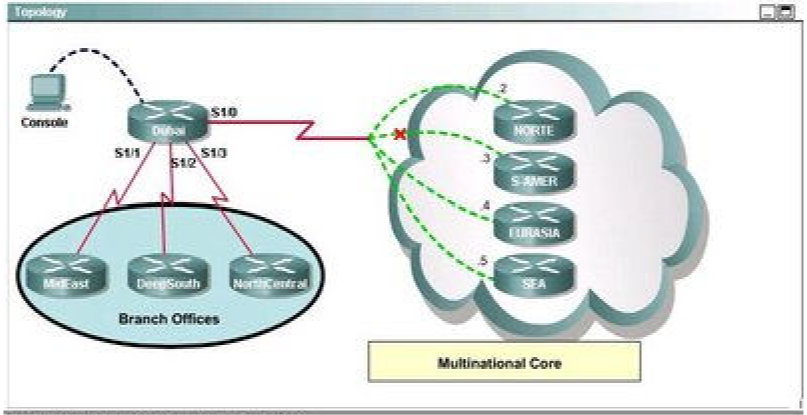
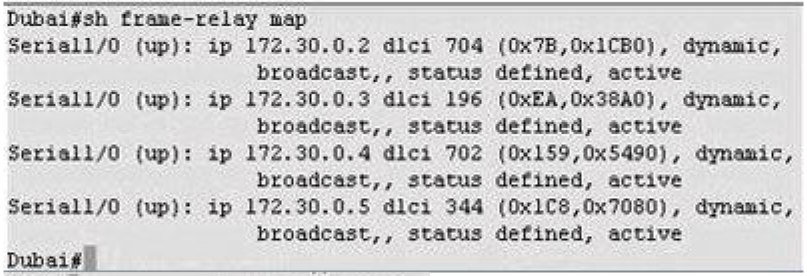
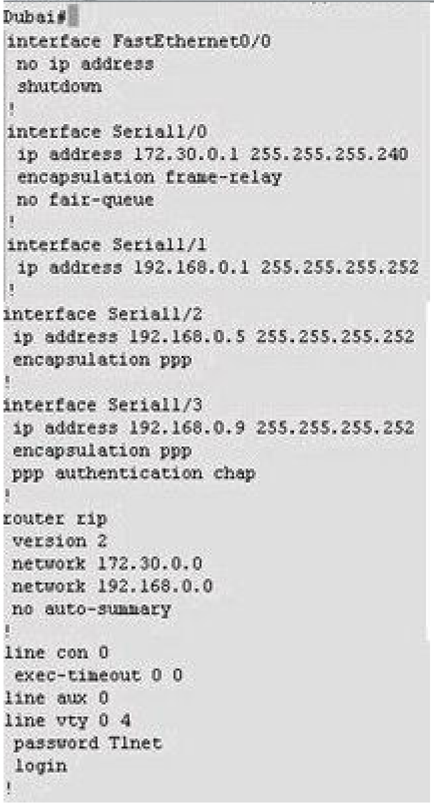
1. Hotspot 2: Topology Question

640-802 CCNA Hotspot Topology Exhibit





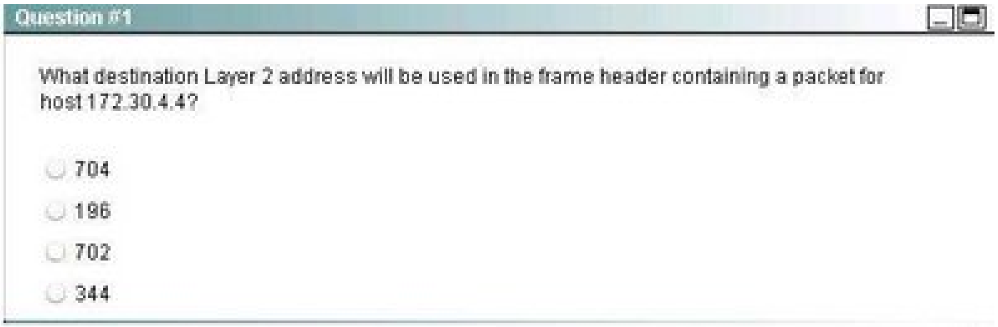
```
Dubai#sh frame-relay map
Seriall/0 (up): ip 172.30.0.2 dlci 704 (0x7B,0x1CB0), dynamic,
                     broadcast,, status defined, active
Seriall/0 (up): ip 172.30.0.3 dlci 196 (0xEA,0x38A0), dynamic,
                     broadcast,, status defined, active
Seriall/0 (up): ip 172.30.0.4 dlci 702 (0x159,0x5490), dynamic,
                     broadcast,, status defined, active
Seriall/0 (up): ip 172.30.0.5 dlci 344 (0x1C8,0x7080), dynamic,
                     broadcast,, status defined, active
Dubai#
```



```
Dubai#
interface FastEthernet0/0
 no ip address
 shutdown
!
interface Serial1/0
 ip address 172.30.0.1 255.255.255.240
 encapsulation frame-relay
 no fair-queue
!
interface Serial1/1
 ip address 192.168.0.1 255.255.255.252
!
interface Serial1/2
 ip address 192.168.0.5 255.255.255.252
 encapsulation ppp
!
interface Serial1/3
 ip address 192.168.0.9 255.255.255.252
 encapsulation ppp
 ppp authentication chap
!
router rip
 version 2
 network 172.30.0.0
 network 192.168.0.0
 no auto-summary
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 password Tlnet
 login
!
```

Question 1:

Note: host 172.30.4.4 is wrongly given in Question the correct host must be 172.30.0.4



What destination Layer 2 address will be used in the frame header containing a packet for host 172.30.4.4?

○ 704

○ 196

○ 702

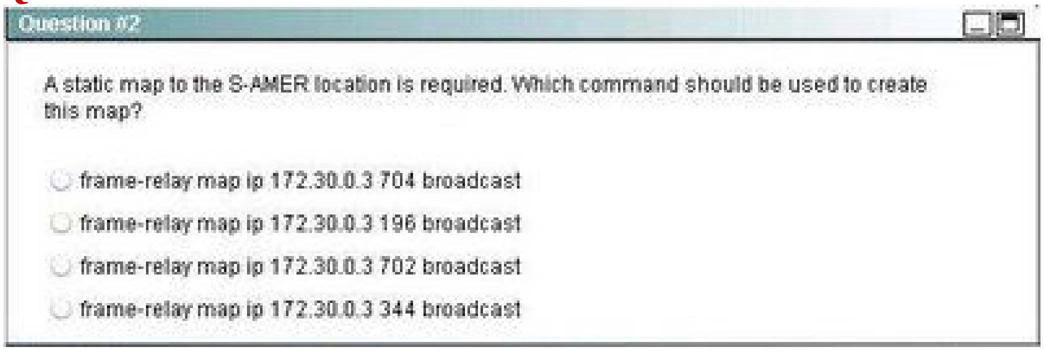
○ 344

Answers: 702

Explanation:

The destination layer 2 address is a DLCI for frame-relay network. The destination host packet address is 172.30.0.4 corresponding DLCI is 702.
This can be confirmed by looking at the **show frame-relay map** output which shows the frame-relay map statements for layer 3 address to its corresponding layer 2 address IP 172.30.0.4 is mapped to DLCI 702 .

Question 2:



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

○ frame-relay map ip 172.30.0.3 704 broadcast

○ frame-relay map ip 172.30.0.3 196 broadcast

○ frame-relay map ip 172.30.0.3 702 broadcast

○ frame-relay map ip 172.30.0.3 344 broadcast

Answers: frame-relay map ip 172.30.0.3 196 broadcast

Explanation:

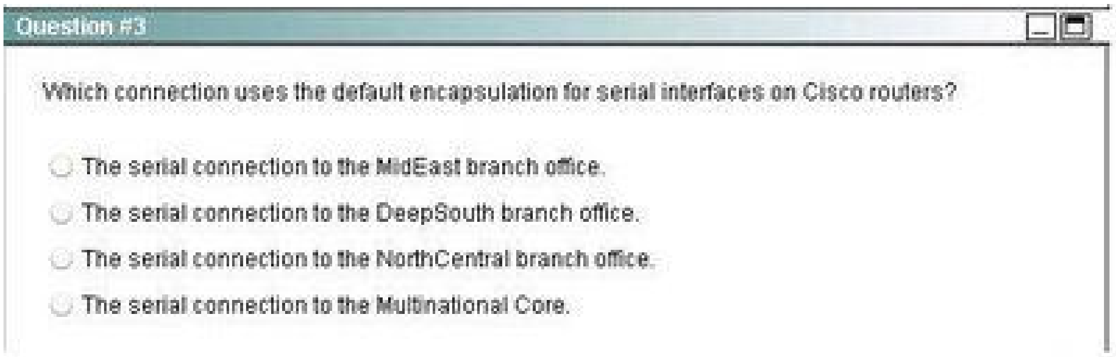
The show frame-relay map command above output provides the dynamic mapping for S-AMER (.3 as per topology the complete address is 172.30.0.3) to DLCI 196.

To create a static frame-relay map on dubai router to S-AMER we use the following command

Syntax: frame-relay map protocol protocol-address dlci [broadcast]

frame-relay map ip 172.30.0.3 196 broadcast

Question 3:



Question #3

Which connection uses the default encapsulation for serial interfaces on Cisco routers?

○ The serial connection to the MidEast branch office.

○ The serial connection to the DeepSouth branch office.

○ The serial connection to the NorthCentral branch office.

○ The serial connection to the Multinational Core.

Answers: The serial connection to the MidEast branch office

Explanation:

By seeing the partial running config provided for Dubai router … We can identify what encapuslation type is configured on each interface

Interface serial 1/0 : encapsulation frame-relay

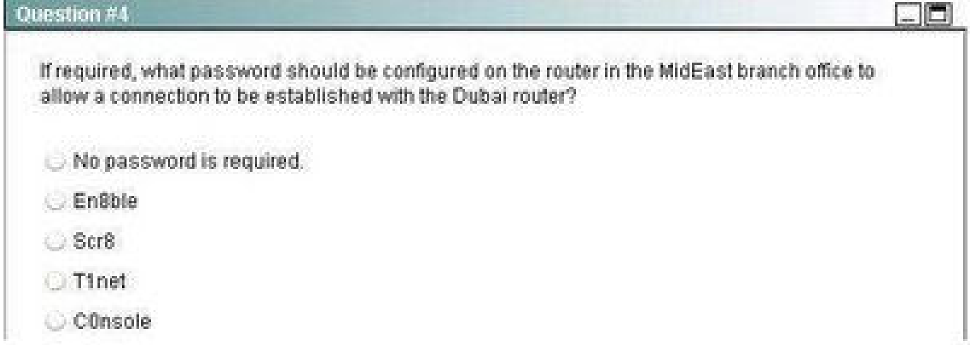
Interface serial 1/2 and serial 1/3 : Both have encapsulation ppp

Interaface serial 1/1: Has no config info on encapsulation type this determines the default encapsulation (HDLC) is not changed on this interface.

Serial 1/1 is connection to MidEast branch office from Dubai router which has the default encapsulation.

www.ccna-4.tk

Question 4:



Question #4

If required, what password should be configured on the router in the MidEast branch office to allow a connection to be established with the Dubai router?

○ No password is required.

○ En8ble

○ Scr8

○ T1net

○ C0nsole

Answers: T1net

Download: http://cisco-training640-802.blogspot.com/

2. Explain and select tasks required for WLAN

CCNA (640-802) exam topic **Explain and select the appropriate administrative tasks required for a WLAN**

Question1:

A single 802.11g access point has been configured and installed in the center of a square office. A few wireless users are experiencing slow performance and drops while most users are operating at peak efficiency. What are three likely causes of this problem? (Choose three.)

A:mismatched TKIP encryption

B:null SSID

C:cordless phones

D:mismatched SSID

E:metal file cabinets

F:antenna type or direction

Answers: C, E, F

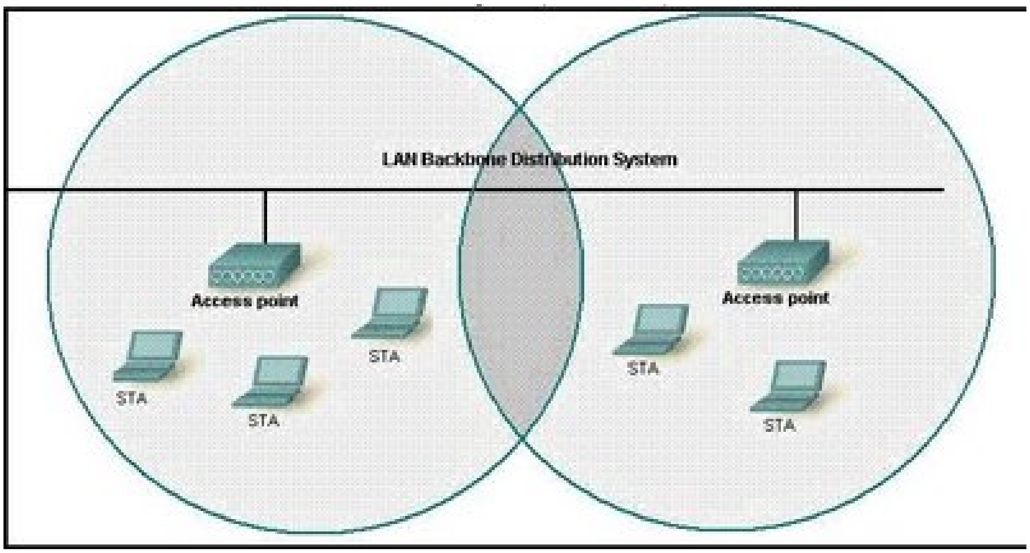
Explanation:

Cordless phones also work on RF so they conflict with WLAN RF and reduce the performance. metal file cabinets also act as obstacles for Radio waves in WLAN results in performane loss.

Antenna adds power gain for radio waves if Antenna selected is not correct type or direction is not exact then performance will effect.

Question 2:

Refer to the exhibit. What two facts can be determined from the WLAN diagram? (Choose two.)



A:The area of overlap of the two cells represents a basic service set (BSS).

B:The network diagram represents an extended service set (ESS).

C:Access points in each cell must be configured to use channel 1.

D:The area of overlap must be less than 10% of the area to ensure connectivity.

E:The two APs should be configured to operate on different channels.

Answers: B, E

Explanation:

The Extended Service Set (ESS) uses multiple APs with overlapping microcells to cover all clients. Microcells should overlap by 10–15 percent for data, and 15–20 percent for voice traffic. Each AP should use a different channel.

Question 3:

Which spread spectrum technology does the 802.11b standard define for operation?

A: IR

B: DSSS

C: FHSS

D: DSSS and FHSS

E: IR, FHSS, and DSSS

Answers: B

Explanation:

802.11b is a widely adopted standard that operates in the 2.4 GHz range and uses Direct Sequence Spread Spectrum (DSSS).

Question 4:

What is the maximum data rate specified for IEEE 802.11b WLANs?

A: 10 Mbps

B: 11 Mbps

C: 54 Mbps

D: 100 Mbps

Answers: B

Explanation:

802.11b supports four data rates: 1, 2, 5.5, and 11 Mbps.

Question 5:

Which two statements best describe the wireless security standard that is defined by WPA? (Choose two.)

A:It specifies use of a static encryption key that must be changed frequently to enhance

B:It requires use of an open authentication method.

C:It specifies the use of dynamic encryption keys that change each time a client establishes a

connection.
D:It requires that all access points and wireless devices use the same encryption key.
E:It includes authentication by PSK.

Answers: C, E

Explanation:
Wi-Fi Protected Access (WPA) is a Wi-Fi Alliance standard.
Uses Temporal Key Integrity Protocol (TKIP) for encryption,
dynamic keys, and 802.1x user authentication.

WPA-PSK (Pre shared Key) is a special mode of WPA for home users without an enterprise authentication server and provides the same strong encryption protection.

Question 6:
Which additional configuration step is necessary in order to connect to an access point that has SSID broadcasting disabled?

A: Set the SSID value in the client software to public.
B: Configure open authentication on the AP and the client.
C: Set the SSID value on the client to the SSID configured on the AP.
D: Configure MAC address filtering to permit the client to connect to the AP.

Answers: C

Explanation:
Since access point has SSID broadcasting disabled here we need to manually configure client the same SSID value configured on AP so that client can associate with the AP.

Question 7:
You and a co-worker have established wireless communication directly between your wireless laptops. What type of wireless topology has been created?

A: BSS
B: ESS
C: IBSS
D: SSID

Answers: C

Explanation:

Ad-hoc mode or Independent Basic Service Set [IBSS] is simply a group of computers talking wirelessly to each other with no access point (AP).

Question 8:

What is one reason that WPA encryption is preferred over WEP?

A: A WPA key is longer and requires more special characters than the WEP key.

B: The access point and the client are manually configured with different WPA key values.

C: WPA key values remain the same until the client configuration is changed.

D: The values of WPA keys can change dynamically while the system is used.

Answers: D

Explanation:

WPA uses dynamic keys ; WEP uses static keys.

Question 9:

Which two devices can interfere with the operation of a wireless network because they operate on similar frequencies? (Choose two.)

A:copier

B:microwave oven

C:toaster

D:cordless phone

E:IP phone

F:AM radio

Answers: B, D

Question 10:

Which encryption type does WPA 2 use ?

A: AES-CCMP

B: PPK via IV

C: PSK

D: TKIP/MIC

Answers: A

Explanation:

WPA 2 uses AES-CCMP encryption . AES-CCMP incorporates two sophisticated cryptographic techniques (counter mode and CBC-MAC) and adapts them to Ethernet frames to provide a robust security protocol between the mobile client and the access point

3. CCNA (640-802) exam topic **Implement, verify, and troubleshoot NAT and ACLs** in a medium-size Enterprise branch office network .

Implement, verify, and troubleshoot NAT and ACLs

Question1:

What are two reasons that a network administrator would use access lists? (Choose two.)

A:to control vty access into a router

B:to control broadcast traffic through a router

C:to filter traffic as it passes through a router

D:to filter traffic that originates from the router

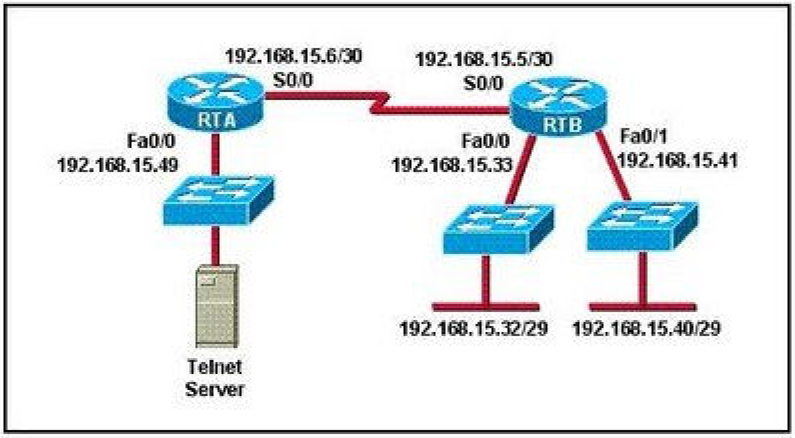
E:to replace passwords as a line of defense against security incursions

Answers: A, C

Question 2:

Refer to the exhibit. The access list has been configured on the S0/0 interface of router RTB in the outbound direction. Which two packets, if routed to the interface, will be denied? (Choose two.)

```
access-list 101 deny tcp 192.168.15.32 0.0.0.15 any eq telnet
access-list 101 permit ip any any
```



A:source ip address: 192.168.15.5; destination port: 21

B:source ip address:, 192.168.15.37 destination port: 21

C:source ip address:, 192.168.15.41 destination port: 21

D:source ip address:, 192.168.15.36 destination port: 23

E:source ip address: 192.168.15.46; destination port: 23

F:source ip address:, 192.168.15.49 destination port: 23

Answers: D, E

Explanation:

access-list 101 deny tcp 192.168.15.32 0.0.0.15 any eq telnet

access-list 101 permit ip any any

The above two access-list statements are configured on RTB router and placed in outbound direction on S 0/0 interface.

First ACL statement denies all **telnet (port 23)** connections from source address range **192.168.15.32 - 192.168.15.47** to any destination hosts.

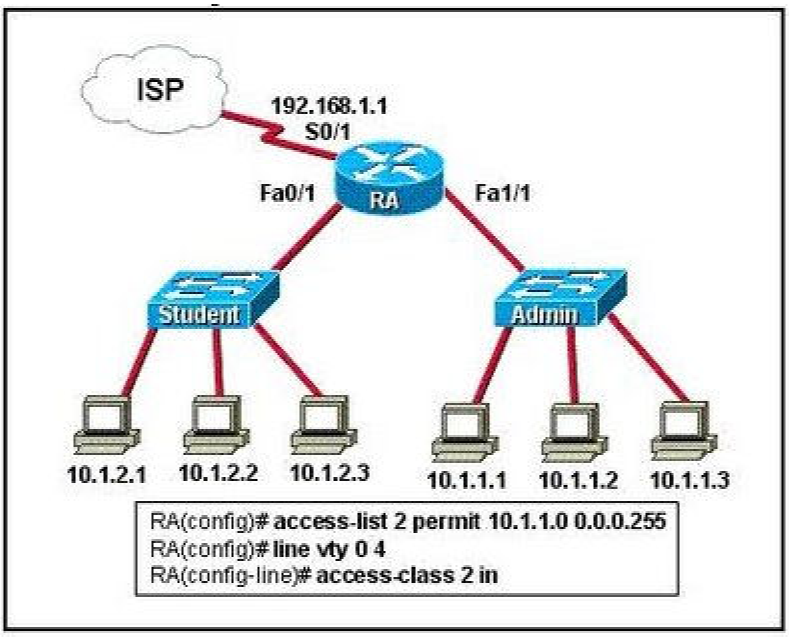
Since we need to find the two packets that will be denied when routed outside s 0/0 interface .

source ip address:, **192.168.15.36** destination port: **23** this matches the ACL statement so this packet is denied.

source ip address: **192.168.15.46**; destination port: **23** also matches the ACL statment so this packet is denied.

Question 3:

Refer to the exhibit. Why would the network administrator configure RA in this manner?



```
RA(config)# access-list 2 permit 10.1.1.0 0.0.0.255
RA(config)# line vty 0 4
RA(config-line)# access-class 2 in
```

A: to give students access to the Internet

B: to prevent students from accessing the command prompt of RA

C: to prevent administrators from accessing the console of RA

D: to give administrators access to the Internet

E: to prevent students from accessing the Internet

F: to prevent students from accessing the Admin network

Answers: B

Explanation:

The above config entered on RA by administrator is to allow only Admin people (10.1.1.0) to access RA command prompt using telnet . Since there is an **implicit deny any** statement at the end of **access-list 2**, so rest all (students) are prevented from accessing command prompt of RA using telnet.

Question 4:

What is the function of the Cisco IOS command ip nat inside source static 10.1.1.5 172.35.16.5?

A: It creates a global address pool for all outside NAT transactions.

B: It establishes a dynamic address pool for an inside static address.

C: It creates dynamic source translations for all inside local PAT transactions.

D: It creates a one-to-one mapping between an inside local address and an inside global address. E: It maps one inside source address to a range of outside global addresses.

Answers: D

Explanation:

This command creates a static NAT translation entry for inside local address(10.1.1.5) to inside global address(172.35.16.5) .

Question 5:

What is the effect of the following access list condition?

access-list 101 permit ip 10.25.30.0 0.0.0.255 any

A: permit all packets matching the first three octets of the source address to all destinations

B: permit all packets matching the last octet of the destination address and accept all source addresses

C: permit all packets from the third subnet of the network address to all destinations

D: permit all packets matching the host bits in the source address to all destinations

E: permit all packets to destinations matching the first three octets in the destination address

Answers: A

Explanation:

The wild card mask (0.0.0.255) " **0**'s in wildcard mask needs a definite match" .

So for the above access-list wildcard mask specifies that it need to match first three octets of source address.

Destination address for the ACL is **any** so it permits all packets that matches the first three octets of source address to all destinations

Question 6:

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

A: the summarized address for all of the internal subnetted addresses

B: the MAC address of the router used by inside hosts to connect to the Internet

C: a globally unique, private IP address assigned to a host on the inside network

D: a registered address that represents an inside host to an outside network

Answers: D

Explanation:

Inside global address— A legitimate IP address assigned by the NIC or service provider that represents one or more inside local IP addresses to the outside world.

Question 7:

What three pieces of information can be used in an extended access list to filter traffic? (Choose three.)

A:protocol

B:VLAN number

C:TCP or UDP port numbers

D:source switch port number

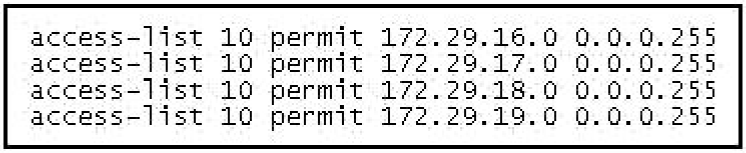
E:source IP address and destination IP address

F:source MAC address and destination MAC address

Answers: A, C, E

Question 8:

An access list was written with the four statements shown in the graphic. Which single access list statement will combine all four of these statements into a single statement that will have exactly the same effect?



```
access-list 10 permit 172.29.16.0 0.0.0.255
access-list 10 permit 172.29.17.0 0.0.0.255
access-list 10 permit 172.29.18.0 0.0.0.255
access-list 10 permit 172.29.19.0 0.0.0.255
```

A: access-list 10 permit 172.29.16.0 0.0.0.255

B: access-list 10 permit 172.29.16.0 0.0.1.255

C: access-list 10 permit 172.29.16.0 0.0.3.255

D: access-list 10 permit 172.29.16.0 0.0.15.255

E: access-list 10 permit 172.29.0.0 0.0.255.255

Answers: C

Explanation:

To combine all four ACL statements into one ACL statement with same effect we need new network that matches all 4 statements network statement and new wildcard mask for the new network we will use.

New Network for the ACL statement: **AND** operation needs to be perform on all four statements.

AND operation: (AND: The output is true only when both inputs A and B are true.)

A - B = **Output**

0 -0 = **0**; 0-1 = **0** ; 1-0 = **0**; 1-1= **1**

Following above AND operations procedure

172.29.16.0 = 10101100.00011101.00010000.00000000

172.29.17.0 = 10101100.00011101.00010001.00000000

172.29.18.0 = 10101100.00011101.00010010.00000000

172.29.19.0 = 10101100.00011101.00010011.00000000

::

172.29.16.0 = 10101100.00011101.00010000.00000000

::

new network after AND operation is **172.29.16.0**

Now to find out Wildcard mask to match all four networks we need to perform **XOR** operations.

XOR operation: (XOR: The output is true when either inputs A or B are true, but not if both A and B are true.)

A - B = **Output**

0 - 0 = **0** ; 0 - 1 = **1** ; 1-0 = **1** ; 1 - 1 = **0**

Following above XOR operations procedure

172.29.16.x = 10101100.00011101.00010000.x

172.29.17.x = 10101100.00011101.00010001.x

172.29.18.x = 10101100.00011101.00010010.x

172.29.19.x = 10101100.00011101.00010011.x

:::

0.0.3.x = 00000000.00000000.00000011.x

:::

Since we are only concern about first three octets the last octet can be 255 so the new wildcard mask is **0.0.3.255**

The complete single acl statement with new network and wildcard mask that matches all four networks is

access-list 10 permit 172.29.16.0 0.0.3.255

Question 9:

An inbound access list has been configured on a serial interface to deny packet entry for TCP and UDP ports 21, 23 and 25. What types of packets will be permitted by this ACL? (Choose three.)

A:FTP

B:Telnet

C:SMTP

D:DNS

E:HTTP

F:POP3

Answers: D, E, F

Explanation:

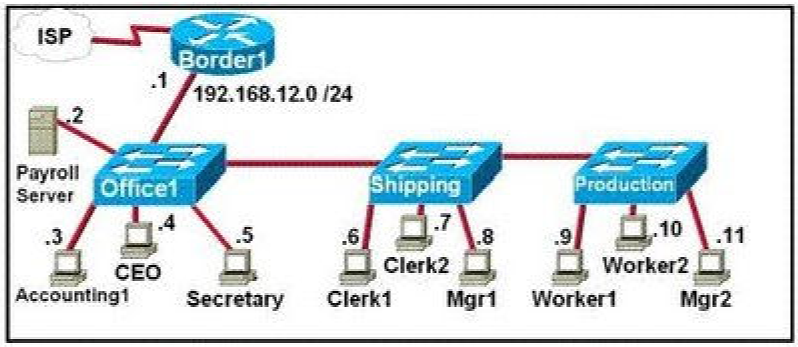
Ports 21, 23 and 25 are denied by ACL.

21 = FTP ; 23= Telnet ; 25= SMTP

Remaining ports are permited so DNS, HTTP and POP3 ports are permitted by ACL.

Quesstion 10:

Refer to the exhibit. The FMJ manufacturing company is concerned about unauthorized access to the Payroll Server. The Accounting1, CEO, Mgr1, and Mgr2 workstations should be the only computers with access to the Payroll Server. What two technologies should be implemented to help prevent unauthorized access to the server? (Choose two.)

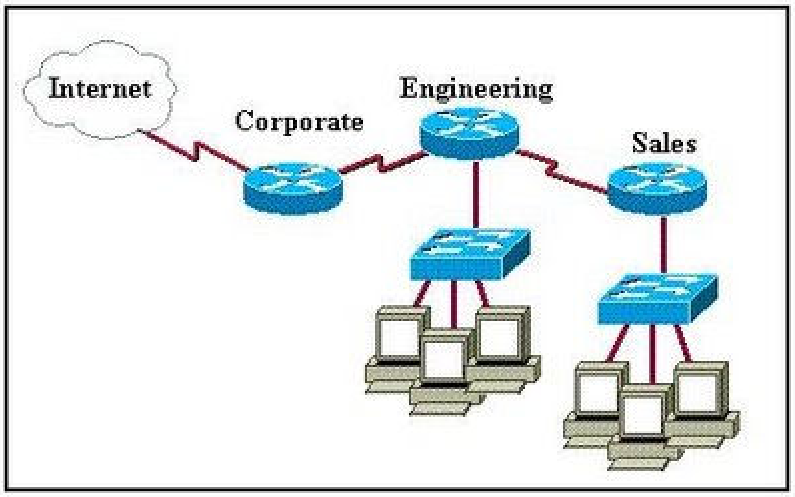


A:access lists
B:encrypted router passwords
C:STP
D:VLANs
E:VTP
F:wireless LANs

Answers: A, D

Explanation:
Access-lists are created to permit only Accounting1, CEO, Mgr1, and Mgr2 workstations to Payroll server.
VLAN can be created which creates a separate Broadcast domain with vlan members only Accounting1, CEO, Mgr1, and Mgr2 workstations including Payroll server.

Question 11:
A network administrator would like to implement NAT in the network shown in the graphic to allow inside hosts to use a private addressing scheme. Where should NAT be configured?



A: Corporate router

B: Engineering router

C: Sales router

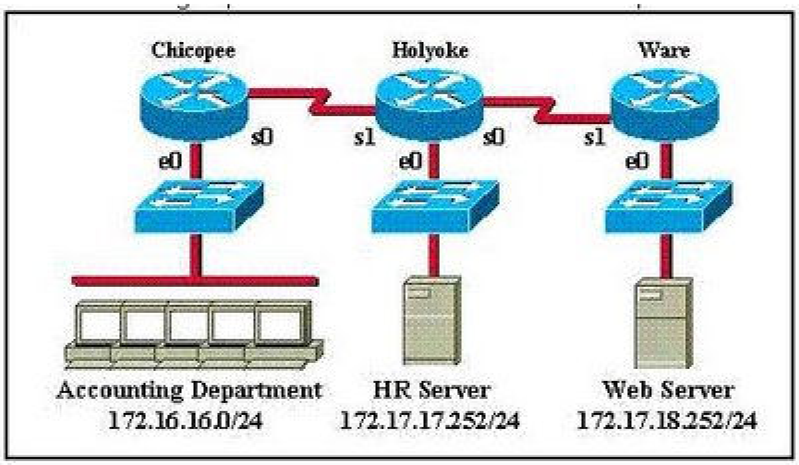
D: all routers

E: all routers and switches

Answers: A

Question 12:

An access list has been designed to prevent HTTP traffic from the Accounting Department from reaching the HR server attached to the Holyoke router. Which of the following access lists will accomplish this task when grouped with the e0 interface on the Chicopee router?



A: permit ip any any

deny tcp 172.16.16.0 0.0.0.255 172.17.17.252 0.0.0.0 eq 80

B: permit ip any any

deny tcp 172.17.17.252 0.0.0.0 172.16.16.0 0.0.0.255 eq 80

C: deny tcp 172.17.17.252 0.0.0.0 172.16.16.0 0.0.0.255 eq 80

permit ip any any

D: deny tcp 172.16.16.0 0.0.0.255 172.17.17.252 0.0.0.0 eq 80

permit ip any any

Answers: D

Explanation:.
We need to create a ACL which denies Account department network from accessing HTTP on HR server.

Source address is account department network: 172.16.16.0 mask 255.255.255.0
Destination address is HR server : 172.17.17.252
Port number for HTTP traffic on destination addresss : 80

First create deny statement
access-list 100 deny tcp 172.16.16.0 0.0.0.255 172.17.17.252 0.0.0.0 80

Since there is a implicit deny any any statement at the end of ACL we need to permit remaining traffic.
access-list 100 permit ip any

4. Implement and verify WAN links

CCNA (640-802) topic Implement and Verify WAN links answers the questions from this topic in exam.

Question 1:

A default Frame Relay WAN is classified as what type of physical network?

A: point-to-point

B: broadcast multi-access

C: nonbroadcast multi-access
D: nonbroadcast multipoint
E: broadcast point-to-multipoint

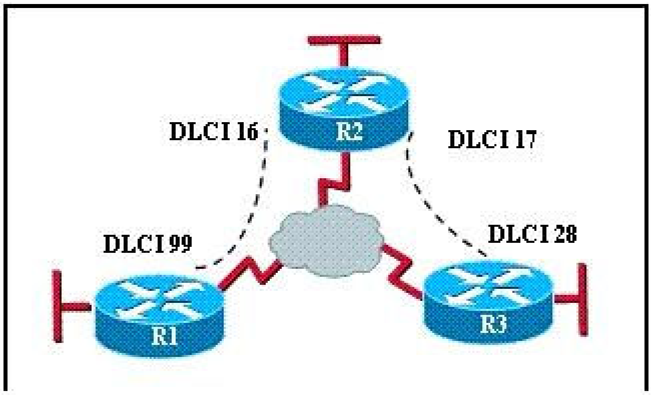
Answers: C

Question 2:
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.

Answers: E

Explanation:
When the frame-relay map command is included in the configuration with the broadcast keyword, it turns Frame Relay network as a broadcast network.

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.

Answers: C

Question 4:

How should a router that is being used in a Frame Relay network be configured to avoid split horizon issues from preventing routing updates?

A: Configure a separate sub-interface for each PVC with a unique DLCI and subnet assigned to the sub-interface.

B: Configure each Frame Relay circuit as a point-to-point line to support multicast and broadcast traffic.

C: Configure many sub-interfaces on the same subnet.

D: Configure a single sub-interface to establish multiple PVC connections to multiple remote router interfaces.

Answers: A

Question 5:

What can a network administrator utilize by using PPP Layer 2 encapsulation? (Choose three.)

A:VLAN support

B:compression

C:authentication

D:sliding windows

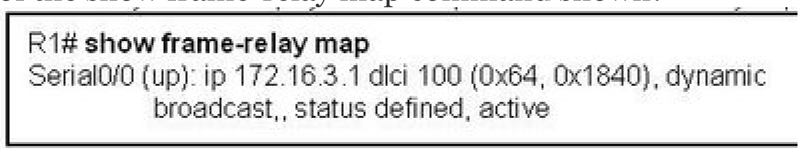
E:multilink support

F:quality of service

Answers: B, C, E

Question 6:

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.

Answers: E

Explanation:
Inverse ARP allows a Frame Relay network to discover the protocol address associated with the virtual circuit dynamically.

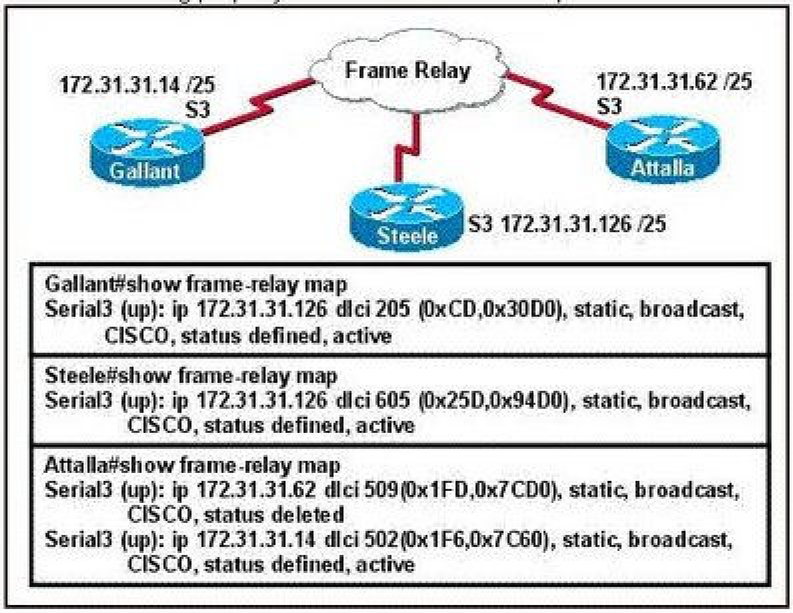
Question 7:
Which of the following describes the roles of devices in a WAN? (Choose three.)
A:A CSU/DSU terminates a digital local loop.
B:A modem terminates a digital local loop.
C:A CSU/DSU terminates an analog local loop.
D:A modem terminates an analog local loop.
E:A router is commonly considered a DTE device.
F:A router is commonly considered a DCE device.

Answers: A, D, E

Question 8:
Which three Layer 2 encapsulation types would be used on a WAN rather than a LAN? (Choose three.)
A:HDLC
B:Ethernet
C:Token Ring
D:PPP
E:FDDI
F:Frame Relay

Answers: A, D, F

Question 9:
The Frame Relay network in the diagram is not functioning properly. What is the cause of the problem?



```
Gallant#show frame-relay map
Serial3 (up): ip 172.31.31.126 dlci 205 (0xCD,0x30D0), static, broadcast,
        CISCO, status defined, active
```

```
Steele#show frame-relay map
Serial3 (up): ip 172.31.31.126 dlci 605 (0x25D,0x94D0), static, broadcast,
          CISCO, status defined, active
```

```
Attalla#show frame-relay map
Serial3 (up): ip 172.31.31.62 dlci 509(0x1FD,0x7CD0), static, broadcast,
          CISCO, status deleted
Serial3 (up): ip 172.31.31.14 dlci 502(0x1F6,0x7C60), static, broadcast,
          CISCO, status defined, active
```

A: The Gallant router has the wrong LMI type configured.

B: Inverse ARP is providing the wrong PVC information to the Gallant router.

C: The S3 interface of the Steele router has been configured with the frame-relay encapsulation ietf command.

D: The frame-relay map statement in the Attalla router for the PVC to Steele is not correct.

E: The IP address on the serial interface of the Attalla router is configured incorrectly.

Answers: D

Explanation:

In above exhibit we need to look at the status of each PVC to identify the problem.
At atlanta we find the show command for first Map **status deleted**. Which is the PVC to Steele because the next map statement in show command is for Gallant and its status is active.

Question 10:

Which of the following are key characteristics of PPP? (Choose three.)

A:can be used over analog circuits

B:maps Layer 2 to Layer 3 address

C:encapsulates several routed protocols

D:supports IP only

E:provides error correction

Answers: A, C, E

Question 11:

A Cisco router that was providing Frame Relay connectivity at a remote site was replaced with a different vendor's frame relay router. Connectivity is now down between the central and remote site. What is the most likely cause of the problem?

A: incorrect IP address mapping

B: mismatched encapsulation types

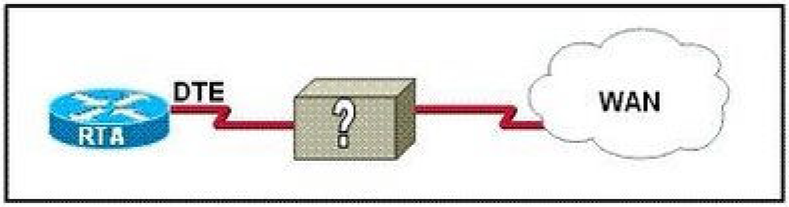
C: incorrect DLCI

D: mismatched LMI types

Answers: B

Question 12:

Refer to the exhibit. The network administrator must complete the connection between the RTA of the XYZ Company and the service provider. To accomplish this task, which two devices could be installed at the customer site to provide a connection through the local loop to the central office of the provider? (Choose two.)



A:WAN switch

B:PVC

C:ATM switch

D:multiplexer

E:CSU/DSU

F:modem

Answers: E, F

Question 13:

When a router is connected to a Frame Relay WAN link using a serial DTE interface, how is the interface clock rate determined?

A: It is supplied by the CSU/DSU.

B: It is supplied by the far end router.

C: It is determined by the clock rate command.

D: It is supplied by the Layer 1 bit stream timing.

5. Topology Based Lab

LAB QUESTION:

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***

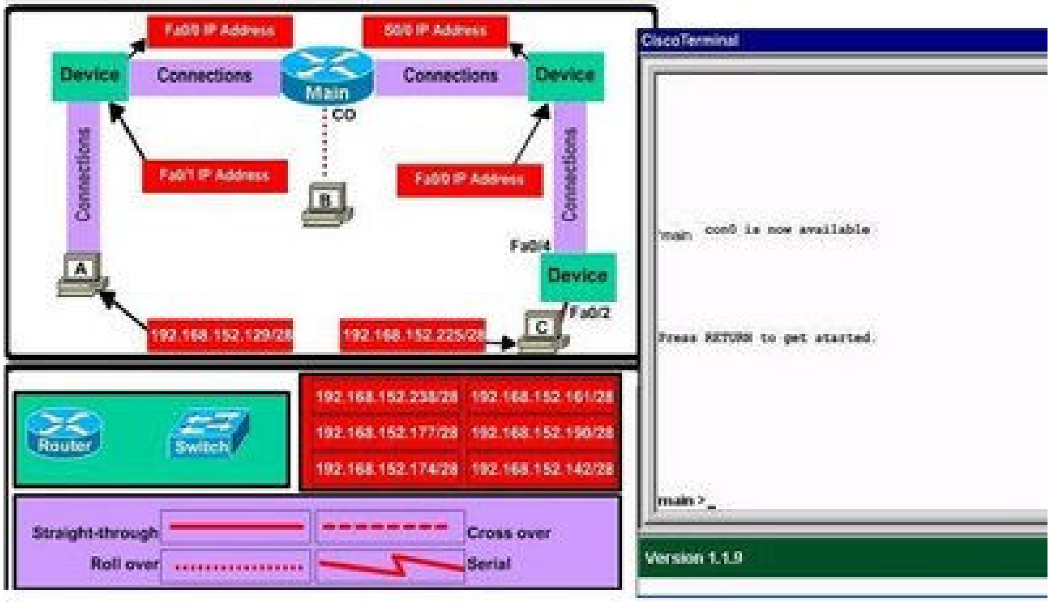
Set the password to allow telnet access to ***telnetpw***

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



```
main con0 is now available



Press RETURN to get started.



main >_
```

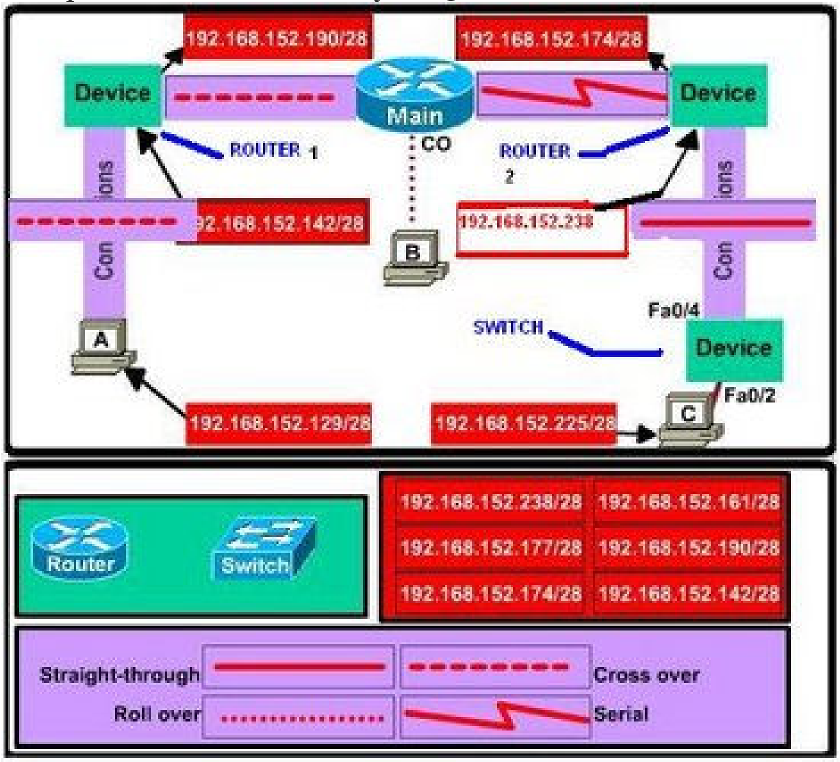
This topology contains 3 routers and 1 switch. Complete the topology.
Drag the appropriate device icons to the locations labeled Device.
Drag the appropriate connections to the locations labeled Connections.
Drag the appropriate IP addresses to the locations labeled IP address. (Hint : Use the given host addresses and the Main router information given)
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. This router does not require configuration.
Configrue each additional router with the following

Configure each additional router with the following
? Configure the interfaces with the correct IP address and enable the interface
? 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:

The question tells us that they are 3 routers and 1 Switch.



Drag the appropriate device icons to the labeled Device

Device Router (1) and Router (2) are connected to main router directly.
We can confirm this because the other Device labeled has Fa 0/2 and Fa 0/4 interfaces therefore this device is a switch.

Drag the appropriate connections to the locations labeled Connections.

1. The Main router is connected over serial link to Router (2) because on Router (2) the exhibit provide S 0/0 IP address icon towards Main router.

2. Router (1) is connected to Main router using a crossover cable. We require a crossover cable to connect two similar devices.

3. To connect host A directly to Router (1) fast ethernet 0/1 we need a crossover cable

4. Straight-through cable is used to connect a router (2) and switch together.

Drag the appropriate IP addresses to the locations labeled IP address (Hint: use the given host addresses and Main router information)

Host A IP address given 192.168.152.129 /28.
Host C IP address given 192.168.152.225 /28

/28 = 11111111. 11111111.11111111.**11110000**
= 255.255.255.**240**
Subnet mask is 255.255.255.240

Various subnet networks and its valid IP address ranges for the above subnet mask

1 – 15
16 – 31
32 – 47
48 – 63
64 – 79
80 – 95

96 – 111

112 -127

128 – 143 (Host A IP address is part of this subnet network IP address range, So Router (1)

Fa 0/1 address is 192.168.152.142)

144 – 159

160 – 175

176 – 191

192 – 207

208 – 223

224 – 239 (Host C IP address is part of this subnet network IP address range, Router (2) Fa 0/0 address is 192.168.1.238)

240 – 255

Use the console of Main router and issue **show running-config** command at enable mode to verify the existing IP address configured on Main router Serial interface so has to identify the Network used in connecting Router (2) over serial link and depending on the network choose the appropriate IP address for S0/0 Router(2).

Similarly verify the Fast Ethernet interface IP address configuration on main router and select a IP address for Router (1) fa 0/0 it should be from same network address range.

Configure Router (1) and Router (2) with the following configuration:

Configure the interfaces with the correct IP address and enable the interfaces.

Router (1): Configuration

```
Router1>enable
Router1#configure terminal
```

```
Router1(config)#interface fa 0/0
```

Assigns IP address to Fa 0/0 and correct subnet mask

```
Router1(config-if)#ip address 192.168.152.190 255.255.255.240
```

Enables the interface

```
Router1(config-if)#no shutdown
```

```
Router1(config-if)#interface fa 0/1
```

Assigns IP address to Fa 0/1 and correct subnet mask

```
Router1(config-if)#ip address 192.168.152.142 255.255.255.240
```

Enables the interface

```
Router1(config-if)#no shutdown
```

Set the console, telnet and privilege mode access password as follows
Console: consolepw ; Telnet: telnetpw ; Privilege mode: privpw

To set console password

```
Router1(config)#line console 0
Router1(config-line)#password consolepw
Router1(config-line)#login
Router1(config-line)#exit
```

To set telnet password

```
Router1(config)#line vty 0 4
Router1(config-line)#password telnetpw
Router1(config-line)#login
Router1(config-line)#exit
```

To set privilege mode password

```
Router1(config)#enable password privpw
```

Router (2): Configuration

```
Router2>enable
Router2#configure terminal
```

```
Router2(config)#interface fa 0/0
```

Assigns IP address to Fa 0/0 and correct subnet mask

```
Router2(config-if)#ip address 192.168.152.238 255.255.255.240
```

Enables the interface

```
Router2(config-if)#no shutdown
```

```
Router2(config-if)#interface serial 0/0
```

Assigns IP address to serial 0/0 and correct subnet mask

```
Router2(config-if)#ip address 192.168.152.174 255.255.255.240
```

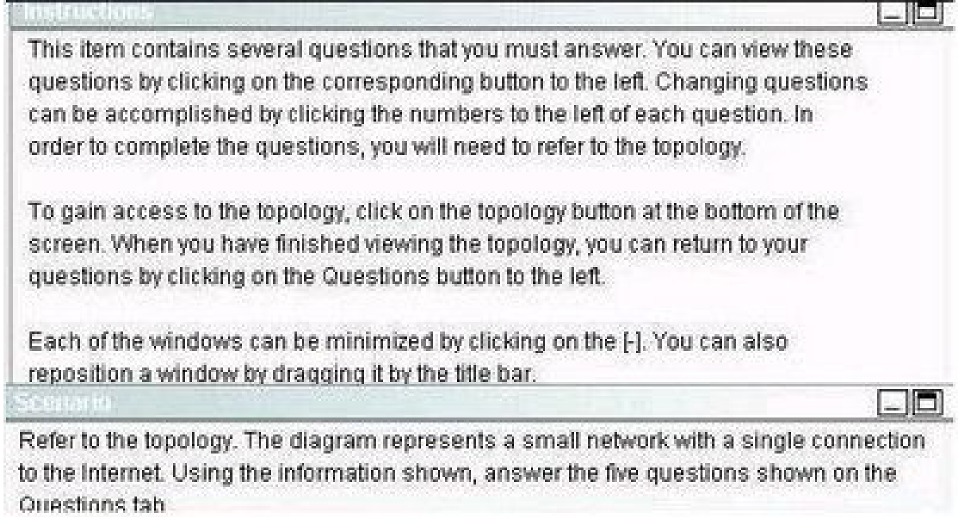
Enables the interface

```
Router2(config-if)#no shutdown
```

Set the console, telnet and privilege mode access password as follows
Console: consolepw ; Telnet: telnetpw ; Privilege mode: privpw

Similar configuration needs to be done for Router (2) to set the passwords for console, telnet and privilege mode as we did for Router(1).

6. Hotspot: Topology Based Questions

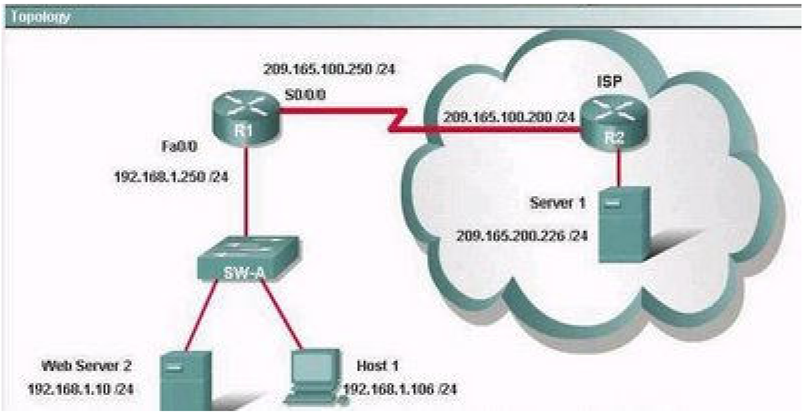


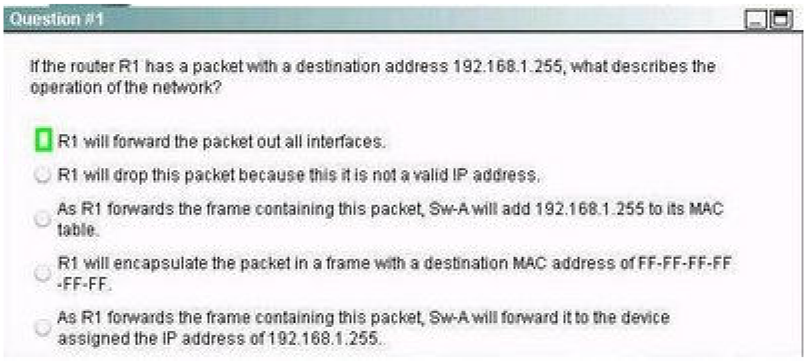
This item contains several questions that you must answer. You can view these questions by clicking on the corresponding button to the left. Changing questions can be accomplished by clicking the numbers to the left of each question. In order to complete the questions, you will need to refer to the topology.

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

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

Refer to the topology. The diagram represents a small network with a single connection to the Internet. Using the information shown, answer the five questions shown on the Questions tab.





If the router R1 has a packet with a destination address 192.168.1.255, what describes the operation of the network?

- ● R1 will forward the packet out all interfaces.
- ○ R1 will drop this packet because this it is not a valid IP address.
- ○ As R1 forwards the frame containing this packet, Sw-A will add 192.168.1.255 to its MAC table.
- ○ R1 will encapsulate the packet in a frame with a destination MAC address of FF-FF-FF-FF-FF-FF.
- ○ As R1 forwards the frame containing this packet, Sw-A will forward it to the device assigned the IP address of 192.168.1.255.

Question 1:

If router has a packet destination address 192.168.1.255. What describes the operation of the network?

Answer:

R1 will drop this packet because it is not a valid ip address

Explanation:

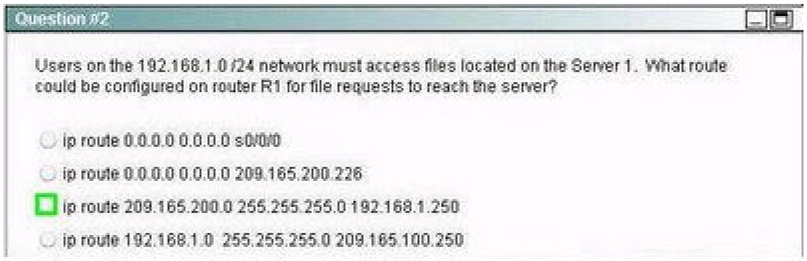
The destination IP address **192.168.1.255** is broadcast address of the network 192168.1.0 /24 on router R1.

Network Address: 192.168.1.0 subnet mask: 255.255.255.0

Network valid host range: 192.168.1.1 – 192.168.1.254

Broadcast Address : 192.168.1.255

Since router (R1) received a packet with destination IP address (192.168.1.255) which is broadcast address so it simply discards the packet as Forwarding broadcast packet can lead to severe storms of packets, and if uncontrolled could lead to network overload.



Question #2

Users on the 192.168.1.0 /24 network must access files located on the Server 1. What route could be configured on router R1 for file requests to reach the server?

○ ip route 0.0.0.0 0.0.0.0 s0/0/0

○ ip route 0.0.0.0 0.0.0.0 209.165.200.226

□ ip route 209.165.200.0 255.255.255.0 192.168.1.250

○ ip route 192.168.1.0 255.255.255.0 209.165.100.250

Question 2:

Users on the 192.168.1.0 /24 network must access files located on the server 1. What route could be configured on router R1 for the file requests to reach the server ?

Answer:

ip route 0.0.0.0 0.0.0.0 s 0/0/0

Explanation:

To enable users on 192.168.1.0 network to access files on server1, we need to establish a default static route.

Static route syntax:

ip route prefix mask {ip-address interface-type interface-number [ip-address]} [distance] [name] [permanent track number] [tag tag]

From the options provided for this question the correct default static route is

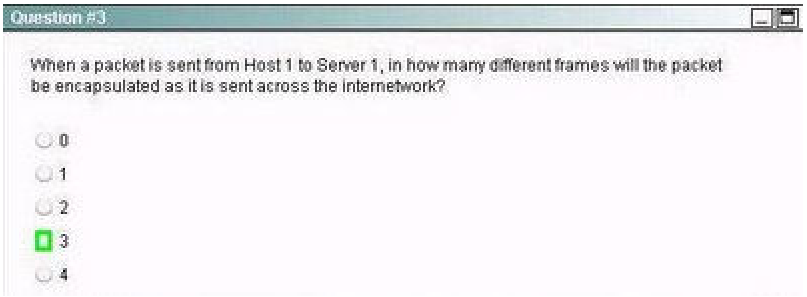
```
ip route 0.0.0.0 0.0.0.0 S 0/0/0
```

PS: As per best practices static route to server1 on R1 should have been

```
ip route 209.165.200.0 255.255.255.0 209.165.100.200
```

(or)

```
ip route 209.165.200.0 255.255.255.0 s 0/0/0
```



When a packet is sent from Host 1 to Server 1, in how many different frames will the packet be encapsulated as it is sent across the internetwork?

○ 0
○ 1
○ 2
☑ 3
○ 4

Question 3:

When a packet is sent from Host1 to Server1,in how many different frames will the packet be encapsulated as it is sent across the internetwork?

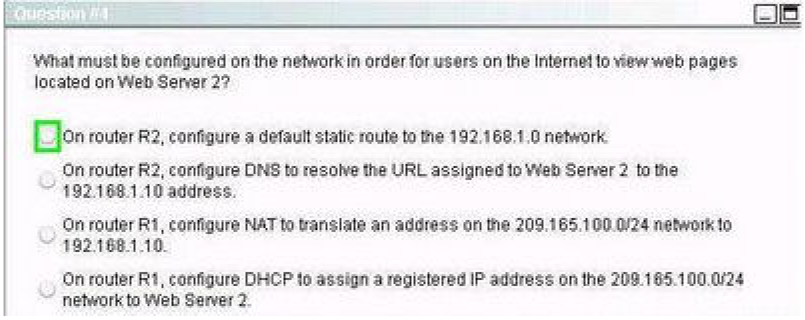
Answer:

3

Explanation:

First: Host1 encapsulates the packet into frames and forwards to the switch. Switch in turn forwards the same frame to router R1.
Second: Router R1 receives the frame on one interface and it is encapsulates into new packet once it leaves the router R1 towards the direction of server1.
Third: R2 receives this packet and it also encapsulates the frame into new packet when it is forwarded to server1 on different interface of R2.

Therefore the packet is sent using three different frames to reach from Host1 to server1.



Question #4

What must be configured on the network in order for users on the Internet to view web pages located on Web Server 2?

☑ On router R2, configure a default static route to the 192.168.1.0 network.

○ On router R2, configure DNS to resolve the URL assigned to Web Server 2 to the 192.168.1.10 address.

○ On router R1, configure NAT to translate an address on the 209.165.100.0/24 network to 192.168.1.10.

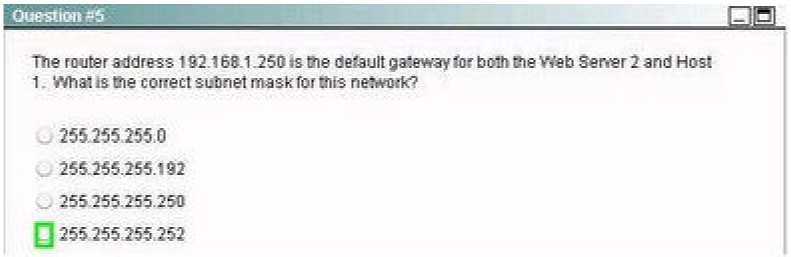
○ On router R1, configure DHCP to assign a registered IP address on the 209.165.100.0/24 network to Web Server 2.

Question 4:

What must be configured on the network in order for users on the internet to view web pages located on web server2?

Answer:

On router R1, configure a NAT to translate address on 209.165.100.0 to 192.168.1.0 network.



Question #5

The router address 192.168.1.250 is the default gateway for both the Web Server 2 and Host 1. What is the correct subnet mask for this network?

○ 255.255.255.0

○ 255.255.255.192

○ 255.255.255.250

☑ 255.255.255.252

Question 5:

The router address 192.168.1.250 is the default gateway for both web server2 and host 1. What is the correct subnet mask for this network?

Answer:

255.255.255.0

Explanation:

Given subnet mask for this network is 255.255.255.0 based on the exhibit.

To find the correct subnet mask for this network based on number of devices shown in the exhibit that are already configured with IP address and by not wasting IP addresses scheme.

The network 192.168.1.0 consists of only three devices as per the exhibits which are configured with IP address.

R1(fa 0/0) : 192.168.1.250 (default gateway as per the question)

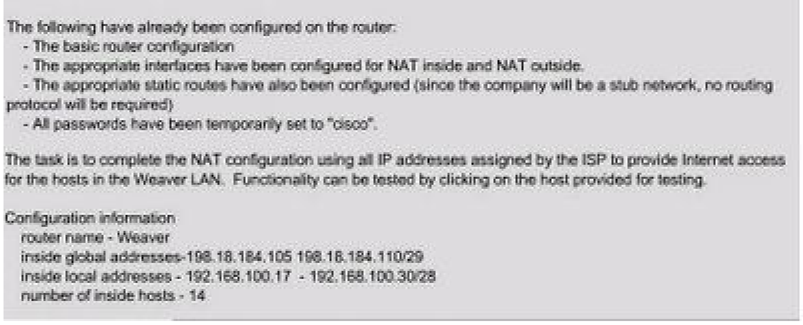
Host1: 192.168.1.10

Web server 2: 192.168.1.106

correct subnet mask that will cover all above IP address is 255.255.255.0

7. CCNA 640-802: NAT SIM

Question: A network associate is configuring a router for the weaver 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 company LAN have been assigned private space addresses in the range of 192.168.100.17 – 192.168.100.30 .

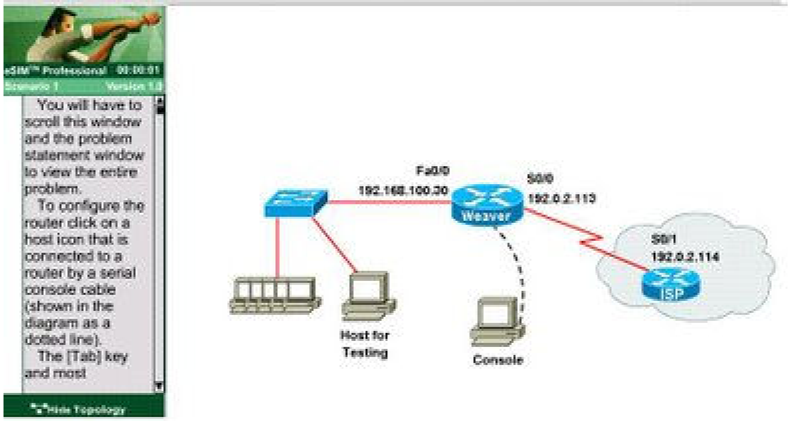


The following have already been configured on the router:

- 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



You will have to scroll this window and the problem statement window to view the entire problem.

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

The [Tab] key and most

Click **Knowledge Base for NAT SIM** to learn the concepts before attempting or learning this SIM Question

NAT SIM Configuration:

The following configuration translates between inside hosts (Weaver LAN) addressed from 192.168.100.16 /28 network (192.168.100.17 – 192.168.100.30) to the globally unique pool of address provided by ISP 198.18.184.105 – 198.18.184.110 /29.

```
Weaver>enable
Weaver#configure terminal
```

Before starting the NAT configuration verify that router hostname currently configured is weaver. If not change hostname to Weaver using the command

```
Router(config)#hostname weaver
```

Step1: Create an access-list to match all the Weaver LAN address that need to be the candidates for NAT translations

```
Weaver(config)#access-list 10 permit 192.168.100.16 0.0.0.15
```

Step2: Create a NAT Pool with pool name isp_adr and specify the pool address range provided by ISP with their netmask.

```
Weaver(config)#ip nat pool isp_adr 198.18.184.105 198.18.184.110 netmask 255.255.255.248
```

Step3: Packets that match access-list 10 will be translated to an address from the pool called "isp_adr".

Overload keyword specify to use Port based NATing to support all the Weaver LAN address range.

```
Weaver(config)#ip nat inside source list 10 pool isp_adr overload
```

SIM Question already provides that appropriate interfaces have been configured for NAT Inside and NAT Outside statements.

For your information configuration would have been like this

```
Weaver(config)#interface fastethernet 0/0
Weaver(config-if)#ip nat inside

Weaver(config)#interface serial 0/0
Weaver(config-if)#ip nat outside
```

Functionality Test:

Our requirements are to allow the hosts (Weaver LAN) the ability to communicate with the Internet. For this test, we ping the Internet device (ISP router S0/1) from Host for testing.

Step1:

Go to **host for testing**:

```
C:\>ping 192.0.2.114
```

PING should be success to 192.0.2.114 since SIM question provides that static route is already configured on router.

Step2:

On console of router (Weaver) :
Issue **show ip nat translation** command to verify the NAT translations.

Sample output:
Considering **host for testing** IP address is 192.168.100.17

```
weaver# show ip nat translation
```

```
Pro Inside global Inside local Outside local Outside global
icmp 198.18.184.105:434 192.168.100.17:434 192.0.2.113:434 192.0.2.114:434
icmp 198.18.184.105:435 192.168.100.17:435 192.0.2.113:435 192.0.2.114:435
icmp 198.18.184.105:436 192.168.100.17:436 192.0.2.113:436 192.0.2.114:436
icmp 198.18.184.105:437 192.168.100.17:437 192.0.2.113:437 192.0.2.114:437
icmp 198.18.184.105:438 192.168.100.17:438 192.0.2.113:438 192.0.2.114:438
```

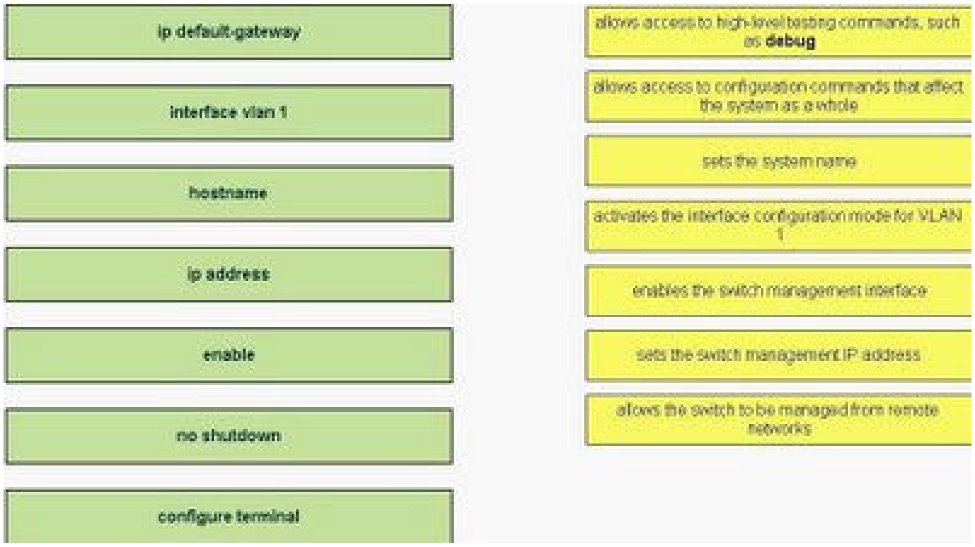
Any Questions on SIMULATOR welcomed.

8. CCNA Exam: Drag & Drop

This section provides all Drag & Drop questions from CCNA Actual Exam.

Question1:

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



ip default-gateway

interface vlan 1

hostname

ip address

enable

no shutdown

configure terminal

allows access to high-level testing commands, such as **debug**

allows access to configuration commands that affect the system as a whole

sets the system name

activates the interface configuration mode for VLAN 1

enables the switch management interface

sets the switch management IP address

allows the switch to be managed from remote networks

Correct order:

Enable

Configure Terminal

Hostname

Interface vlan 1

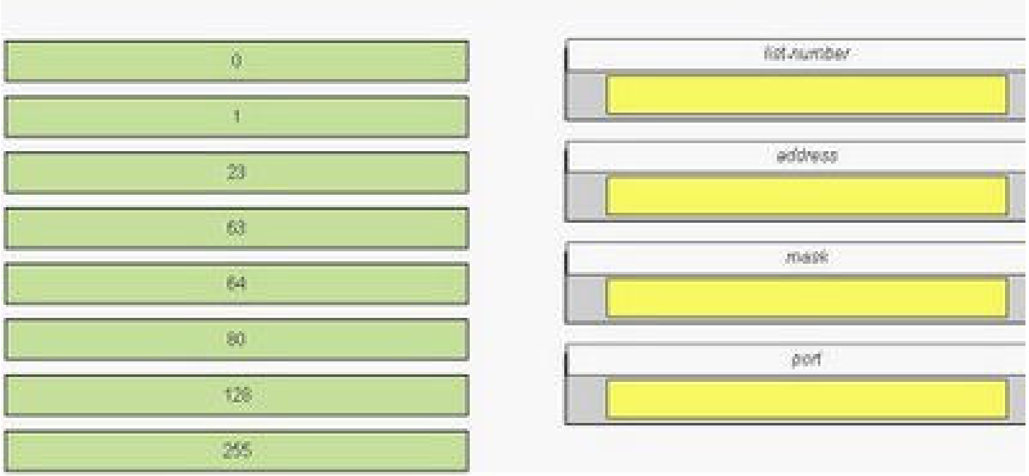
No shutdown

Ip address

Ip default-gateway

Question 2:

All hosts in the same subnet with 172.16.5.118/26 must be denied Telnet access to hosts outside the LAN. 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 is **128** (extended access list)

Address is **64** (network 172.16.5.64 /26)

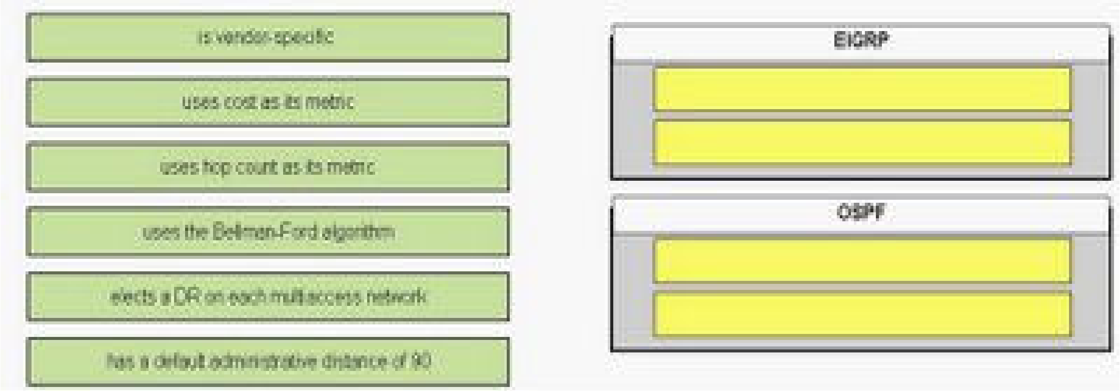
Mask is **63** (wildcard mask 0.0.0.63 to allow 63 hosts)

Port is **23** (telnet port number is 23)

access-list 128 deny tcp 172.16.5.64 0.0.0.63 any eq port 23

Questions 3:

Drag the description on the left to the routing protocol on the right.


is vendor-specific
uses cost as its metric
uses hop count as its metric
uses the Bellman-Ford algorithm
elects a DR on each multiaccess network
has a default administrative distance of 90
EIGRP
OSPF

Answer:

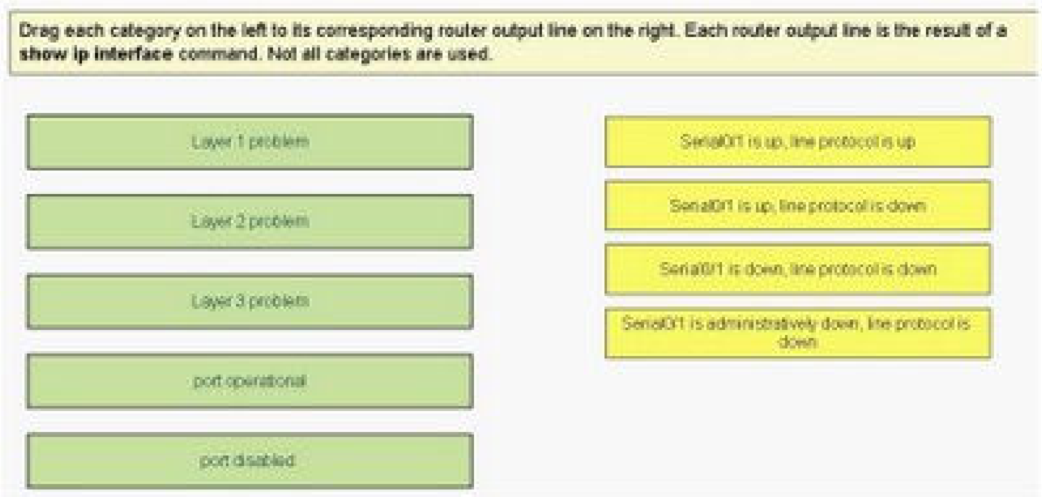
EIGRP:

Is vendor specific and has default administrative distance of 90

OSPF:

elects a DR on each multiaccess network
uses cost as its metric

Question 4:



Drag each category on the left to its corresponding router output line on the right. Each router output line is the result of a **show ip interface** command. Not all categories are used.

Layer 1 problem

Layer 2 problem

Layer 3 problem

port operational

port disabled

Serial0/1 is up, line protocol is up

Serial0/1 is up, line protocol is down

Serial0/1 is down, line protocol is down

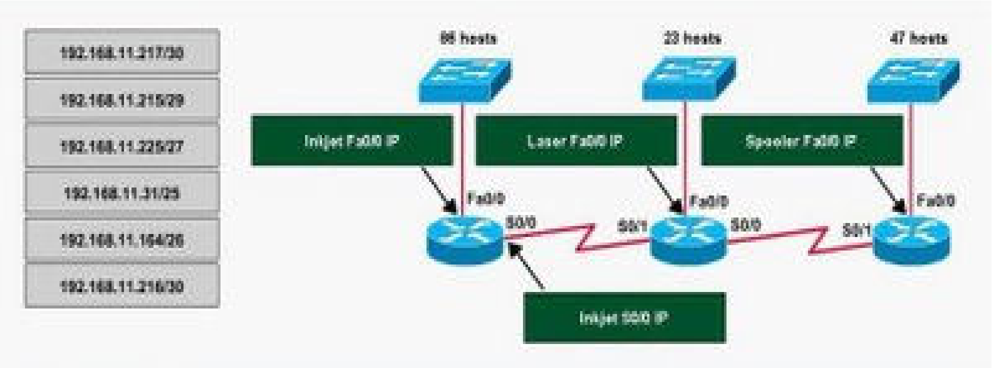
Serial0/1 is administratively down, line protocol is down

Answer:

Serial 0/1 is up, line protocol is up : **Port Operation**
Serial 0/1 is up, line protocol is down: **Layer 2 Problem**
Serial 0/1 is down, line protocol is down: **Layer 1 Problem**
Serial 0/1 is administratively down, line protocol is down: **Port disable**

Question 5:

Printers, inc. is redesigning the network that connects its three locations. The administrator gave tbe networking team 192.168.11.0 to use for addressing the entire network. 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 conserve unused address for future growth. With those goals in mind, drag the host addresses on the left to the correct router interface. One of the routers is partially configured. Move your mouse over a router to view its configuration. Not all of the host address on the left are necessary.



Answer:

Inkjet fa 0/0 IP : **192.168.11.31 /25**

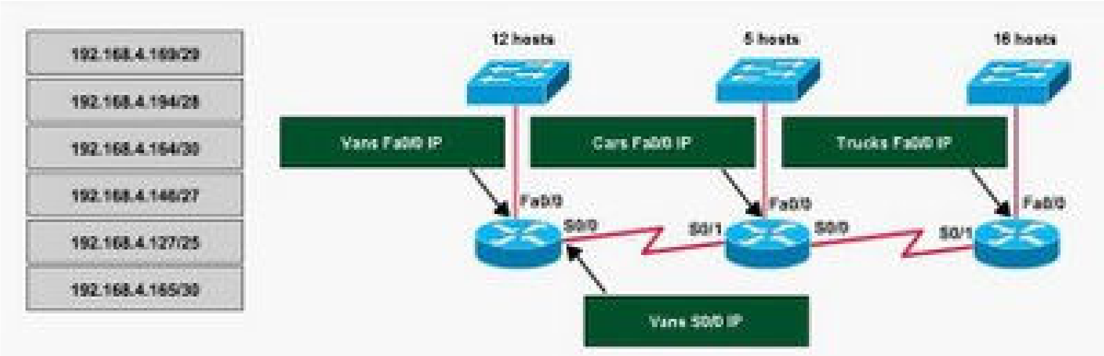
Laser Fa 0/0 IP: **192.168.11.225 /27**

Spooler Fa 0/0 IP: **192.168.11.164 /26**

Inkjet S0/0 IP: **192.168.11.217 /30**

Question 6:

Riverside towing is redesigning the network that connects its three locations. The administrator gave the networking team 192.168.4.0 to use for addressing the entire network. 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 conserve unused address for future growth. With those goals in mind, drag the host addresses on the left to the correct router interface. One of the routers is partially configured. Move your mouse over a router to view its configuration. Not all of the host address on the left are necessary.

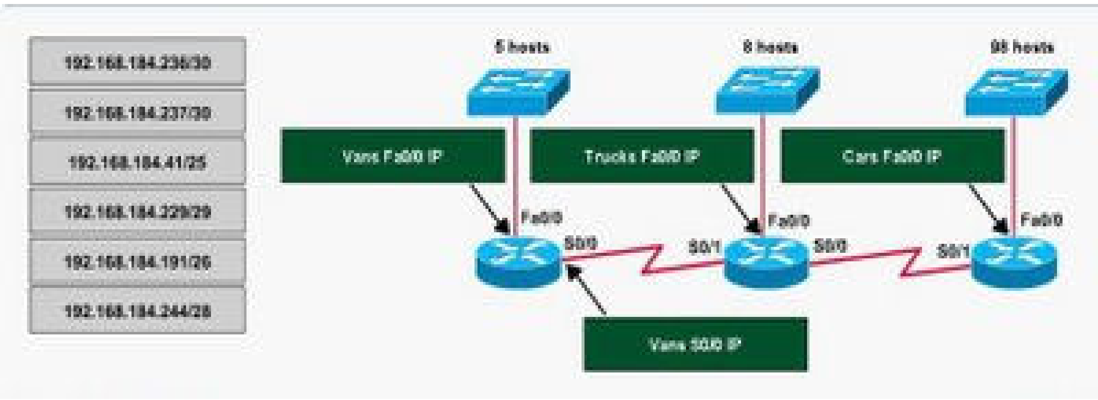


Answer:

Vans 0/0 IP : **192.168.4.194 /28**
Cars Fa 0/0 IP: **192.168.4.169 /29**
Trucks Fa 0/0 IP: **192.168.4.146 /27**
Vans S0/0 IP: **192.168.4.165 /30**

Question 7:

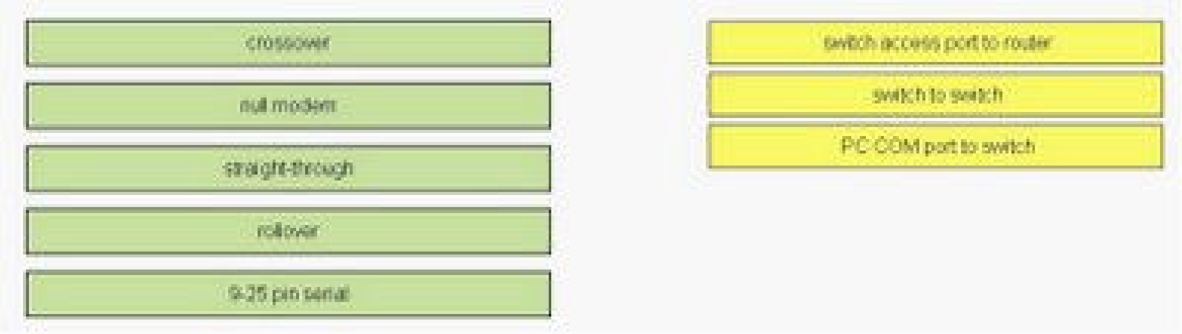
Riverside towing is redesigning the network that connects its three locations. The administrator gave the networking team 192.168.184.0 to use for addressing the entire network. After subnetting the address,the team is ready to assign the addresses. The administrator plans to configure **ip subnet-zero** 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 conserve unused address for future growth. With those goals in mind, drag the host addresses on the left to the correct router interface. One of the routers is partially configured. Move your mouse over a router to view its configuration. Not all of the host address on the left are necessary.



Answer:
Vans fa 0/0 IP : **192.168.184.229 /29**
Trucks Fa 0/0 IP: **192.168.184.244 /28**
Cars Fa 0/0 IP: **192.168.184.41 /25**
Vans S0/0 IP: **192.168.184.237 /30**

Question 8:

Drag the cable type on the left to the purpose for which it is best suited on the right (Not all options are used).


crossover
null modem
straight-through
rollover
9-25 pin serial

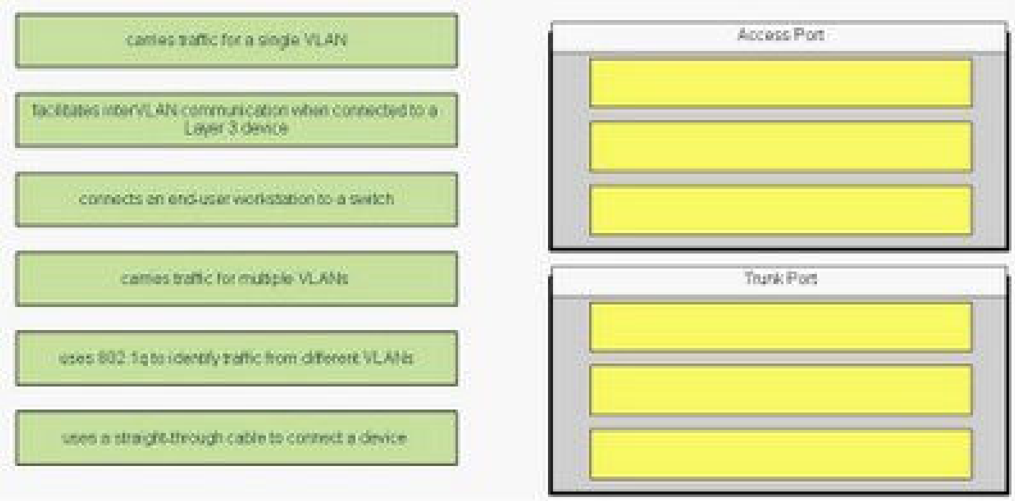
switch access port to router
switch to switch
PC COM port to switch

Answer:

Switch access port to router : **Straight-through**
Switch to switch : **crossover**
PC COM port to switch: **rollover**

Question 9:

Drag the options on the left under the type of switch port that they describe on the right.


carries traffic for a single VLAN
facilitates interVLAN communication when connected to a Layer 3 device
connects an end-user workstation to a switch
carries traffic for multiple VLANs
uses 802.1q to identify traffic from different VLANs
uses a straight-through cable to connect a device

Access Port

Trunk Port

Answer:

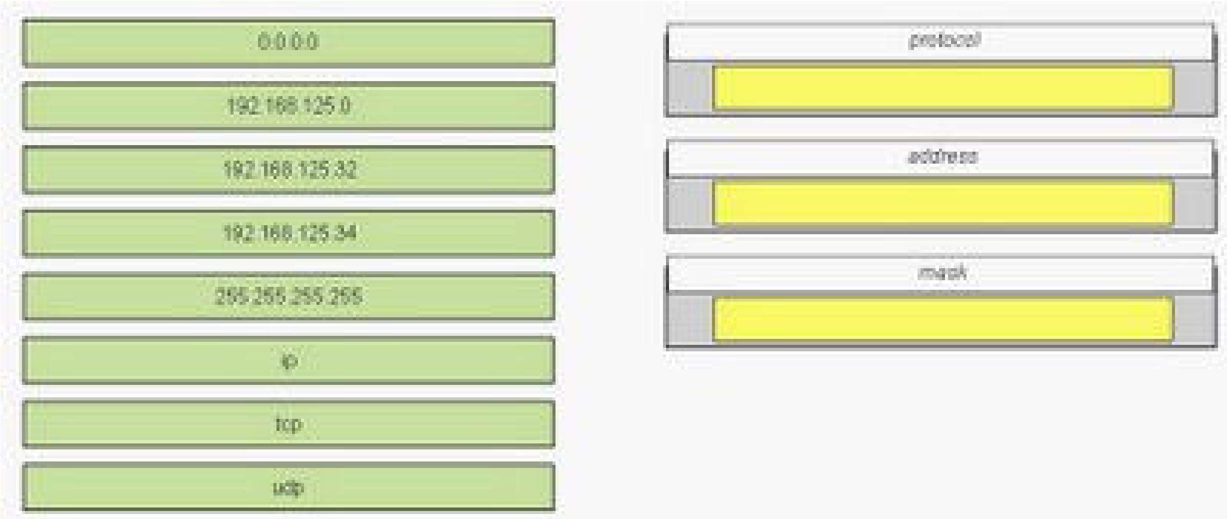
Access Port:
Carries traffic for a single VLAN
Connects an end-user workstation to a switch
Uses a straight-through cable to connect a device.

Trunk Port:

Uses 802.1q to identity traffic from different VLANs
Carries traffic for multiple VLANs
Facilitates interVLAN communication when connected to a Layer3 device

Question 10:

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.



0.0.0.0
192.168.125.0
192.168.125.32
192.168.125.34
255.255.255.255
ip
tcp
udp

protocol

address

mask

Answer:

Protocol : **IP**

Address: **192.168.125.34** (host address)

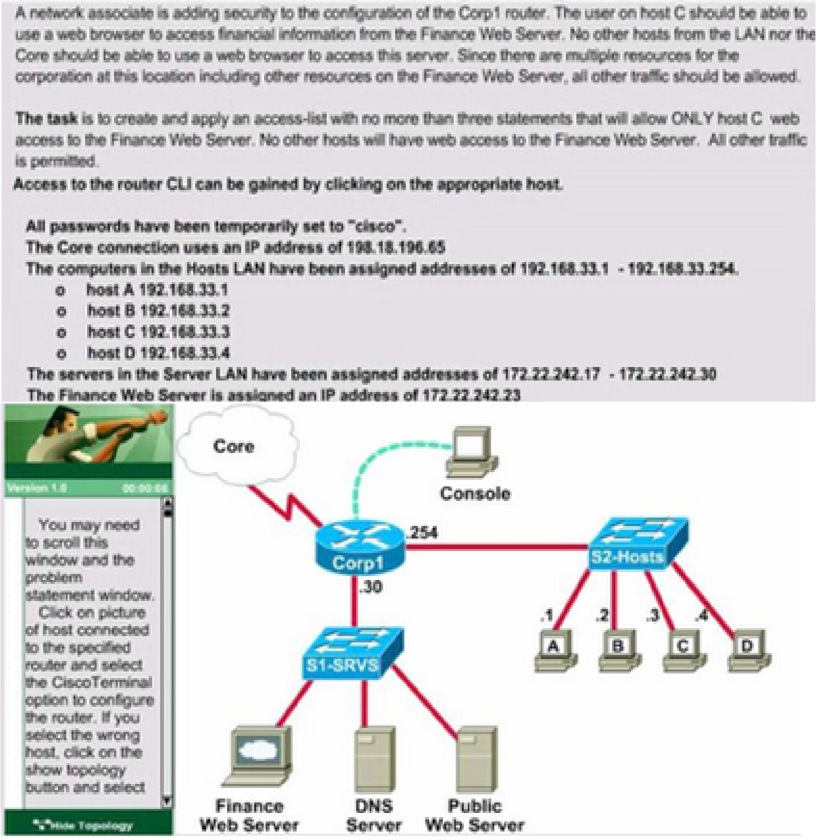
Mask: **0.0.0.0** (wildcard mask for host)

access-list 100 deny ip 192.168.125.34 0.0.0.0 any

9. CCNA Router Simulator Question - ACL SIM

CCNA EXAM HAVE TWO SIMULATORS

ACL SIM



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 an 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

Version 1.0 00:00:08

You may need to scroll this window and the problem statement window. Click on picture of host connected to the specified router and select the CiscoTerminal option to configure the router. If you select the wrong host, click on the show topology button and select

Answer:

Select the **console** on Corp1 router

Configuring ACL

```
Corp1>enable
Corp1#configure terminal
```

comment: To permit only Host C (192.168.33.3){source addr} to access finance server address (172.22.242.23) {destination addr} on port number 80 (web)

```
Corp1(config)#access-list 100 permit tcp host 192.168.33.3 host 172.22.242.23 eq 80
```

comment: To deny any source to access finance server address (172.22.242.23) {destination addr} on port number 80 (web)

```
Corp1(config)#access-list 100 deny tcp any host 172.22.242.23 eq 80
```

comment: To permit ip protocol from any source to access any destination because of the implicit deny any any statement at the end of ACL.

```
Corp1(config)#access-list 100 permit ip any any
```

Applying the ACL on the Interface

Check ***show ip interface brief*** *command to identify the interface type and number* by checking the IP address configured.

```
Corp1(config)#interface fa 0/1
```

If the ip address configured already is incorrect as well as the subnet mask. this should be corrected in order ACL to work

type this commands at interface mode :

no ip address 192.x.x.x 255.x.x.x *(removes incorrect configured ip address and subnet mask)*

Configure Correct IP Address and subnet mask :

ip address 172.22.242.30 255.255.255.240 *(range of address specified going to server is given as 172.22.242.17 - 172.22.242.30)*

comment: Place the ACL to check for packets going outside the interface towards the finance web server.

```
Corp1(config-if)#ip access-group 100 out
```

```
Corp1(config-if)#end
```

Important: To save your running config to startup before exit.

```
Corp1#copy running-config startup-config
```

Verifying the Configuration :

Step1: **show ip interface brief** command identifies the interface on which to apply access list .

Step2: Click on each host A,B,C & D . Host opens a web browser page , Select address box of the web browser and type the ip address of finance web server(172.22.242.23) to test whether it permits /deny access to the finance web Server .

Step 3: Only Host C (192.168.33.3) has access to the server . If the other host can also access then maybe something went wrong in your configuration . check whether you configured correctly and in order.

Step 4: If only Host C (192.168.33.3) can access the Finance Web Server you can click on NEXT button to successfully submit the ACL SIM.

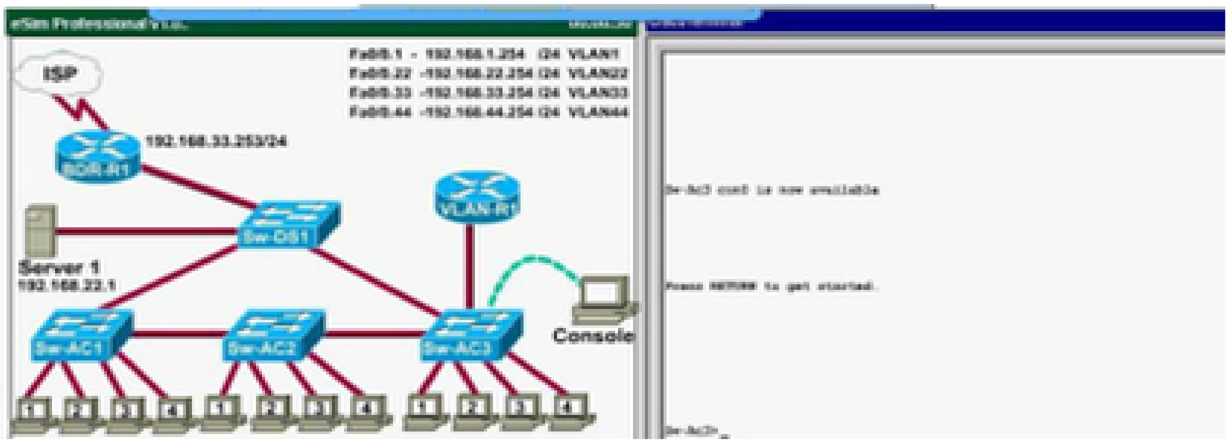
10. CCNA Router Simulator Question - VTP SIM

VTP SIM TESTLET IS ANOTHER SIM EXAM QUESTION

VTP SIM

Question:

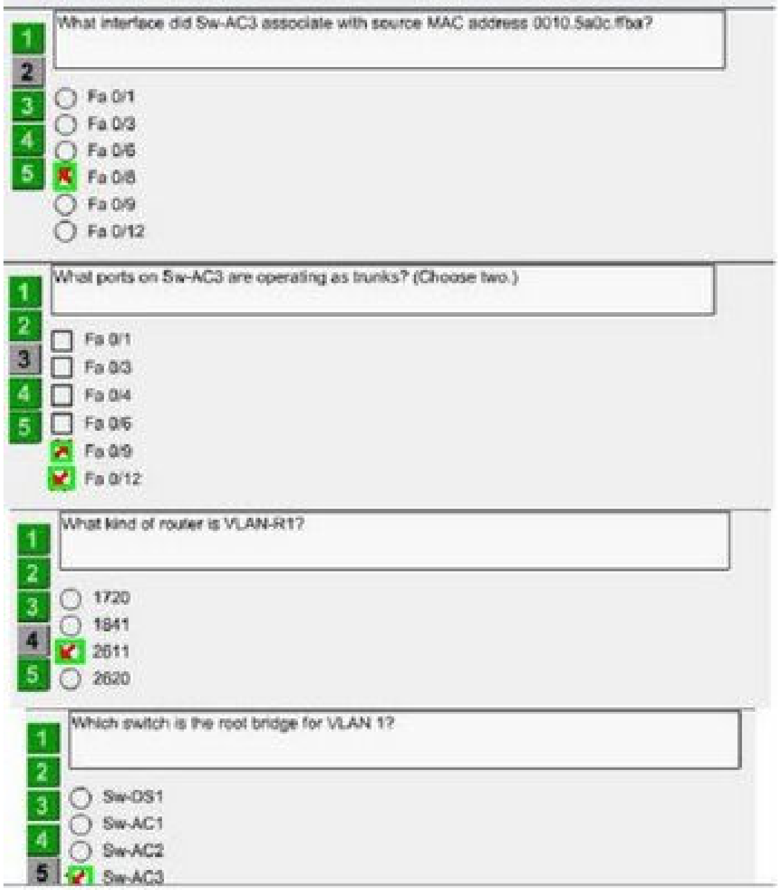
This task requires you to use the CLI of Sw-AC3 to answer five multiple-choice questions. This does not require any configuration.
To answer the multiple-choice questions, click on the numbered boxes in the right panel.
There are five multiple-choice questions with this task. Be sure to answer all five questions before leaving this item.


ISP
Fa0/0.1 - 192.168.1.254 /24 VLAN1
Fa0/0.22 -192.168.22.254 /24 VLAN22
Fa0/0.33 -192.168.33.254 /24 VLAN33
Fa0/0.44 -192.168.44.254 /24 VLAN44
192.168.33.253/24
BDR-R1
VLAN-R1
Sw-DS1
Server 1
192.168.22.1
Sw-AC1
Sw-AC2
Sw-AC3
Console
1
2
3
4
1
2
3
4
1
2
3
4

```
Sw-AC3 con0 is now available

Press RETURN to get started.

Sw-AC3>_
```



What interface did Sw-AC3 associate with source MAC address 0010.5a0c.ffba?

○ Fa 0/1
○ Fa 0/3
○ Fa 0/6
☑ Fa 0/8
○ Fa 0/9
○ Fa 0/12

What ports on Sw-AC3 are operating as trunks? (Choose two.)

□ Fa 0/1
□ Fa 0/3
□ Fa 0/4
□ Fa 0/6
☑ Fa 0/9
☑ Fa 0/12

What kind of router is VLAN-R1?

○ 1720
○ 1841
☑ 2611
○ 2620

Which switch is the root bridge for VLAN 1?

○ Sw-DS1
○ Sw-AC1
○ Sw-AC2
☑ Sw-AC3

Important: *The VTP simlet has a pool of 10 question . Test may have only 5 Questions for VTP SIM*

some very usefull commands to answer this simlet:

show cdp neighbor , show cdp neighbor detail , show interface trunk or switchport , show mac-address-table, show spanning-tree, show vlan , show vtp status , show run .

The pool of 10 questions are discussed here starting with the 4 questions in the above picture.

Question 1 :

What interface did **Sw-AC3** associate with source MAC address 0010.5a0c.ffba ?

Answer:

Fa 0/8 (As per the picture above)

To find out the associate interface number for a given mac address on the switch use the **show mac-address-table** command and search for the mac address 0010.5a0c.ffba and its associated interface number.

Question 2 :

what ports on **Sw-AC3** are operating has trunks (choose two)?

Answer:

Fa 0/9 and Fa 0/12 (As per the picture above)

To find out the ports operating has trunks on a switch

Use the **show interface trunk command** this will display all the trunk ports configured on switch.

(or)

Use the **show interface switchport command** and check the output of the command for operational mode : type trunk for each and every interface.

Question 3:

What kind of router is VLAN-R1 ?

Answer:

2611 (as per picture above)

To know details of directly connected Neighbor, use the following command on the switch **show cdp neighbors** command, this output gives the following details about its neighbors

Device ID, Local Interface ,Holdtme, Capability, **Platform**, Port ID

To know what kind of router is VLAN-R1 we need to identify its **platform** details from above command output.

Question 4:

Which switch is the root bridge for VLAN 1 ?

Answer:

Sw-AC3 (As per the question above in picture)

Step1: Use the Show spanning-tree vlan 1 command this output provide the mac address of the root bridge.

Step2: now use the show mac-address-table command this output associates the mac address to a interface number.

Step3: use the command show cdp neighbors this output will give us the local interface associated with the hostname(Device ID).

Question 5 :

Out of which port on switch **Sw-Ac3** would a frame containing an IP packet with destination address that is not on a local LAN be forwarded?

Answer:

To forward any packet with destination address other then the subnet network of the switch, the switch usually forwards this IP packets to the layer 3 device example router connected to it.

Step1: Find the default-gateway(Router or layer 3 device) configured on the switch.

use the Show run command to view the IP address used to configure default-gateway on the switch.

Step2: Look for the router **VLAN-R1** after using the show cdp neighbor detail command

Sample output of **show cdp neighbor detail** command for better understanding the output details

Device ID: C2950-1

Entry address(es):

Platform: Cisco WS-C2950T-24, Capabilities: Switch IGMP

Interface: FastEthernet0/0, Port ID (outgoing port): FastEthernet0/15

Holdtime : 139 sec

Two things to notice from above output

Interface: FastEthernet0/0 this statement provides that the neighbor(c2950-1) is connected to fa 0/0 on the c3660-2 local switch.

Port ID (outgoing port): FastEthernet0/15 this explains that neighbor (c2950-1) uses fa 0/15 port to reach c3660-2 switch.

FOR OUR QUESTION WE SHOULD LOOK FOR THE ROUTER VLAN-R1 corresponding details and to which port it is connected on local switch Sw-Ac3.

Step3: The port number to which the routerVLAN-R1 is connected on switch Sw-Ac3 is used to forward the packets with destination address that is not on a local LAN.

Question 6:

What address should be configured as the default-gateway for the host connected to interface fa 0/4 of **SW-Ac3** ?

Answer:

Step1: Find the details of the VLAN assigned to interface fa 0/4 by using the **show vlan** command on Sw-Ac3.

The above exhibit question has fa 0/4 configured has VLAN1 based on the output from **show vlan** command.

Step2: From the exhibit question we know that VLAN1 is configured on router using sub-interface fa 0/0.1 with IP address 192.168.1.254 /24.

Step3: 192.168.1.254 should be configure as default-gateway address for the host connected to fa 0/4 on switch.

Because VLAN1 corresponds to fa 0/4 on Sw-Ac3 and host connected to fa 0/4 will be member of vlan1.

Question 7:

Out of which ports will frame with source mac-address 0015.5A0Cc.A086 and destination mac-address 000A.8A47.0612 be forwarded ?

Answer:

Step1: Use **Show mac-address-table** command on the switch.

The output of a show mac-address-table provides the mapping of mac address with port numbers. Search the output for the two mac-addresses provided in the question and select the destination mac address corresponding port number for correct answers.

Step2: If you do not find the above destination mac-address in SHOW MAC-ADDRESS-TABLE output , then the frame will be broadcast or flooded to all ports (*all ports may be ports of particular vlan on switch ,Selection of VLAN will be depending on the source mac-address port vlan membership*) except the port it recieved from.

Question 8:

From which switch did **Sw-Ac3** receive VLAN information ?

Answer:

Step1: Use Sw-Ac3#**show vtp status** command .

Sample output of show vtp status command

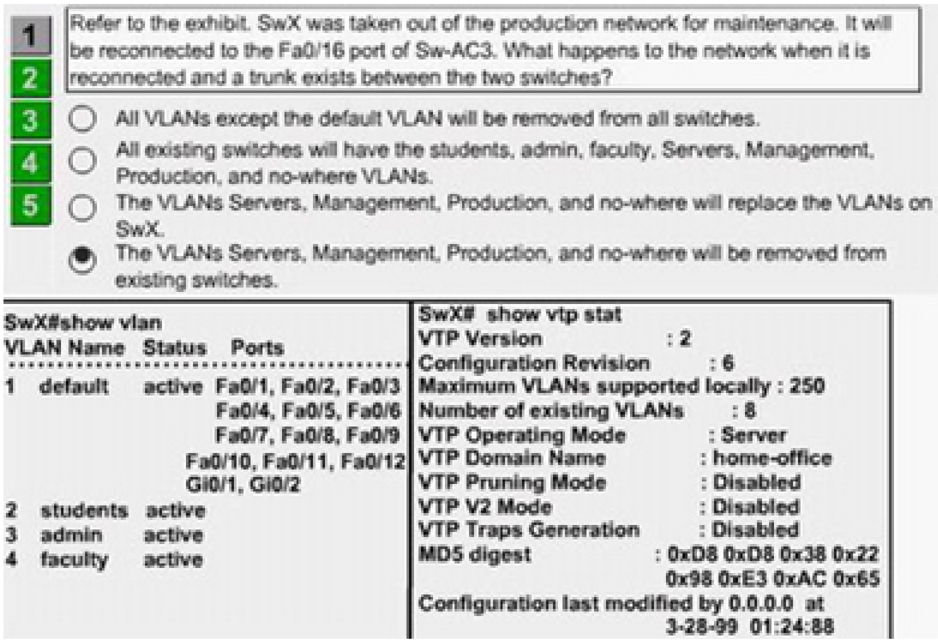
```
switch# show vtp status
VTP Version : 2
Configuration Revision : 255
Maximum VLANs supported locally : 1005
Number of existing VLANs : 35
VTP Operating Mode : Server
VTP Domain Name : Lab_Network
VTP Pruning Mode : Enabled
VTP V2 Mode : Enabled
VTP Traps Generation : Disabled
MD5 digest : 0x08 0x7E 0x54 0xE2 0x5A 0x79 0xA9 0x2D
Configuration last modified by 127.0.0.12 at 8-7-02 11:21:43
Local updater ID is 127.0.0.12 on interface E00/0 (first interface found)
```

The local updater ID in the above output identifies the ip address of the device which is providing the VLAN information. The address could also be of the switch itself.

Step 2: Show cdp neighbor detail provides the hostname for corresponding to that IP address.

Question 9:

Refer to the exhibit. **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?



Refer to the exhibit. SwX was taken out of the production network for maintenance. It will be reconnected to the Fa0/16 port of Sw-AC3. What happens to the network when it is reconnected and a trunk exists between the two switches?

○ All VLANs except the default VLAN will be removed from all switches.

○ All existing switches will have the students, admin, faculty, Servers, Management, Production, and no-where VLANs.

○ The VLANs Servers, Management, Production, and no-where will replace the VLANs on SwX.

● The VLANs Servers, Management, Production, and no-where will be removed from existing 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
```

Answer:

Step1: On switch **Sw-Ac3** use **show vtp status** command. Notice the output for domain name, Both switches must have same domain name configured to exchange vtp messages (exhibit domain name: home-office).

Step2: If domain name matches, Then note **Configuration Revision number** of the **Sw-Ac3** and compare it with the **SwX ,** Whichever switch has highest configuration revision number will become the vtp updater. The switch which becomes vtp updater will replace other switch vlan information with its own vlan information.

Example if **SwX** revision number is highest , Then VLAN information that is configured in **Sw-Ac3** will be replaced by the VLAN information in the **SwX.**