traffic because the "echo-reply" message will be sent over the outbound direction.

Question 2:

What would be the effect of issuing the command *ip access-group 114 in* to the fa0/0 interface?

A – Attempts to telnet to the router would fail
B – It would allow all traffic from the 10.4.4.0 network
C – IP traffic would be passed through the interface but TCP and UDP traffic would not
D – Routing protocol updates for the 10.4.4.0 network would not be accepted from the fa0/0 interface

Answer: B

Explanation:

From the output of access-list 114: **access-list 114 permit ip 10.4.4.0 0.0.0.255** any we can easily understand that this access list allows all traffic (ip) from 10.4.4.0/24 network

Question 3:

What would be the effect of issuing the command *access-group 115 in* on the s0/0/1 interface?

A – No host could connect to Router through s0/0/1
B – Telnet and ping would work but routing updates would fail.
C – FTP, FTP-DATA, echo, and www would work but telnet would fail
D – Only traffic from the 10.4.4.0 network would pass through the interface

Answer: A

Explanation:

First let's see what was configured on interface S0/0/1:

```
interface Serial0/0/1
 bandwidth 64
 ip address 10.45.45.1 255.255.255.0
 ip access-group 102 in
```

Recall that each interface only accepts one access-list, so when using the command "ip access-group 115 in" on the s0/0/1 interface it will overwrite the initial access-list 102. Therefore any telnet connection will be accepted (so we can eliminate answer C).
B is not correct because if telnet and ping can work then routing updates can, too.
D is not correct because access-list 115 does not mention about 10.4.4.0 network. So the most reasonable answer is A.

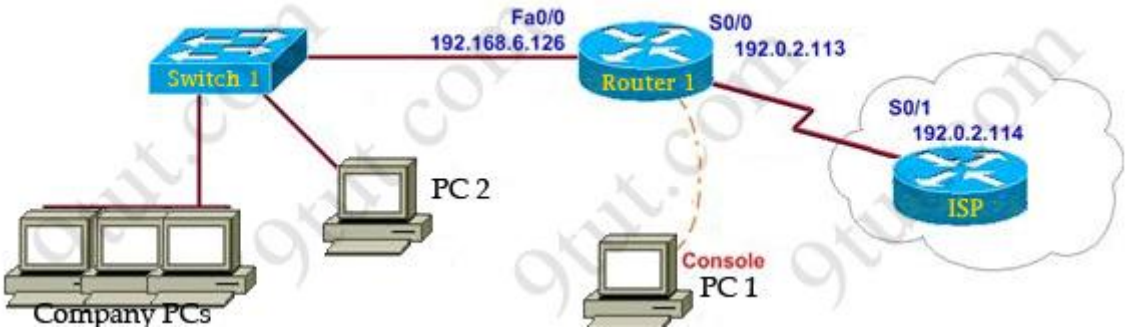
But here raise a question…

The wildcard mask of access-list 115, which is 255.255.255.0, means that only host with ip addresses in the form of x.x.x.0 will be accepted. But we all know that x.x.x.0 is likely to be a network address so the answer A: "no host could connect to Router through s0/0/1" seems right…

But what will happen if we don't use a subnet mask of 255.255.255.0? For example we can use an ip address of 10.45.45.0 255.255.0.0, such a host with that ip address exists and we can connect to the router through that host. Now answer A seems incorrect!

CCNA NAT SIM Question 2

Question



You work as a network technician at 9tut.com. Study the exhibit carefully. You are required to perform configurations to enable Internet access. The Router ISP has given you six public IP addresses in the 198.18.32.65 198.18.32.70/29 range.
9tut.com has 62 clients that needs to have simultaneous internet access. These local hosts use private IP addresses

in the 192.168.6.65 – 192.168.6.126/26 range.
You need to configure Router1 using the PC1 console.
You have already made basic router configuration. You have also configured the appropriate NAT interfaces; NAT inside and NAT outside respectively.
Now you are required to finish the configuration of Router1.

Solution

Note: If you are not sure how NAT & PAT work, please read my Network Address Translation NAT Tutorial. You can download a similar sim to practice here: http://www.9tut.com/download/9tut.com_CCNA_NAT_sim_question.zip

The company has 62 hosts that need to access the internet simultaneously but we just have 6 public IP addresses from 198.18.32.65 to 198.18.32.70/29 => we have to use NAT overload (or PAT)

Double click on PC1 to access Router1′s command line interface

Router1>enable
Router1#configure terminal

Create a NAT pool of global addresses to be allocated with their netmask (notice that /29 = 248)

Router1(config)#ip nat pool mypool 198.18.32.65 198.18.32.70 netmask 255.255.255.248

Create a standard access control list that permits the addresses that are to be translated

Router1(config)#access-list 1 permit 192.168.6.64 0.0.0.63

Establish dynamic source translation, specifying the access list that was defined in the prior step

Router1(config)#ip nat inside source list 1 pool mypool overload

This command translates all source addresses that pass access list 1, which means a source address from 192.168.6.65 to 192.168.6.126, into an address from the pool named mypool (the pool contains addresses from 198.18.32.65 to 198.18.32.70)

Overload keyword allows to map multiple IP addresses to a single registered IP address (many-to-one) by using different ports

The question said that appropriate interfaces have been configured for NAT inside and NAT outside statements.

This is how to configure the NAT inside and NAT outside, just for your understanding:

Router1(config)#interface fa0/0
Router1(config-if)#ip nat inside

Router1(config-if)#exit

Router1(config)#interface s0/0
Router1(config-if)#ip nat outside

Before leaving Router1, you should save the configuration:

Router1(config)#end (or Router1(config-if)#end)
Router1#copy running-config startup-config

Check your configuration by going to PC2 and type:

C:\>ping 192.0.2.114

The ping should work well and you will be replied from 192.0.2.114

CCNA Implementation SIM

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

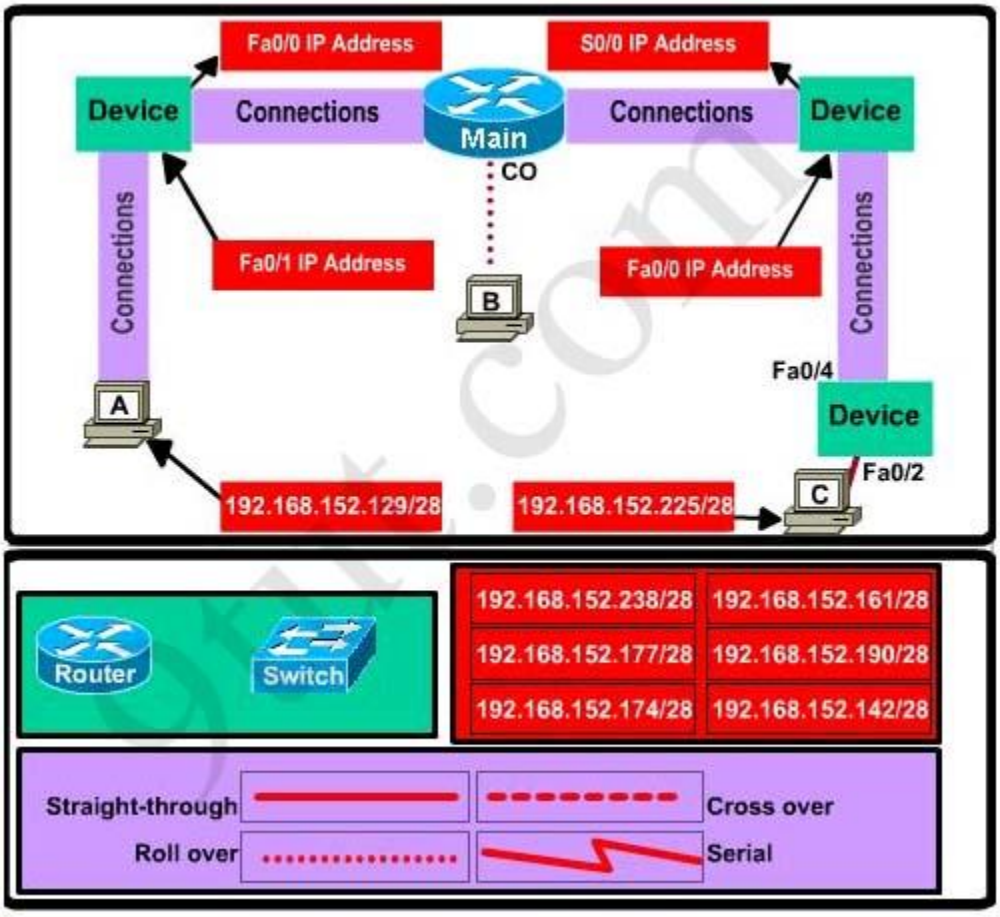
(Hint: use the given host addresses and Main router information)
To remove a device or connection, drag it away from the topology.

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**

Note: 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 and **Explanation**

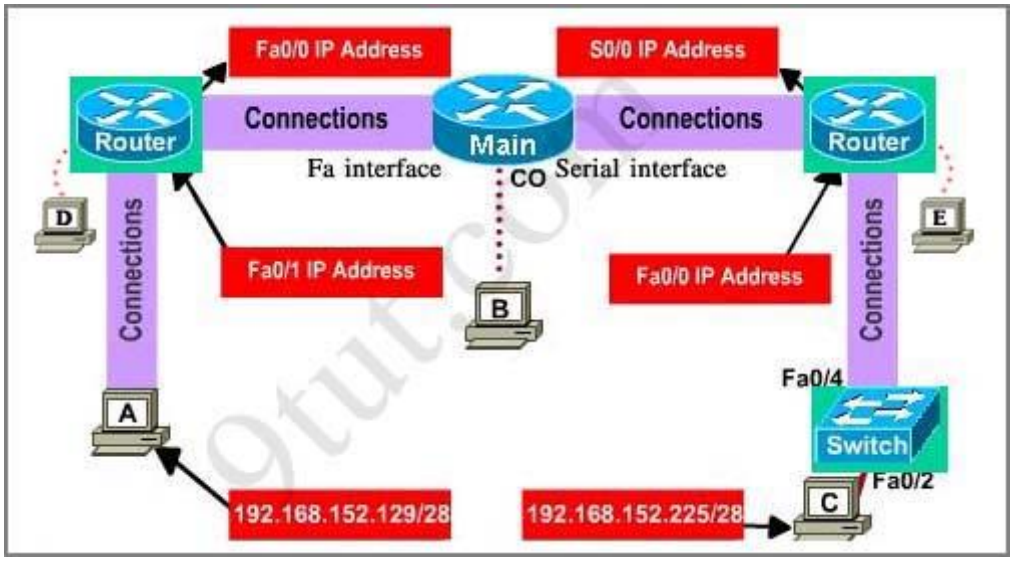
Note: You can download this sim to practice here:
http://www.9tut.com/download/9tut.com_CCNA_Implementation_question.zip

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)

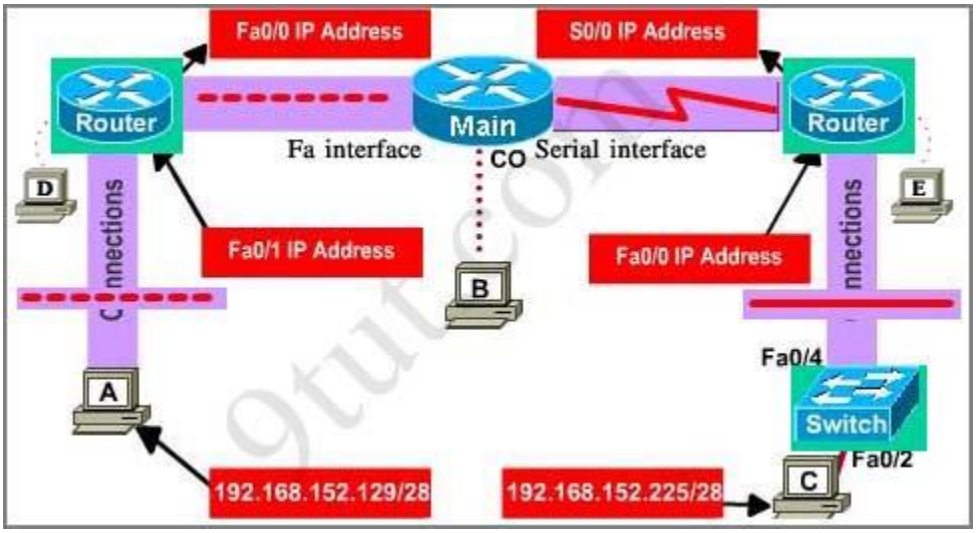
Specify appropriate connections between these devices:

+ 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:

```
Main#show running-config
interface FastEthernet0/0
  ip address 192.168.152.177  255.255.255.240
!
interface Serial0/0
  ip address 192.168.152.161  255.255.255.240
  clockrate 64000
<output omitted>
```

(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

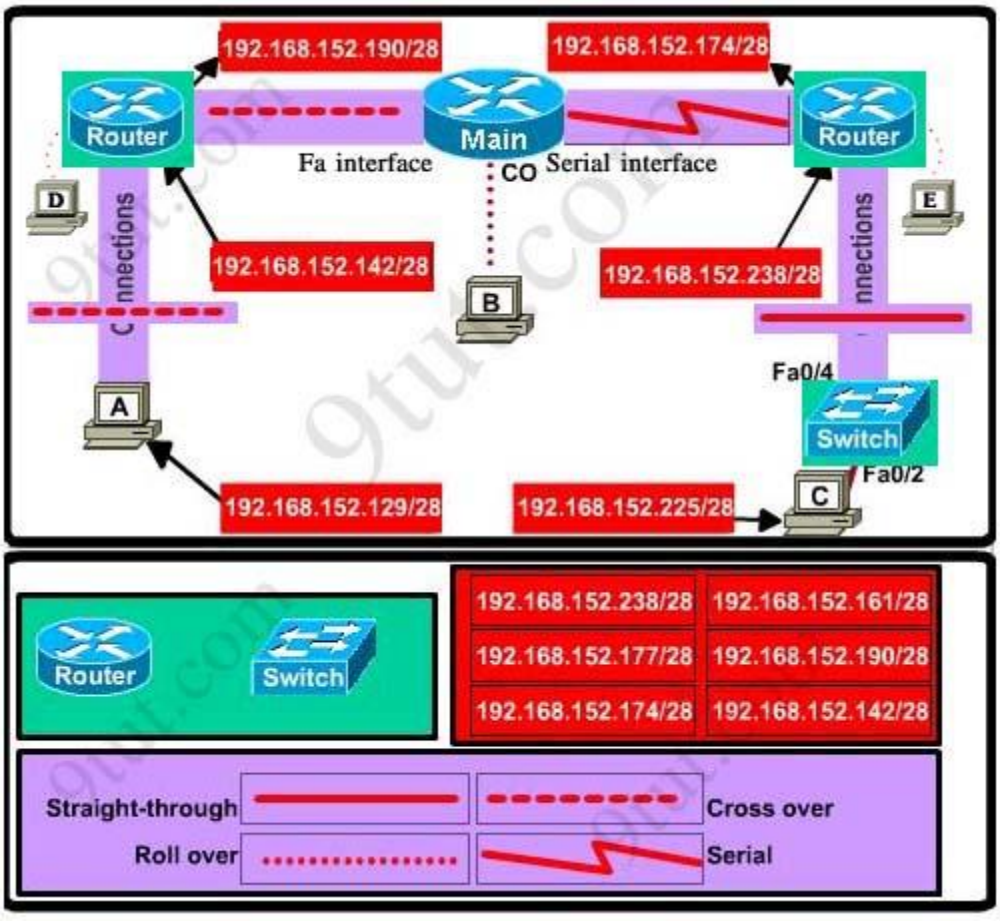
Interface Fa0/0 of the router on the right

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

and set console, telnet and privilege mode passwords for Router2 as we did for Router1, remember to save the configuration when you finished

CCNA EIGRP LAB Question

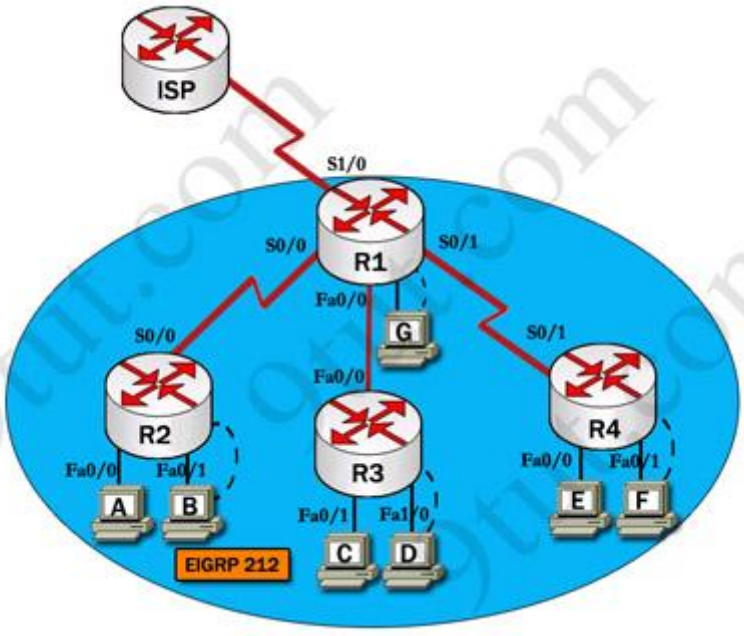
Question

After adding R3 router, no routing updates are being exchanged between R3 and the new location. All other inter connectivity and Internet access for the existing locations of the company are working properly.

The task is to identify the fault(s) and correct the router configuration to provide full connectivity between the routers.

Access to the router CLI can be gained by clicking on the appropriate host. All passwords on all routers are cisco.

IP addresses are listed in the chart below.



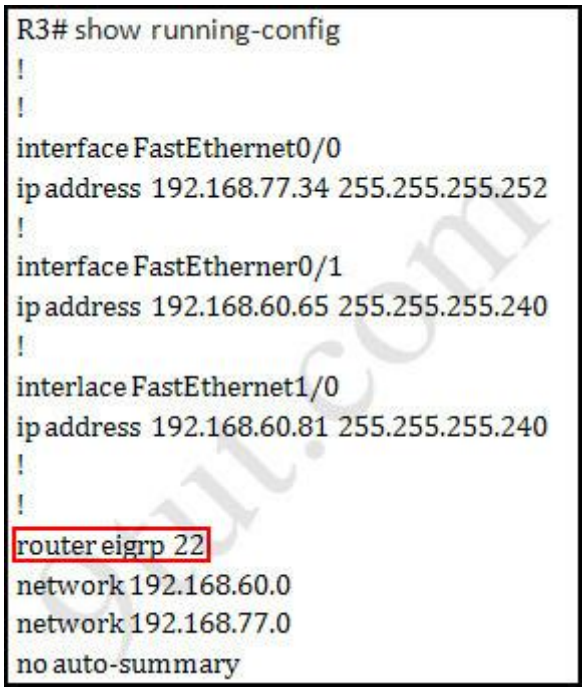
R1 **Fa0/0:** 192.168.77.33 **S1/0:** 198.0.18.6 **S0/1:** 192.168.60.25 **S0/0:** 192.168.36.13	**R2** **Fa0/0:** 192.168.60.97 **Fa0/1:** 192.168.60.113 **S0/0:** 192.168.36.14

R3	R4
Fa0/0: 192.168.77.34	**Fa0/0:** 192.168.60.129
Fa0/1: 192.168.60.65	**Fa0/1:** 192.168.60.145
Fa1/0: 192.168.60.81	**S0/1:** 192.168.60.26

Answer and **Explanation**

(Note: If you are not sure how EIGRP works, please read my EIGRP tutorial: http://www.9tut.com/eigrp-routing-protocol-tutorial. Note: You can download this sim to practice here: http://www.9tut.com/download/9tut.com_CCNA_EIGRP_sim_question.zip)

We should check the configuration of the new added router first because it does not function properly while others work well. From the command line interface of R3 router, enter the **show running-config** command



From the output above, we know that this router was wrongly configured with an autonomous number (AS) of 22. When the AS numbers among routers are mismatched, no adjacency is formed.

(You should check the AS numbers on other routers for sure)

To solve this problem, we simply re-configure router R3 with the following commands:

R3>enable (you have to enter **cisco** as its password here)

R3#configure terminal

R3(config)#no router eigrp 22

R3(config)#router eigrp 212

R3(config-router)#network 192.168.60.0

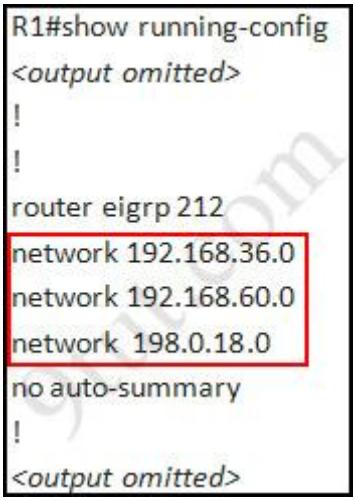
R3(config-router)#network 192.168.77.0

R3(config-router)#no auto-summary

R3(config-router)#end

R3#copy running-config startup-config

Check R1 router with the **show running-config** command:



Notice that it is missing a definition to the network R3. Therefore we have to add it so that it can recognize R3 router

R1>enable (you have to enter **cisco** as its password here)

R1#configure terminal

R1(config)#router eigrp 212

R1(config-router)#network 192.168.77.0

R1(config-router)#end

R1#copy running-config startup-config

Now the whole network will work well. You should check again with **ping** command from router R3 to other routers!

Modifications:

Maybe in this EIGRP Sim you will see the “passive-interface …” command somewhere in R1 configuration. If the link between R1 to R2; or R1 to R3; or R1 to R4) routers has the “passive interface” then we have to remove it with the “no passive-interface …” command because it prevents

EIGRP update from being sent on that interface. But if the "passive interface" is applied to the link **between R1 and ISP router** like this:

R1:

```
!
router eigrp 212
passive-interface s1/0
!
```

then we just leave it. **Don't use the "no passive-interface s1/0″ on R1** because the link between R1 & ISP doesn't need EIGRP to run on it. A static route from R1 to ISP & "ip default-network" command in R1 are correct so that all the routers (R1, R2, R3, R4) can access the Internet.

(Note: The "ip default-network" command in R1 will advertise the static route of R1 (to go to the Internet) to other routers (R2,R3,R4) so that they can access the Internet too). In the exam you will see these lines in R1 configuration:

```
!
ip default-network 198.0.18.0
ip route 0.0.0.0 0.0.0.0 198.0.18.5
!
```

If you want to learn more about "ip default-network" command please read:
http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080094374.shtml

I read recent comments and realized that you will see the "passive-interface" in the link **between R1 & ISP router** so just leave it.

Note: Also some readers confuse about if we should use the wildcard masks on the "network" statements under EIGRP process or not. For example should we use:

```
router eigrp 212
network 192.168.77.0 0.0.0.3
```

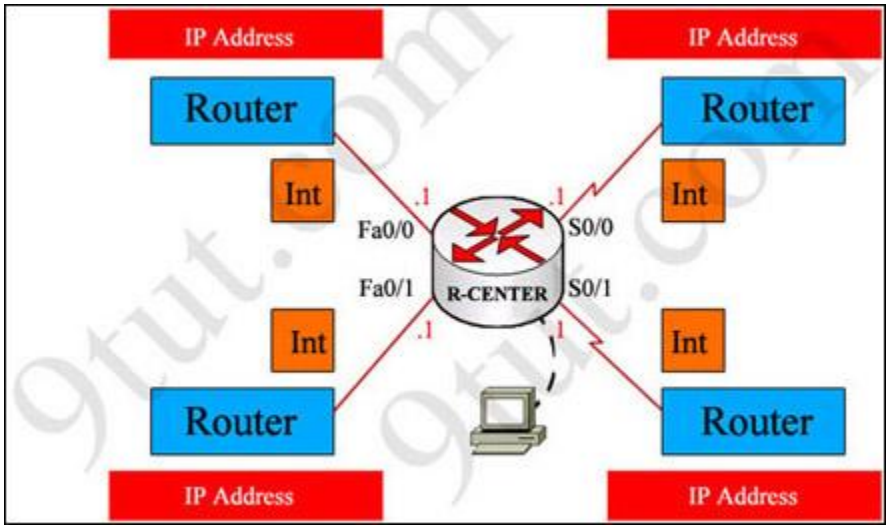
The answer is: we can use wildcard masks or not, it does not matter. Not having a wildcard mask does not make the routes conflicting. The "network …" command in EIGRP (and OSPF, RIP) does not means "advertise this network" but means "If I has interface(s) belongs to this network please turn on EIGRP on that interface. Therefore when you don't use wildcard mask EIGRP will turn on EIGRP on all interfaces that belongs to the network you specify in the "network …" command.

You should only use wildcard mask on EIGRP if you have 2 or more interfaces that belong to the same major networks but you don't want to run EIGRP on all of them. For example if your router has 2 interfaces whose IP addresses are 192.168.30.1/28 and 192.168.30.17/28 but you only want to run EIGRP on the first interface, you can type "network 192.168.30.0 0.0.0.15″ under EIGRP process.

CCNA Drag and Drop SIM Question

Question

You have been hired by Specialty Hardware Incorporated to document the layout of the network. Complete the following tasks: Complete the network topology shown in the graphic by dragging the labels below with the appropriate router types, interface types, and IP addresses to the graphic . Find the information you need by using the router console attached to the R-CENTER router.



Answer and **Explanation**

Note: You can download this sim to practice here:
http://www.9tut.com/download/9tut.com_CCNA_drag_and_drop_sim_question.pkt

This is the simplest lab question in four labs you see in the real CCNA exam. First we should identify the types of these routers by using the **show cdp neighbors** command:

R-CENTER# show cdp neighbors

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

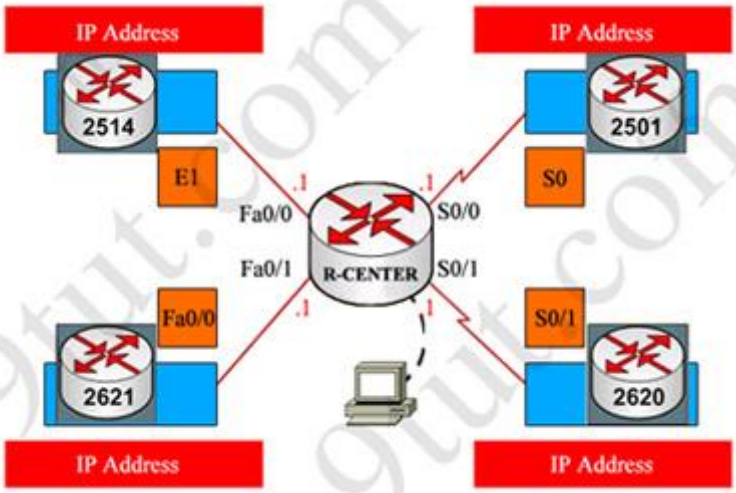
There are 3 columns we should pay more attention to:

+ **Local Interface:** the interface on the device you are using "show cdp neighbors" command. In this case it is the interface of R-CENTER router

+ **Platform:** the platform of neighbor device

+ **Port ID:** the neighbor device's port or interface on which the CDP packets are multicast

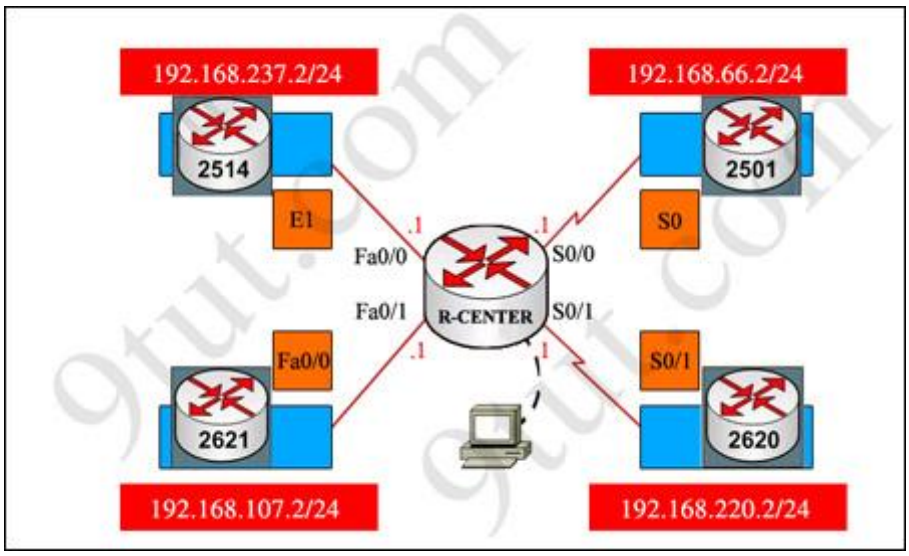
From the exhibit, the "Local Interface", "Platform" and "Port ID" columns, we can identify where these four routers should be placed and their corresponding associated ports



Finally, use the show running-config command to find out the ip addresses of four interfaces on R-CENTER

```
R-CENTER# show running-config
!
interface FastEthernet0/0
ip address 192.168.237.1  255.255.255.0  duplex auto
speed auto
!
interface FastEthernet0/1
ip address 192.168.107.1  255.255.255.0  duplex auto
speed auto
!
interface Serial0/0
ip address 192.168.66.1  255.255.255.0
!
interface Serial0/1
ip address 192.168.220.1  255.255.255.0
!
```

And we can easily assign corresponding ip addresses to four neighbor routers, which are on the same network with R-CENTER router's interfaces



Please remember in the real CCNA Exam the routers' types, ip addresses and interfaces may be different! So make sure you understand how it works.

CCNA NAT SIM Question 1

Question

A network associate is configuring a router for the CCNA Training company to provide internet access. The ISP has provided the company six public IP addresses of 198.18.184.105 198.18.184.110. The company has 14 hosts that need to access the internet simultaneously. The hosts in the CCNA Training company LAN have been assigned private space addresses in the range of 192.168.100.17 – 192.168.100.30.

The task is to complete the NAT configuration using all IP addresses assigned by the ISP to provide Internet access for the hosts in the Weaver LAN. Functionality can be tested by clicking on the host provided for testing.

Configuration information
router name – Weaver
inside global addresses – 198.18.184.105 198.18.184.110/29
inside local addresses – 192.168.100.17 – 192.168.100.30/28
number of inside hosts – 14

The following have already been configured on the router：

- The basic router configuration

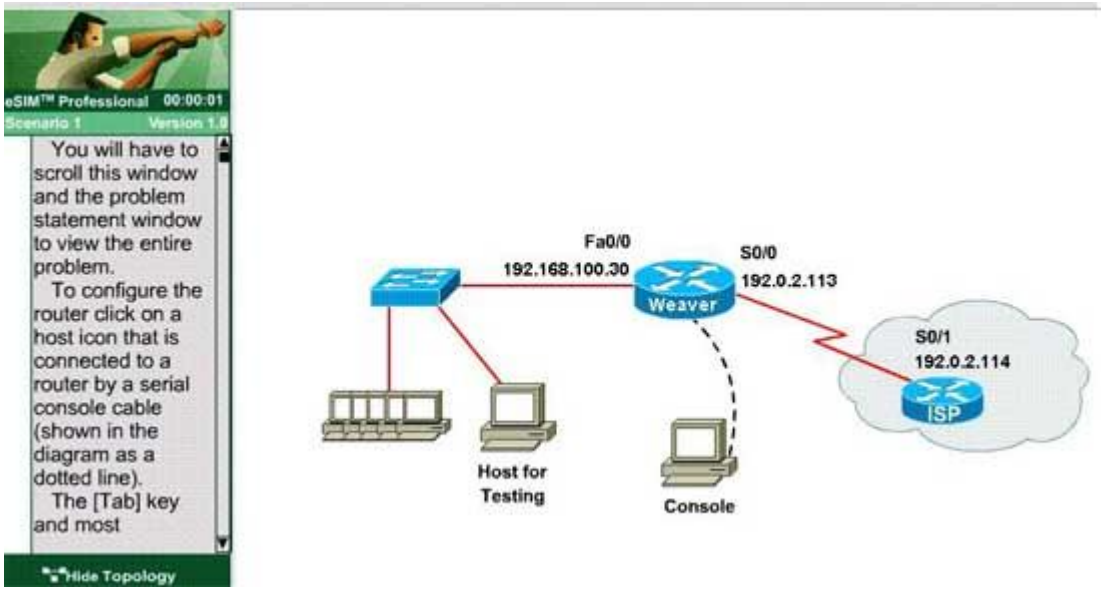
- The appropriate interfaces have been configured for NAT inside and NAT outside

- The appropriate static routes have also been configured (since the company will be a stub network, no routing protocol will be required.)

- All passwords have been temporarily set to “cisco”

The task is to complete the NAT configuration using all IP addresses assigned by the ISP to provide Internet access for the hosts in the Weaver LAN. Functionality can be tested by clicking on the host provided for testing.

Configuration information
router name - Weaver
inside global addresses-198.18.184.105 198.18.184.110/29
inside local addresses - 192.168.100.17 - 192.168.100.30/28
number of inside hosts - 14



Solution

Note: If you are not sure how NAT & PAT work, please read my Network Address Translation NAT Tutorial. You can download this sim to practice here: http://www.9tut.com/download/9tut.com_CCNA_NAT_sim_question.zip

The CCNA Training company has 14 hosts that need to access the internet simultaneously but we just have 6 public IP addresses from 198.18.184.105 to 198.18.184.110/29. Therefore we have to use NAT overload (or PAT)

Double click on the Weaver router to open it

Router>enable
Router#configure terminal

First you should change the router's name to Weaver

Router(config)#hostname Weaver

Create a NAT pool of global addresses to be allocated with their netmask (/29 = 255.255.255.248). There were reports that the simulator in the real exam did not accept "prefix-length" keryword so you should use "netmask" keyword.

Weaver(config)#ip nat pool mypool 198.18.184.105 198.18.184.110 netmask 255.255.255.248

Create a standard access control list that permits the addresses that are to be translated

Weaver(config)#access-list 1 permit 192.168.100.16 0.0.0.15

Establish dynamic source translation, specifying the access list that was defined in the prior step

Weaver(config)#ip nat inside source list 1 pool mypool overload

This command translates all source addresses that pass access list 1, which means a source address from 192.168.100.17 to 192.168.100.30, into an address from the pool named mypool (the pool contains addresses from 198.18.184.105 to 198.18.184.110)

Overload keyword allows to map multiple IP addresses to a single registered IP address (many-to-one) by using different ports

The question said that appropriate interfaces have been configured for NAT inside and NAT outside statements.

This is how to configure the NAT inside and NAT outside, just for your understanding:

Weaver(config)#interface fa0/0
Weaver(config-if)#ip nat inside

Weaver(config-if)#exit

Weaver(config)#interface s0/0
Weaver(config-if)#ip nat outside
Weaver(config-if)#end

Finally, we should save all your work with the following command:

Weaver#copy running-config startup-config

Check your configuration by going to “Host for testing” and type:

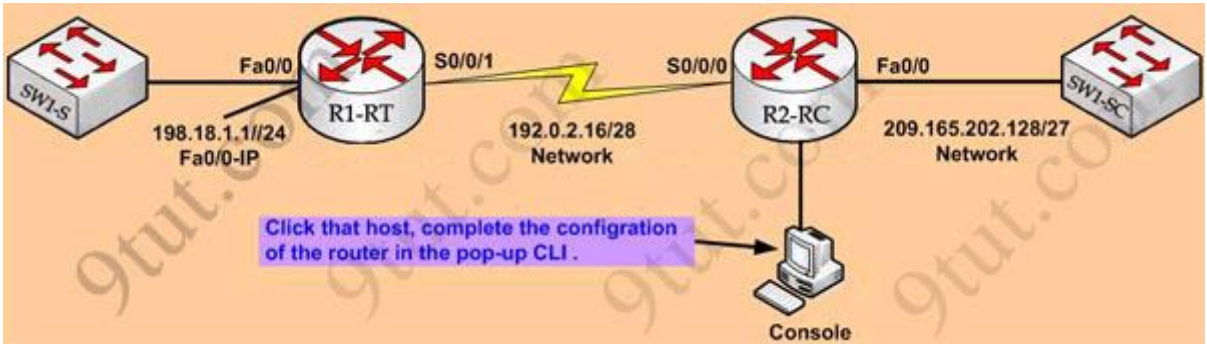
C:\>ping 192.0.2.114

The ping should work well and you will be replied from 192.0.2.114

CCNA Configuration SIM Question

Question:

To configure the router (R2-RC) 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)



CCNA Training Company recently installed a new router in their office. Complete the network installation by performing the initial router configurations and configuring RIPV2 routing using the router command line interface (CLI) on the R2-RC.

Name of the router is **R2-RC**
Enable-secret password is **cisco1**
The password to access user EXEC mode using the console is **cisco2**
The password to allow telnet access to the router is **cisco3**
IPV4 addresses must be configured as follows:
Ethernet network **209.165.202.128/27** – router has last assignable host address in subnet
Serial network is **192.0.2.16/28** – router has last assignable host address in the subnet. Interfaces should be enabled.
Router protocol is **RIP V2**

Attention :
In practical examinations, please note the following, the actual information will prevail.
1. Name of the router is xxx
2. Enable-secret password is xxx
3. Password to access user EXEC mode using the console is xxx
4. The password to allow telnet access to the router is xxx
5. IP information

Solution

(Note: If you are not sure how RIP works, please read my RIP tutorial: http://www.9tut.com/rip-routing-protocol-tutorial. Note: You can download this sim to practice here: http://www.9tut.com/download/9tut.com_CCNA_RIP_Configuration.zip)

1) Name the router:

Router>enable
Router#configure terminal
Router(config)#hostname R2-RC

2) Set secret password:

R2-RC(config)# enable secret cisco1

3) Set password for the console:

R2-RC(config)#line console 0
R2-RC(config-line)#password cisco2
R2-RC(config-line)#login
R2-RC(config-line)#exit

4) Set the Telnet password:

R2-RC(config)#line vty 0 4
R2-RC(config-line)#password cisco3
R2-RC(config-line)#login
R2-RC(config-line)#exit

5) Assign IP address for Ethernet interface (Fa0/0):

The Ethernet network **209.165.202.128/27** has**:**

Increment:32 (/27 = 255.255.255.224 or 1111 1111.1111 1111.1111 1111.111**1**0 0000)
Network address: 209.165.202.128
Broadcast address: 209.165.202.159 (because 128 + 32 – 1 = 159)

Therefore the last assignable host address in this subnet is **209.165.202.158** and we will assign it to Fa0/0 interface with these commands:

R2-RC(config)# interface fa0/0
R2-RC(config-if)#ip address 209.165.202.158 255.255.255.224
R2-RC(config-if)#no shutdown
R2-RC(config-if)#exit

6) Assign IP address for Serial interface (S0/0/0):

Serial network **192.0.2.16/28** has:

Increment:16 (/28 = 255.255.255.240 or 1111 1111.1111 1111.1111 1111.111**1** 0000)
Network address: 192.0.2.16
Broadcast address: 192.0.2.31 (because 16 + 16 – 1 = 31)

So the last assignable host address in this subnet is **192.0.2.30**. Finally we assign it to s0/0/0 interface:

R2-RC(config)# interface s0/0/0
R2-RC(config-if)#ip address 192.0.2.30 255.255.255.240
R2-RC(config-if)#no shutdown
R2-RC(config-if)#exit

7) Configure RIP v2 routing protocol:

R2-RC(config)#router rip
R2-RC(config-router)#version 2
R2-RC(config-router)#network 209.165.202.0
R2-RC(config-router)#network 192.0.2.0
R2-RC(config-router)#end
R2-RC#copy running-config startup-config

Note: We should use classful networks (209.165.202.0 & 192.0.2.0) when configuring RIP. If we use detailed networks (209.165.202.128 & 192.0.2.16) the router will automatically convert them into classful networks.