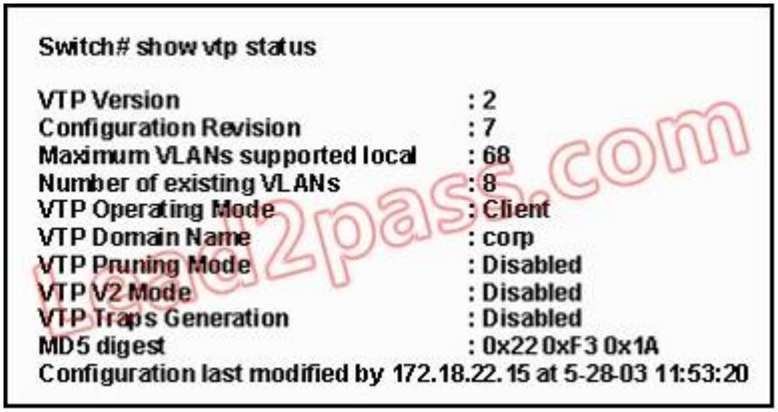
the entire router.
An example of a global command is one used for the hostname of the router.

QUESTION 321
An administrator is unsuccessful in adding VLAN 50 to a switch. While troubleshooting the problem, the administrator views the output of the show vtp status command, which is displayed in the graphic. What commands must be issued on this switch to add VLAN 50 to the database? (Choose two.)



```
Switch# show vtp status

VTP Version                          : 2
Configuration Revision               : 7
Maximum VLANs supported local        : 68
Number of existing VLANs             : 8
VTP Operating Mode                   : Client
VTP Domain Name                      : corp
VTP Pruning Mode                     : Disabled
VTP V2 Mode                          : Disabled
VTP Traps Generation                 : Disabled
MD5 digest                           : 0x22 0xF3 0x1A
Configuration last modified by 172.18.22.15 at 5-28-03 11:53:20
```

A. `Switch(config-if)# switchport access vlan 50`
B. `Switch(vlan)# vtp server`
C. `Switch(config)# config-revision 20`
D. `Switch(config)# vlan 50 name Tech`
E. `Switch(vlan)# vlan 50`
F. `Switch(vlan)# switchport trunk vlan 50`

Answer: BE

QUESTION 322
Which of the following IP addresses fall into the CIDR block of 115.64.4.0/22? (Choose three.)

A. 115.64.8.32
B. 115.64.7.64
C. 115.64.6.255
D. 115.64.3.255
E. 115.64.5.128
F. 115.64.12.128

Answer: BCE

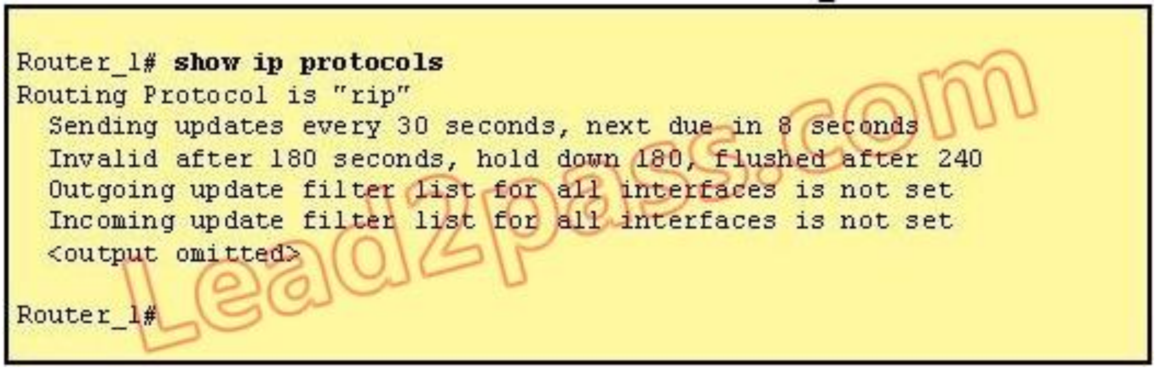
QUESTION 323
Which of the following are types of flow control? (Choose three.)

A. buffering
B. cut-through
C. windowing

D. congestion avoidance
E. load balancing

Answer: ACD

QUESTION 324
Refer to the exhibit. After a RIP route is marked invalid on Router_1, how much time will elapse before that route is removed from the routing table?

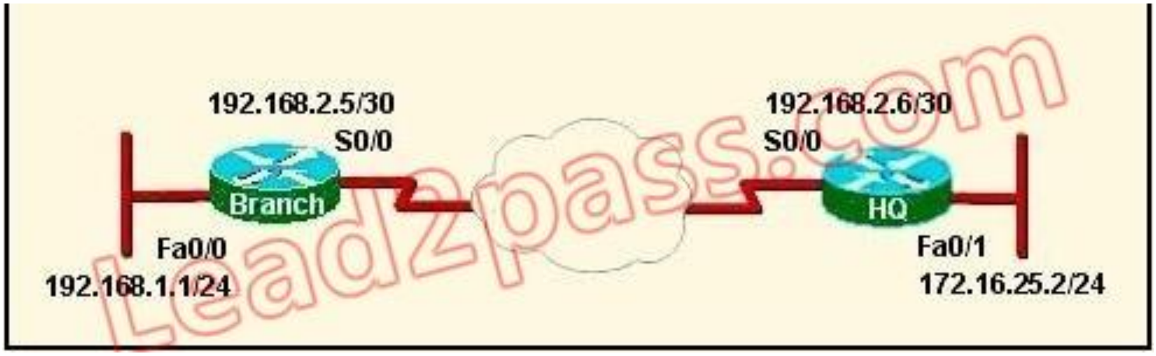


```
Router_1# show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 8 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  <output omitted>

Router_1#
```

A. 30 seconds
B. 60 seconds
C. 90 seconds
D. 180 seconds
E. 240 seconds

Answer: E

QUESTION 325
Refer to the exhibit. A network associate has configured the internetwork that is shown in the exhibit, but has failed to configure routing properly.



Which configuration will allow the hosts on the Branch LAN to access resources on the HQ LAN with the least impact on router processing and WAN bandwidth?

A. `HQ(config)# ip route 192.168.1.0 255.255.255.0 192.168.2.5`
`Branch(config)# ip route 172.16.25.0 255.255.255.0 192.168.2.6`
B. `HQ(config)# router rip`

```
HQ(config-router)# network 192.168.2.0
HQ(config-router)# network 172.16.0.0
Branch(config)# router rip
Branch(config-router)# network 192.168.1.0
Branch(config-router)# network 192.168.2.0
```

C.
```
HQ(config)# router eigrp 56
HQ(config-router)# network 192.168.2.4
HQ(config-router)# network 172.16.25.0
Branch(config)# router eigrp 56
Branch(config-router)# network 192.168.1.0
Branch(config-router)# network 192.168.2.4
```

D.
```
HQ(config)# router ospf 1
HQ(config-router)# network 192.168.2.4 0.0.0.3 area 0
HQ(config-router)# network 172.16.25.0 0.0.0.255 area 0
Branch(config)# router ospf 1
Branch(config-router)# network 192.168.1.0 0.0.0.255 area 0
```

Answer: A

QUESTION 326
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. Configured MAC address filtering to permit the client to connect to the AP.

Answer: C

QUESTION 327
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.

Answer: D

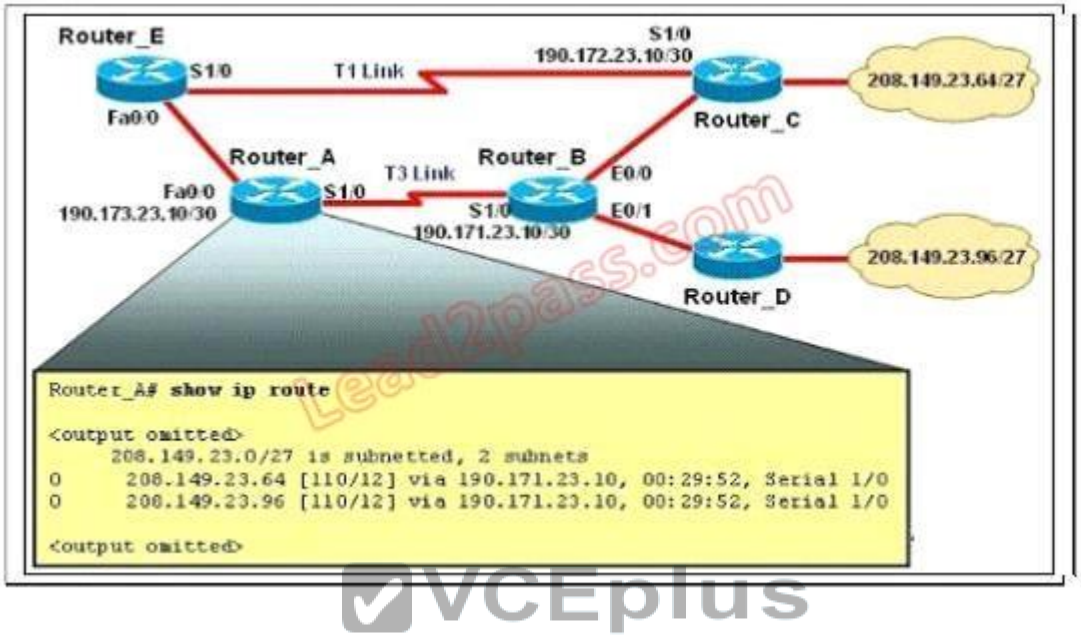
QUESTION 328
All WAN links inside the ABC University network use PPP with CHAP for authentication security. Which command will display the CHAP authentication process as it occur between two routers in the network?

A. `show chap authentication`
B. `show interface serial0`
C. `debug ppp authentication`
D. `debug chap authentication`
E. `show ppp authentication chap`

Answer: C

QUESTION 329

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



```
Router_A# show ip route

<output omitted>
     208.149.23.0/27 is subnetted, 2 subnets
O      208.149.23.64 [110/12] via 190.171.23.10, 00:29:52, Serial 1/0
O      208.149.23.96 [110/12] via 190.171.23.10, 00:29:52, Serial 1/0

<output omitted>
```

A. 208.149.23.64[110/13] via 190.173.23.10, 00:00:00:07, FastEthernet0/0
   208.149.23.96[110/13] via 190.173.23.10, 00:00:00:16, FastEthernet0/0

B. 208.149.23.64[110/1] via 190.173.23.10, 00:00:00:07, Serial1/0
   208.149.23.96[110/3] via 190.173.23.10, 00:00:00:16, FastEthernet0/0

C. 208.149.23.64[110/13] via 190.173.23.10, 00:00:00:07, Serial1/0
   208.149.23.96[110/13] via 190.173.23.10, 00:00:00:16, Serial1/0
   208.149.23.96[110/13] via 190.173.23.10, 00:00:00:16, FastEthernet0/0

D. 208.149.23.64[110/13] via 190.173.23.10, 00:00:00:07, Serial1/0
   208.149.23.96[110/13] via 190.173.23.10, 00:00:00:16, Serial1/0

Answer: A

QUESTION 330

What are two characteristics of SSH? (Choose two.)

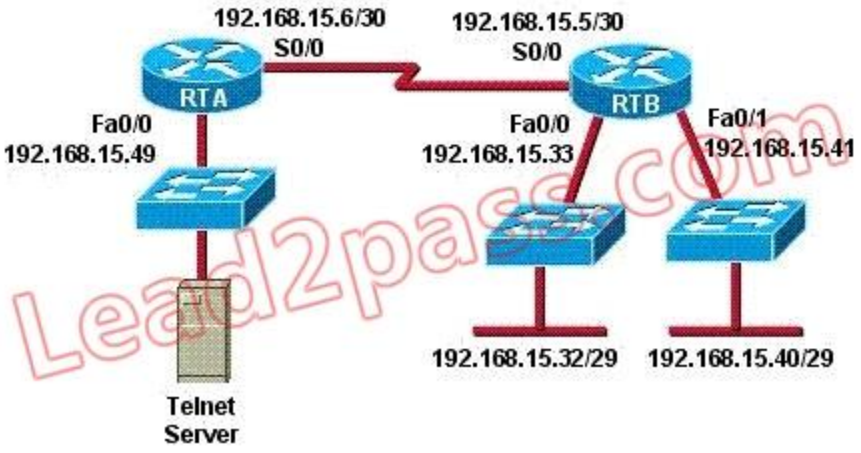
A. most common remote-access method
B. unsecured
C. encrypted
D. uses port 22
E. operates at the transport layer

Answer: DE

QUESTION 331

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
```

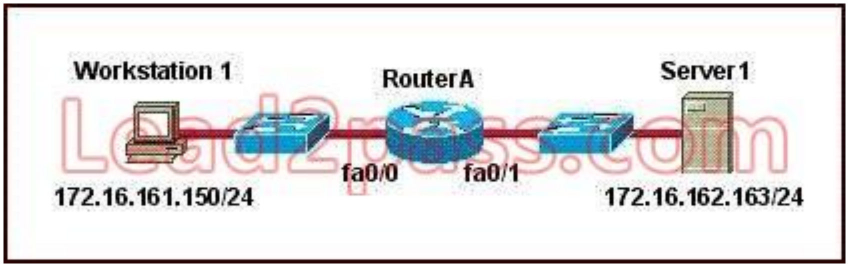


A. `source ip address: 192.168.15.5; destination port: 21`
B. `source ip address:, 192.168.15.37 destination port: 21`
C. `source ip address:, 192.168.15.41 destination port: 21`
D. `source ip address:, 192.168.15.36 destination port: 23`
E. `source ip address: 192.168.15.46; destination port: 23`
F. `source ip address:, 192.168.15.49 destination port: 23`

Answer: DE

QUESTION 332

Refer to the graphic. It has been decided that Workstation 1 should be denied access to Server1. Which of the following commands are required to prevent only Workstation 1 from accessing Server1 while allowing all other traffic to flow normally? (Choose two.)

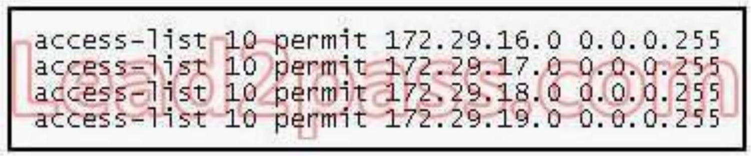


A. RouterA(config)# interface fa0/0
RouterA(config-if)# ip access-group 101 out
B. RouterA(config)# interface fa0/0
RouterA(config-if)# ip access-group 101 in
C. RouterA(config)# access-list 101 deny ip host 172.16.161.150 host 172.16.162.163
RouterA(config)# access-list 101 permit ip any any
D. RouterA(config)# access-list 101 deny ip 172.16.161.150 0.0.0.255 172.16.162.163 0.0.0.0

RouterA(config)# access-list 101 permit ip any any

Answer: BC

QUESTION 333
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`

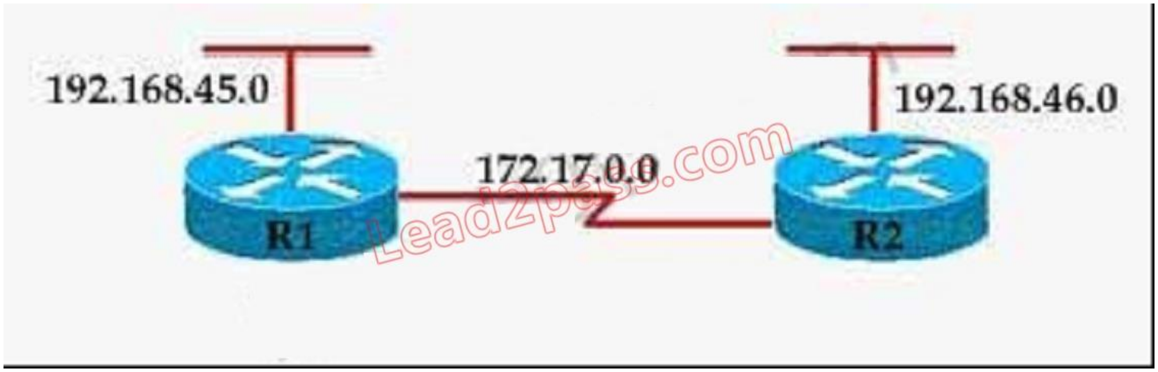
Answer: C

QUESTION 334
A network administrator wants to add a line to an access list that will block only Telnet access by the hosts on subnet 192.168.1.128/28 to the server at 192.168.1.5. What command should be issued to accomplish this task?

A.
```
access-list 101 deny tcp 192.168.1.128 0.0.0.15 192.168.1.5 0.0.0.0 eq 23
access-list 101 permit ip any any
```
B.
```
access-list 101 deny tcp 192.168.1.128 0.0.0.240 192.168.1.5 0.0.0.0 eq 23
access-list 101 permit ip any any
```
C.
```
access-list 1 deny tcp 192.168.1.128 0.0.0.255 192.168.1.5 0.0.0.0 eq 21
access-list 1 permit ip any any
```
D.
```
access-list 1 deny tcp 192.168.1.128 0.0.0.15 host 192.168.1.5 eq 23
access-list 1 permit ip any any
```

Answer: A

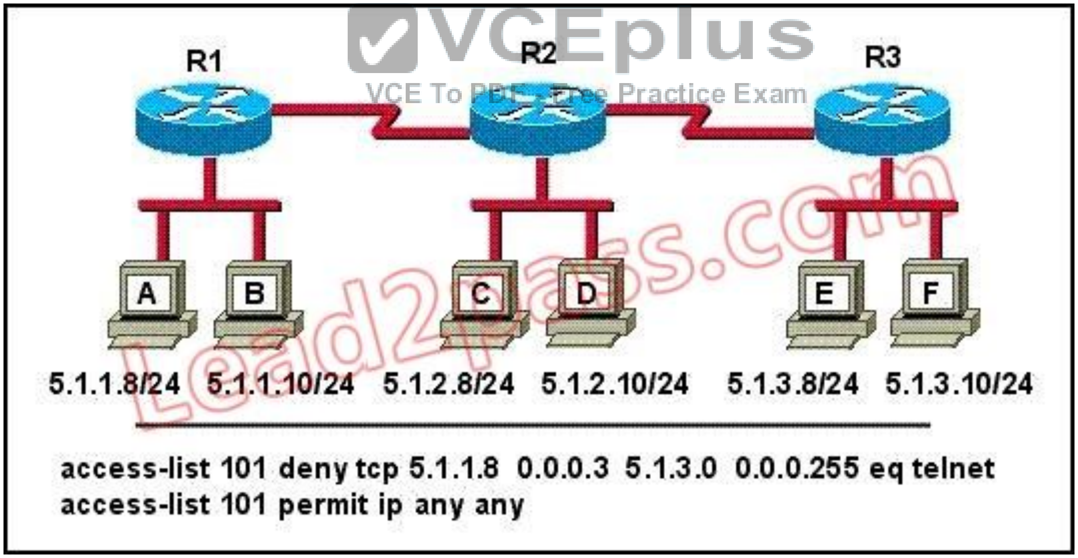
QUESTION 335
As a network administrator, you have been instructed to prevent all traffic originating on the LAN from entering the R2 router.
Which the following command would implement the access list on the interface of the R2 router?



A. access-list 101 in
B. access-list 101 out
C. ip access-group 101 in
D. ip access-group 101 out

Answer: C

QUESTION 336
The access control list shown in the graphic has been applied to the Ethernet interface of router R1 using the ip access-group 101 in command.
Which of the following Telnet sessions will be blocked by this ACL? (Choose two.)



```
access-list 101 deny tcp 5.1.1.8  0.0.0.3  5.1.3.0  0.0.0.255 eq telnet
access-list 101 permit ip any any
```

A. from host A to host 5.1.1.10
B. from host A to host 5.1.3.10
C. from host B to host 5.1.2.10
D. from host B to host 5.1.3.8
E. from host C to host 5.1.3.10
F. from host F to host 5.1.1.10

Answer: BD

QUESTION 337
The following access list below was applied outbound on the E0 interface connected to the 192.169.1.8/29 LAN: access-list 135 deny tcp 192.169.1.8 0.0.0.7 eq 20 any access-list 135 deny tcp 192.169.1.8 0.0.0.7 eq 21 any How will the above access lists affect traffic?

A. FTP traffic from 192.169.1.22 will be denied
B. No traffic, except for FTP traffic will be allowed to exit E0
C. FTP traffic from 192.169.1.9 to any host will be denied
D. All traffic exiting E0 will be denied
E. All FTP traffic to network 192.169.1.9/29 will be denied

Answer: D

QUESTION 338
The following configuration line was added to router R1 Access-list 101 permit ip 10.25.30.0 0.0.0.255 any. What is the effect of this access list configuration?

A. ermit all packets matching the first three octets of the source address to all destinations
B. permit all packet matching the last octet of the destination address and accept all source addresses
C. permit all packet matching the host bits in the source address to all destinations
D. permit all packet from the third subnet of the network address to all destinations

Answer: A

QUESTION 339
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

Answer: C

QUESTION 340
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

Answer: ACE

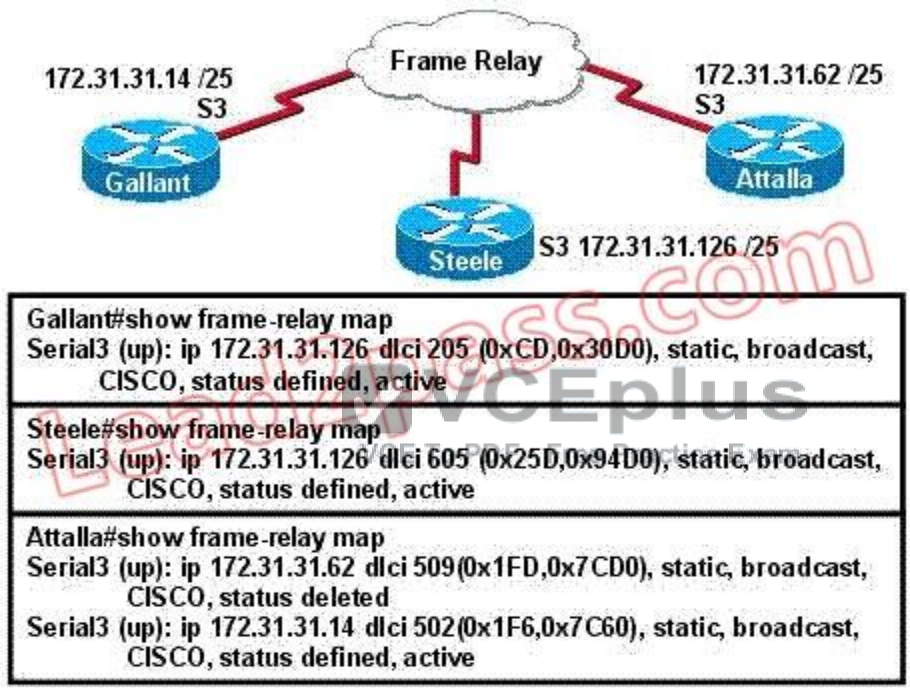
QUESTION 341
How should a router that is being used in a Frame Relay network be configured to avoid split

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

Answer: A

QUESTION 342
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

Answer: D

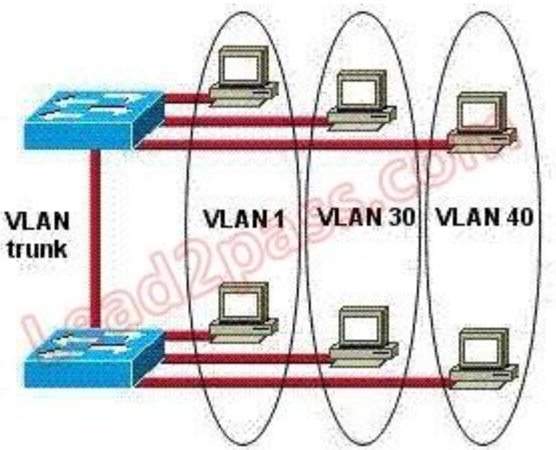
QUESTION 343
As a CCNA candidate, you must have a firm understanding of the IPv6 address structure. Refer to IPv6 address, could you tell me how many bits are included in each filed?

A. 24
B. 4

C. 3
D. 16

Answer: D

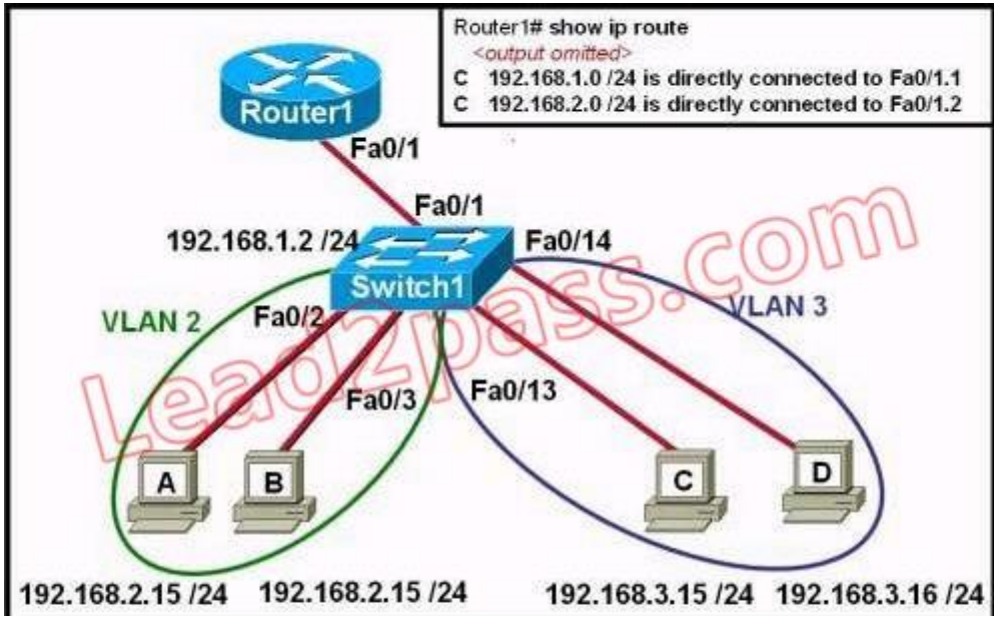
QUESTION 344
Refer to the exhibit. How many broadcast domains exist in the exhibited topology?



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

Answer: C

QUESTION 345
Refer to the exhibit. The network administrator has created a new VLAN on Switch1 and added host C and host D. The administrator has properly configured switch interfaces FastEthernet0/13 through FastEthernet0/14 to be members of the new VLAN. However, after the network administrator completed the configuration, host A could communicate with host B, but host A could not communicate with host C or host D. Which commands are required to resolve this problem?



```
Router1# show ip route
   <output omitted>
C   192.168.1.0 /24 is directly connected to Fa0/1.1
C   192.168.2.0 /24 is directly connected to Fa0/1.2
```

A.
```
Router(config)# interface fastethernet 0/1.3
Router(config-if)# encapsulation dot1q 3
Router(config-if)# ip address 192.168.3.1 255.255.255.0
```

B.
```
Router(config)# router rip
Router(config-router)# network 192.168.1.0
Router(config-router)# network 192.168.2.0
Router(config-router)# network192.168.3.0
```

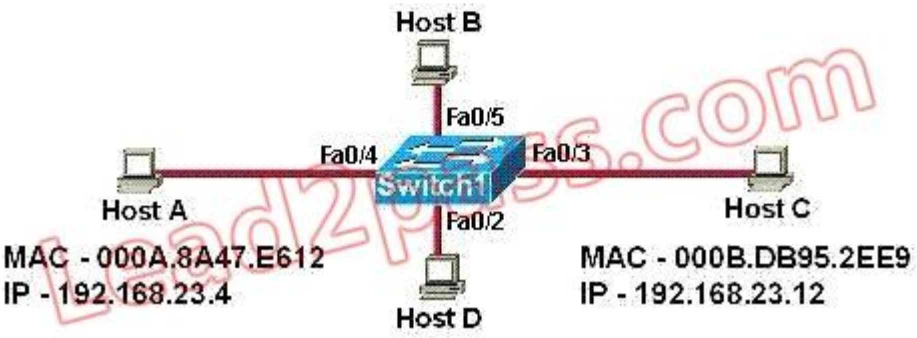
C.
```
Switch1# vlan database
Switch1(vlan)# vtp v2-mode
Switch1(vlan)# vtp domain cisco
Switch1(vlan)# vtp server
```

D.
```
Switch1(config)# interface fastethernet 0/1
Switch1(config-if)# switchport mode trunk
Switch1(config-if)# switchport trunk encapsulation isl
```

Answer: A

QUESTION 346

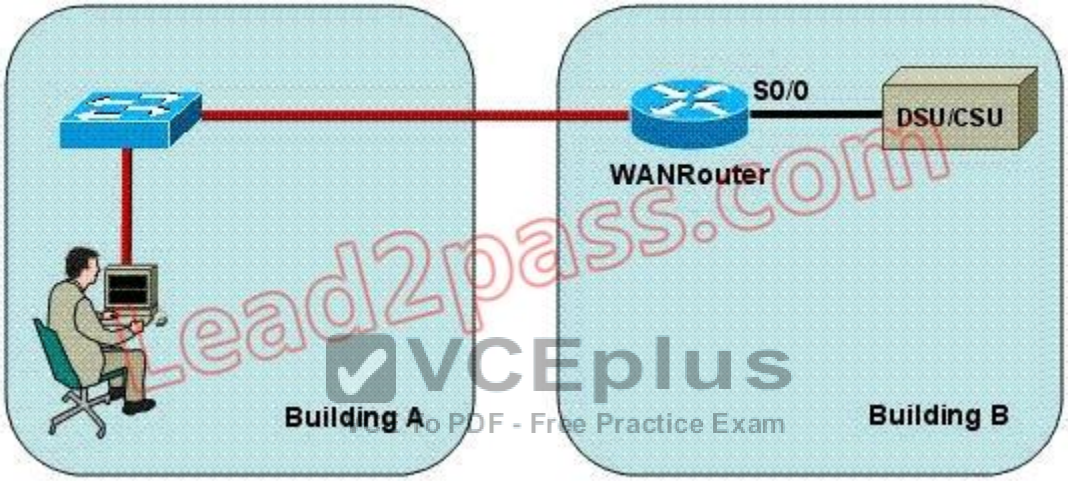
On a network of one department, there are four PCs connected to a switch, as shown in the following figure: After the Switch1 restarts. Host A (the host on the left) sends the first frame to Host C (the host on the right). What the first thing should the switch do?



A. Switch1 will add 192.168.23.12 to the switching table.
B. Switch1 will add 192.168.23.4 to the switching table.
C. Switch1 will add 000A.8A47.E612 to the switching table.
D. None of the above

Answer: C

QUESTION 347
Refer to the exhibit. The network administrator is in a campus building distant from Building B. WANRouter is hosting a newly installed WAN link on interface S0/0. The new link is not functioning and the administrator needs to determine if the correct cable has been attached to the S0/0 interface. How can the administrator accurately verify the correct cable type on S0/0 in the most efficient manner?



A. Telnet to WANRouter and execute the command show interfaces S0/0
B. Telnet to WANRouter and execute the command show processes S0/0
C. Telnet to WANRouter and execute the command show running-configuration
D. Telnet to WANRouter and execute the command show controller S0/0
E. Physically examine the cable between WANRouter S0/0 and the DCE.
F. Establish a console session on WANRouter and execute the command show interfaces S0/0

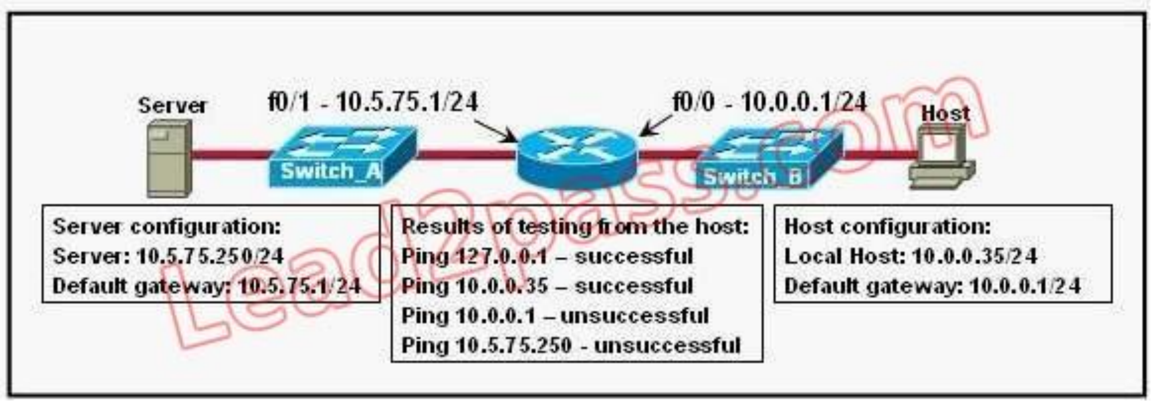
Answer: D

QUESTION 348
While troubleshooting a connectivity issue from a PC you obtain the following information:

```
Local PC IP address: 10.0.0.35/24
Default Gateway: 10.0.0.1
Remote Sever: 10.5.75.250/24
```

You then conduct the following tests from the local PC:

```
Ping 127.0.0.1 - Successful
Ping 10.0.0.35 - Successful
Ping 10.0.0.1 - Unsuccessful
Ping 10.5.75.250 - Unsuccessful
```



Server configuration:
Server: 10.5.75.250/24
Default gateway: 10.5.75.1/24

Results of testing from the host:
Ping 127.0.0.1 – successful
Ping 10.0.0.35 – successful
Ping 10.0.0.1 – unsuccessful
Ping 10.5.75.250 - unsuccessful

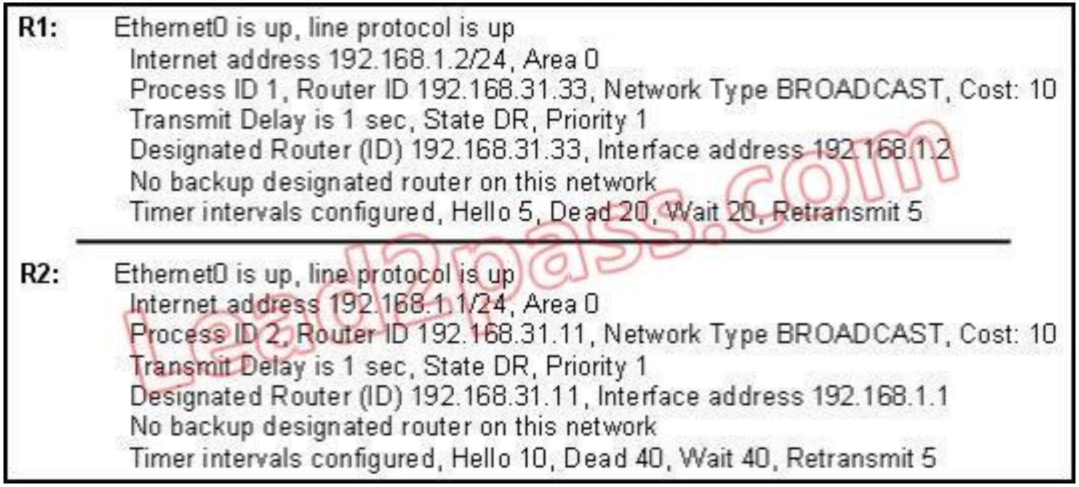
Host configuration:
Local Host: 10.0.0.35/24
Default gateway: 10.0.0.1/24

What is the underlying cause of this problem?

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

Answer: D

QUESTION 349
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.



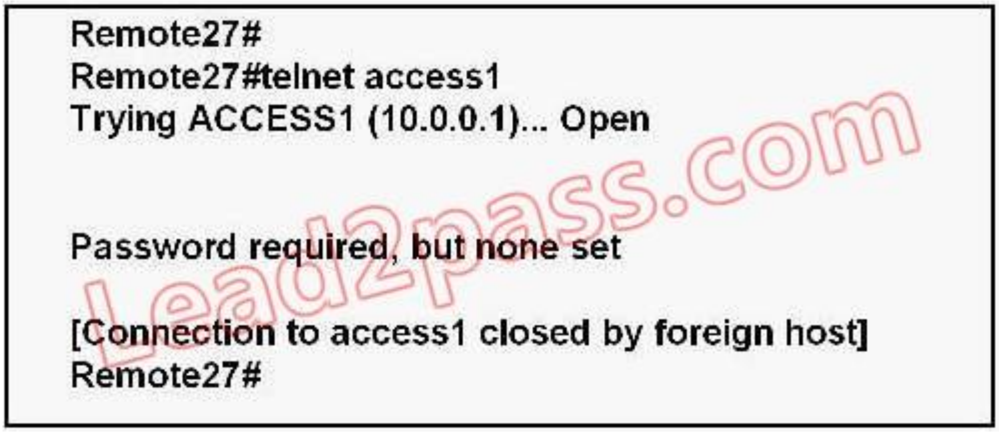
```
R1:   Ethernet0 is up, line protocol is up
        Internet address 192.168.1.2/24, Area 0
        Process ID 1, Router ID 192.168.31.33, Network Type BROADCAST, Cost: 10
        Transmit Delay is 1 sec, State DR, Priority 1
        Designated Router (ID) 192.168.31.33, Interface address 192.168.1.2
        No backup designated router on this network
        Timer intervals configured, Hello 5, Dead 20, Wait 20, Retransmit 5
      ----------------------------------------------------------------------
R2:   Ethernet0 is up, line protocol is up
        Internet address 192.168.1.1/24, Area 0
        Process ID 2, Router ID 192.168.31.11, Network Type BROADCAST, Cost: 10
        Transmit Delay is 1 sec, State DR, Priority 1
        Designated Router (ID) 192.168.31.11, Interface address 192.168.1.1
        No backup designated router on this network
        Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
```

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

QUESTION 350
This graphic shows the results of an attempt to open a Telnet connection to router ACCESS1 from router Remote27.



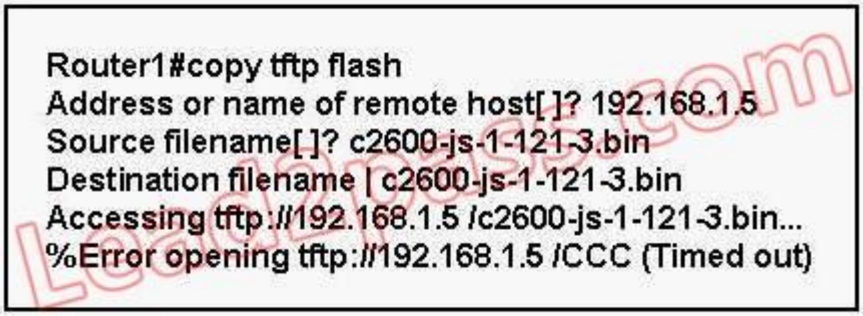
```
Remote27#
Remote27#telnet access1
Trying ACCESS1 (10.0.0.1)... Open


Password required, but none set

[Connection to access1 closed by foreign host]
Remote27#
```

Which of the following command sequences will correct this problem?

A.
```
ACCESS1(config)# line console 0
ACCESS1(config-line)# password cisco
```
B.
```
Remote27(config)# line console 0
Remote27(config-line)# login
Remote27(config-line)# password cisco
```
C.
```
ACCESS1(config)# line vty 0 4
ACCESS1(config-line)# login
ACCESS1(config-line)# password cisco
```
D.
```
Remote27(config)# line vty 0 4
Remote27(config-line)# login
Remote27(config-line)# password cisco
```
E.
```
ACCESS1(config)# enable password cisco
```
F.
```
Remote27(config)# enable password cisco
```

Answer: C

QUESTION 351
When upgrading the IOS image, the network administrator receives the exhibited error message.



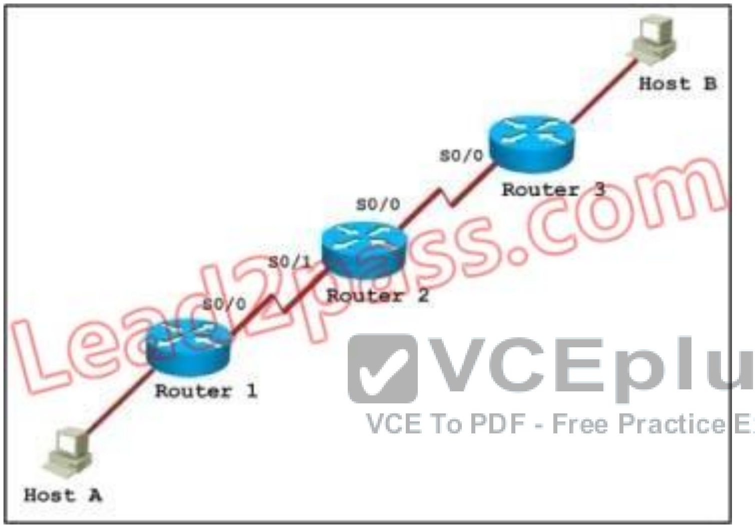
```
Router1#copy tftp flash
Address or name of remote host[ ]? 192.168.1.5
Source filename[ ]? c2600-js-1-121-3.bin
Destination filename [c2600-js-1-121-3.bin
Accessing tftp://192.168.1.5 /c2600-js-1-121-3.bin...
%Error opening tftp://192.168.1.5 /CCC (Timed out)
```

What could be the cause of this error?

A. The new IOS image is too large for the router flash memory.
B. The TFTP server is unreachable from the router.
C. The new IOS image is not correct for this router platform.
D. The IOS image on the TFTP server is corrupt.
E. There is not enough disk space on the TFTP server for the IOS image.

Answer: B

QUESTION 352
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

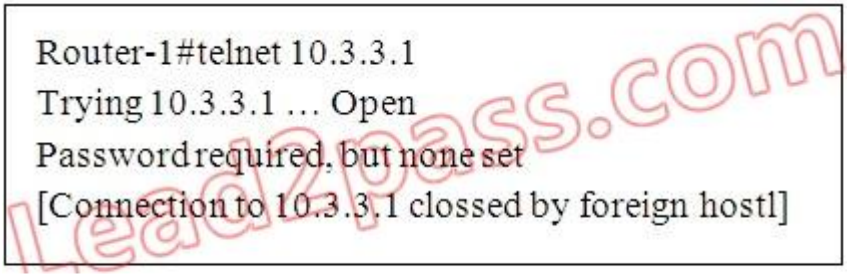
QUESTION 353
Which statement is true, as relates to classful or classless routing?

A. Automatic summarization at classful boundries can cause problems on discontinuous subnets
B. EIGRP and OSPF are classful routing protocols and summarize routes by default
C. RIPv1 and OSPF are classless routing protocols
D. Classful routing protocols send the subnet mask in routing updates

Answer: A

QUESTION 354

Refer to the exhibit. Why does the telnet connecting fail when a host attempts to connect a remote router?



```
Router-1#telnet 10.3.3.1
Trying 10.3.3.1 ... Open
Password required, but none set
[Connection to 10.3.3.1 clossed by foreign hostl]
```

A. No password was set for tty lines
B. No password was set for aux lines
C. No password was set for vty lines
D. No password was set for cty lines

Answer: C

QUESTION 355

Which name describes an IPV6 host-enable tunneling technique that uses IPV4 UDP,does not require dedicated gateway tunnels,and can pass through existing IPV4 NAT gateways?

A. dual stack
B. dynamic
C. Teredo
D. Manual 6to4

Answer: C

QUESTION 356

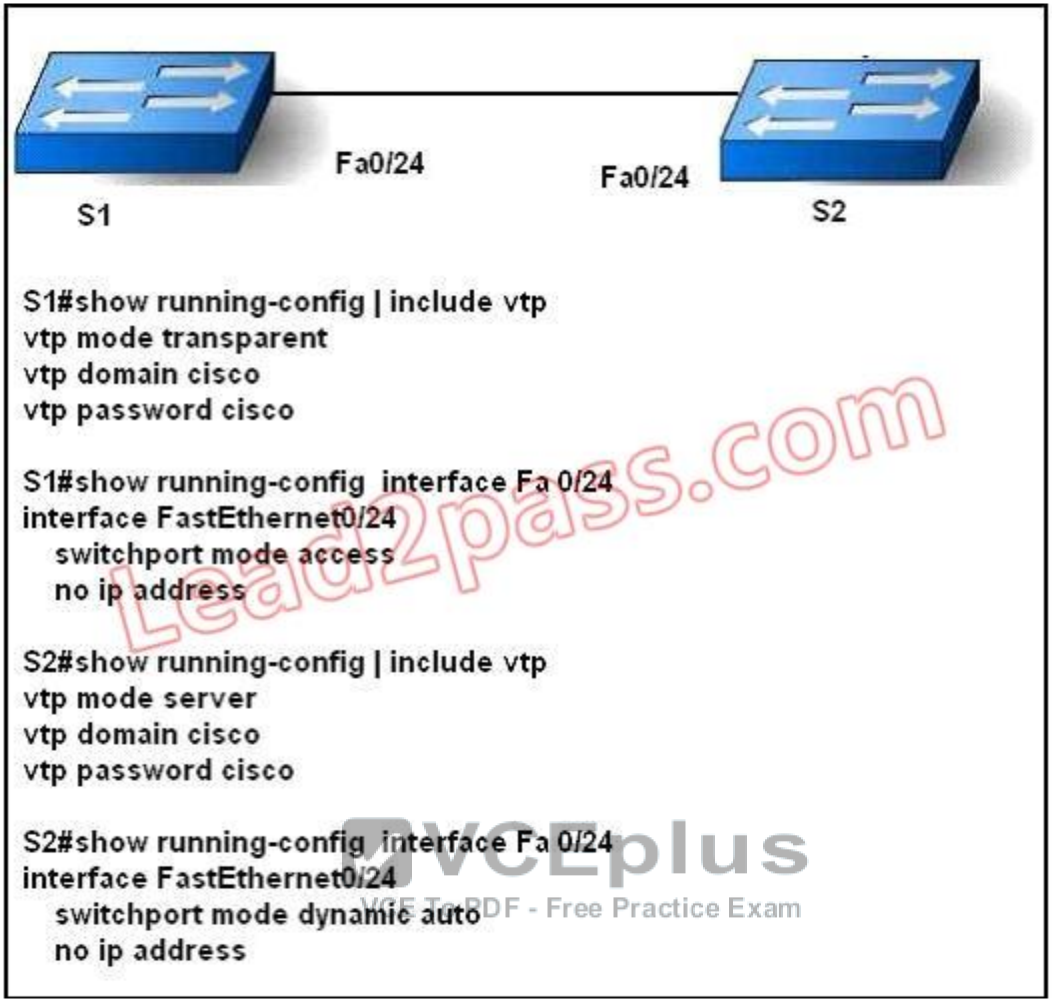
Which pairing reflects a correct protocol-and-metric relationship?

A. OSPF and mumber of hops and reliability
B. EIGRP and link cost
C. IS-IS and delay and reliability
D. RIPv2 and number of hops

Answer: D

QUESTION 357

Refer to the exhibit, The VLAN configuration of S1 is not being in this VTP enabled environment. The VTP and uplink port configurations for each switch are displayed. Which two command sets, if issued, resolve this failure and allow VTP to operate as expected?(choose two)



```
S1#show running-config | include vtp
vtp mode transparent
vtp domain cisco
vtp password cisco

S1#show running-config  interface Fa 0/24
interface FastEthernet0/24
   switchport mode access
   no ip address

S2#show running-config | include vtp
vtp mode server
vtp domain cisco
vtp password cisco

S2#show running-config  interface Fa 0/24
interface FastEthernet0/24
   switchport mode dynamic auto
   no ip address
```

A. `S2(config)#vtp mode transparent`

B. `S1(config)#vtp mode client`

C.
```
S2(config)#interface f0/24
S2(config-if)#switchport mode access
S2(config-if)#end
```

D. `S2(config)#vtp mode client`

E.
```
S1(config)#interface f0/24
S1(config-if)#switchport mode trunk
S1(config-if)#end
```

Answer: BE

QUESTION 358

How are VTP advertisements delivered to switches across the network?

A. anycast frames

B. multicast frames

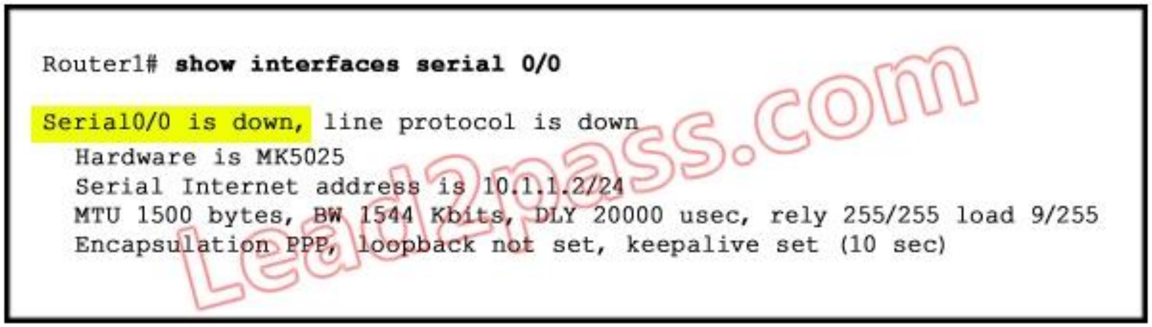
C. broadcast frames

D. unicast frames

Answer: B

QUESTION 359

Refer to the exhibit. What could be possible causes for the "Serial0/0 is down" interface status? (Choose two.)



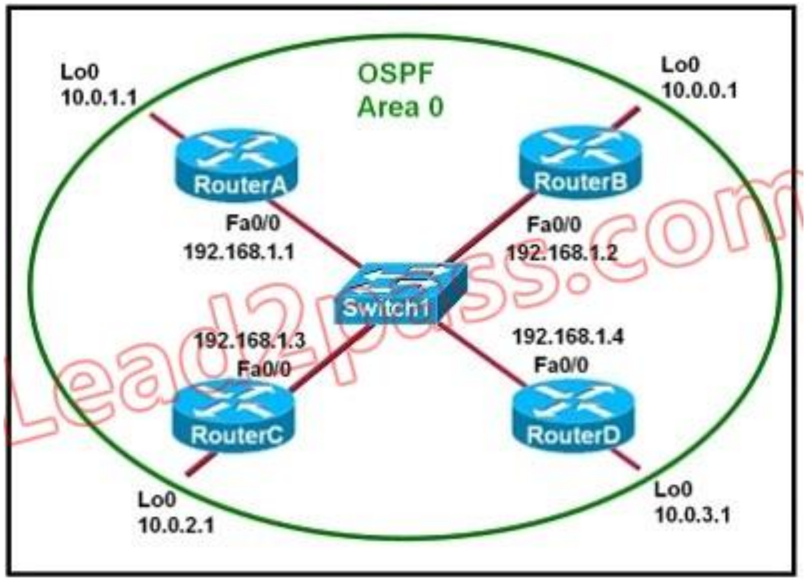
```
Router1# show interfaces serial 0/0

Serial0/0 is down, line protocol is down
   Hardware is MK5025
   Serial Internet address is 10.1.1.2/24
   MTU 1500 bytes, BW 1544 Kbits, DLY 20000 usec, rely 255/255 load 9/255
   Encapsulation PPP, loopback not set, keepalive set (10 sec)
```

A. A Layer 1 problem exists.
B. The bandwidth is set too low.
C. A protocol mismatch exists.
D. An incorrect cable is being used.
E. There is an incorrect IP address on the Serial 0/0 interface.

Answer: AD

QUESTION 360

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



A. It ensures that data will be forwarded by RouterB.
B. It provides stability for the OSPF process on RouterB.
C. It specifies that the router ID for RouterB should be 10.0.0.1.

D. It decreases the metric for routes that are advertised from RouterB.
E. It indicates that RouterB should be elected the DR for the LAN.

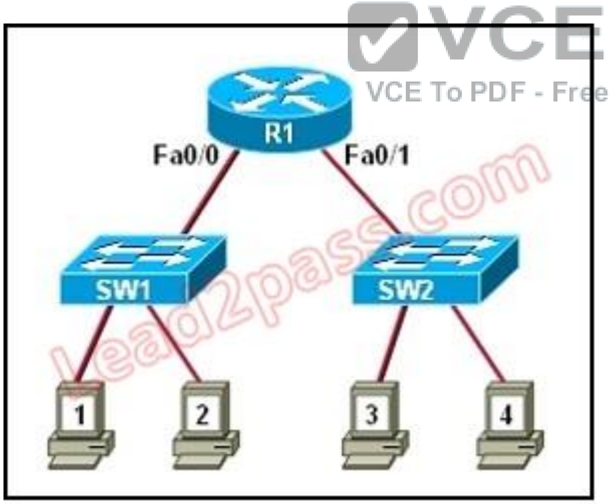
Answer: BC

QUESTION 361
A network administrator is explaining VTP configuration to a new technician. What should the network administrator tell the new technician about VTP configuration? (Choose three.)

A. A switch in the VTP client mode cannot update its local VLAN database.
B. A trunk link must be configured between the switches to forward VTP updates.
C. A switch in the VTP server mode can update a switch in the VTP transparent mode.
D. A switch in the VTP transparent mode will forward updates that it receives to other switches.
E. A switch in the VTP server mode only updates switches in the VTP client mode that have a higher VTP revision number.
F. A switch in the VTP server mode will update switches in the VTP client mode regardless of the configured VTP domain membership.

Answer: ABD

QUESTION 362
Refer to the exhibit. Both switches are using a default configuration. Which two destination addresses will host 4 use to send data to host 1? (Choose two.)



A. the IP address of host 1
B. the IP address of host 4
C. the MAC address of host 1
D. the MAC address of host 4
E. the MAC address of the Fa0/0 interface of the R1 router
F. the MAC address of the Fa0/1 interface of the R1 router

Answer: AF

QUESTION 363

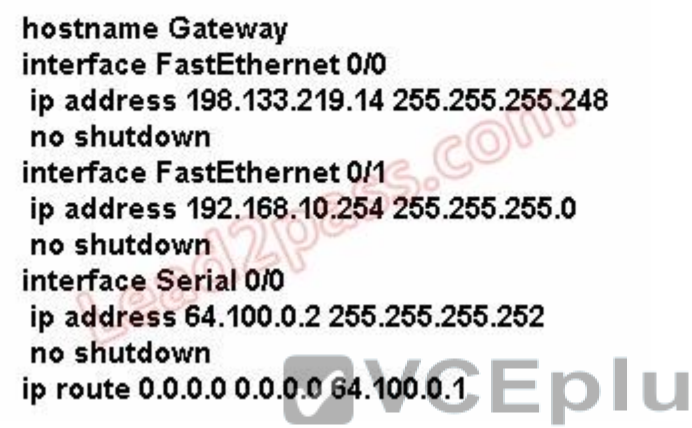
What are two reasons a network administrator would use CDP? (Choose two.)

A. to verify the type of cable interconnecting two devices
B. to determine the status of network services on a remote device
C. to obtain VLAN information from directly connected switches
D. to verify Layer 2 connectivity between two devices when Layer 3 fails
E. to obtain the IP address of a connected device in order to telnet to the device
F. to determine the status of the routing protocols between directly connected routers

Answer: DE

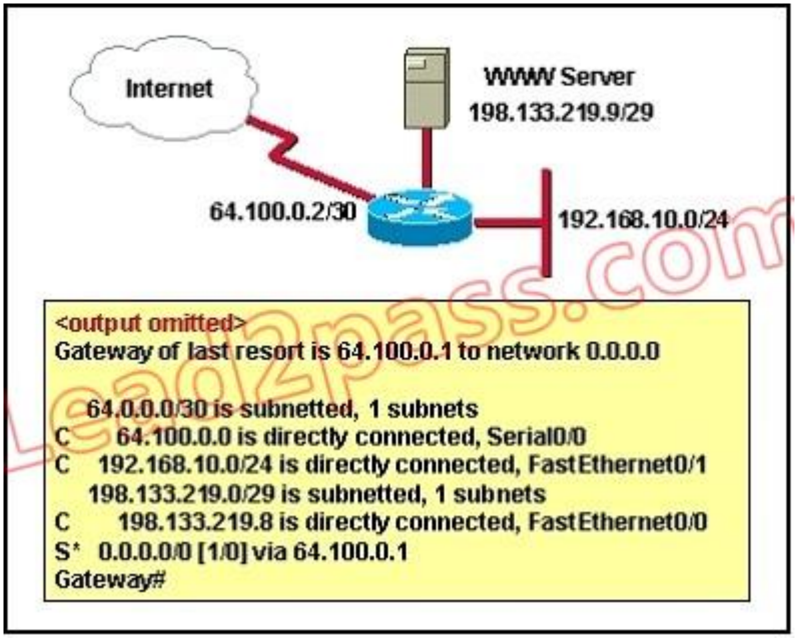
QUESTION 364

Refer to the exhibit. The router has been configured with these commands:



```
hostname Gateway
interface FastEthernet 0/0
 ip address 198.133.219.14 255.255.255.248
 no shutdown
interface FastEthernet 0/1
 ip address 192.168.10.254 255.255.255.0
 no shutdown
interface Serial 0/0
 ip address 64.100.0.2 255.255.255.252
 no shutdown
ip route 0.0.0.0 0.0.0.0 64.100.0.1
```

What are the two results of this configuration? (Choose two.)



```
<output omitted>
Gateway of last resort is 64.100.0.1 to network 0.0.0.0

     64.0.0.0/30 is subnetted, 1 subnets
C       64.100.0.0 is directly connected, Serial0/0
C    192.168.10.0/24 is directly connected, FastEthernet0/1
     198.133.219.0/29 is subnetted, 1 subnets
C       198.133.219.8 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 64.100.0.1
Gateway#
```

A. The default route should have a next hop address of 64.100.0.3.
B. Hosts on the LAN that is connected to FastEthernet 0/1 are using public IP addressing.

C. The address of the subnet segment with the WWW server will support seven more servers.
D. The addressing scheme allows users on the Internet to access the WWW server.
E. Hosts on the LAN that is connected to FastEthernet 0/1 will not be able to access the Internet without address translation.

Answer: DE

QUESTION 365
A company is installing IP phones. The phones and office computers connect to the same device. To ensure maximum throughput for the phone data, the company needs to make sure that the phone traffic is on a different network from that of the office computer data traffic. What is the best network device to which to directly connect the phones and computers, and what technology should be implemented on this device? (Choose two.)

A. hub
B. router
C. switch
D. STP
E. subinterfaces
F. VLAN

Answer: CF

QUESTION 366
What are two benefits of using VTP in a switching environment? (Choose two.)

A. It allows switches to read frame tags.
B. It allows ports to be assigned to VLANs automatically.
C. It maintains VLAN consistency across a switched network.
D. It allows frames from multiple VLANs to use a single interface.
E. It allows VLAN information to be automatically propagated throughout the switching environment.

Answer: CE

QUESTION 367
Which two statements are true about the command ip route 172.16.3.0 255.255.255.0 192.168.2.4? (Choose two.)

A. It establishes a static route to the 172.16.3.0 network.
B. It establishes a static route to the 192.168.2.0 network.
C. It configures the router to send any traffic for an unknown destination to the 172.16.3.0 network.
D. It configures the router to send any traffic for an unknown destination out the interface with the address 192.168.2.4.
E. It uses the default administrative distance.
F. It is a route that would be used last if other routes to the same destination exist.

Answer: AE

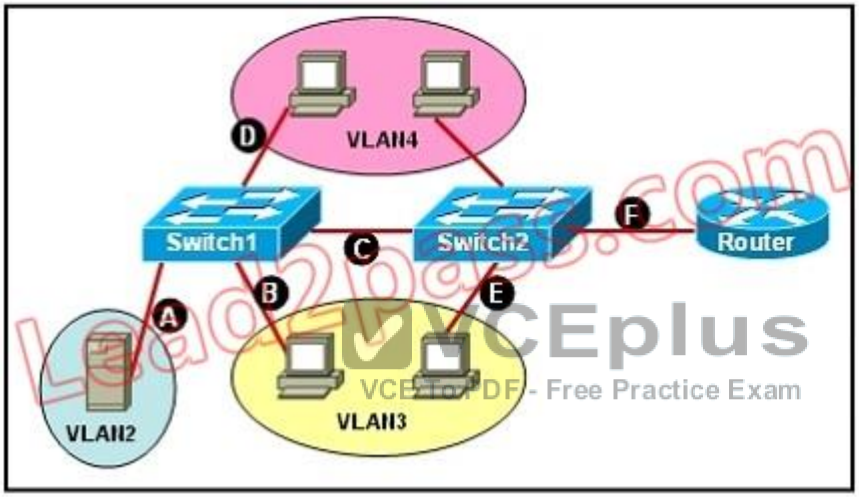
QUESTION 368

What are two advantages of Layer 2 Ethernet switches over hubs? (Choose two.)

A. decreasing the number of collision domains
B. filtering frames based on MAC addresses
C. allowing simultaneous frame transmissions
D. increasing the size of broadcast domains
E. increasing the maximum length of UTP cabling between devices

Answer: BC

QUESTION 369
Refer to the exhibit. A network associate needs to configure the switches and router in the graphic so that the hosts in VLAN3 and VLAN4 can communicate with the enterprise server in VLAN2. Which two Ethernet segments would need to be configured as trunk links? (Choose two.)



A. A
B. B
C. C
D. D
E. E
F. F

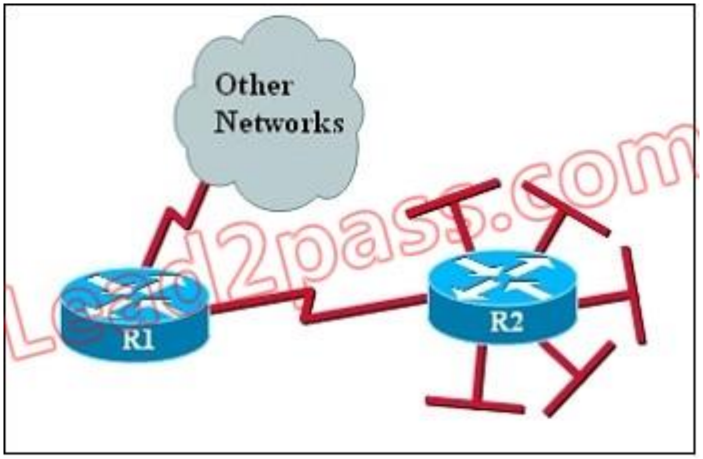
Answer: CF

QUESTION 370
Which two values are used by Spanning Tree Protocol to elect a root bridge? (Choose two.)

A. amount of RAM
B. bridge priority
C. IOS version
D. IP address
E. MAC address
F. speed of the links

Answer: BE

QUESTION 371
Refer to the exhibit. The networks connected to router R2 have been summarized as a 192.168.176.0/21 route and sent to R1. Which two packet destination addresses will R1 forward to R2? (Choose two.)



A. 192.168.194.160
B. 192.168.183.41
C. 192.168.159.2
D. 192.168.183.255
E. 192.168.179.4
F. 192.168.184.45

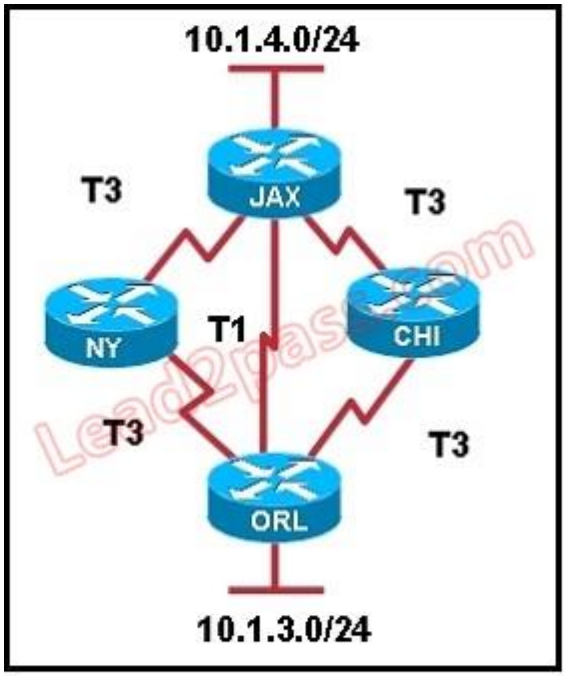
Answer: BE

QUESTION 372
Which three statements are typical characteristics of VLAN arrangements? (Choose three.)

A. A new switch has no VLANs configured.
B. Connectivity between VLANs requires a Layer 3 device.
C. VLANs typically decrease the number of collision domains.
D. Each VLAN uses a separate address space.
E. A switch maintains a separate bridging table for each VLAN.
F. VLANs cannot span multiple switches.

Answer: BDE

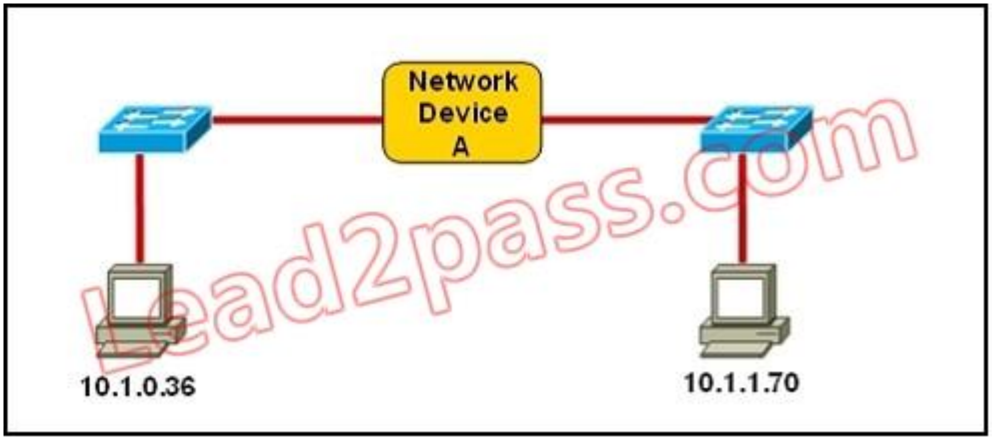
QUESTION 373
Refer to the exhibit. Which three statements are true about how router JAX will choose a path to the 10.1.3.0/24 network when different routing protocols are configured? (Choose three.)



A. By default, if RIPv2 is the routing protocol, only the path JAX-ORL will be installed into the routing table.
B. The equal cost paths JAX-CHI-ORL and JAX- NY-ORL will be installed in the routing table if RIPv2 is the routing protocol.
C. When EIGRP is the routing protocol, only the path JAX-ORL will be installed in the routing table by default.
D. When EIGRP is the routing protocol, the equal cost paths JAX-CHI-ORL, and JAX-NY-ORL will be installed in the routing table by default.
E. With EIGRP and OSPF both running on the network with their default configurations, the EIGRP paths will be installed in the routing table.
F. The OSPF paths will be installed in the routing table, if EIGRP and OSPF are both running on the network with their default configurations.

Answer: ADE

QUESTION 374
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.

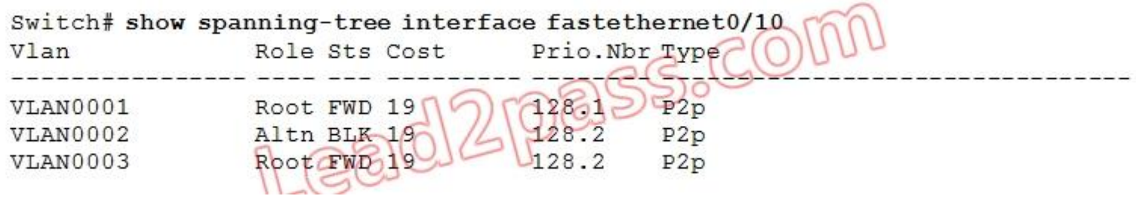
Answer: BDE

QUESTION 375
Switch ports operating in which two roles will forward traffic according to the IEEE 802.1w standard? (Choose two.)

A. alternate
B. backup
C. designated
D. disabled
E. root

Answer: CE

QUESTION 376
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
```

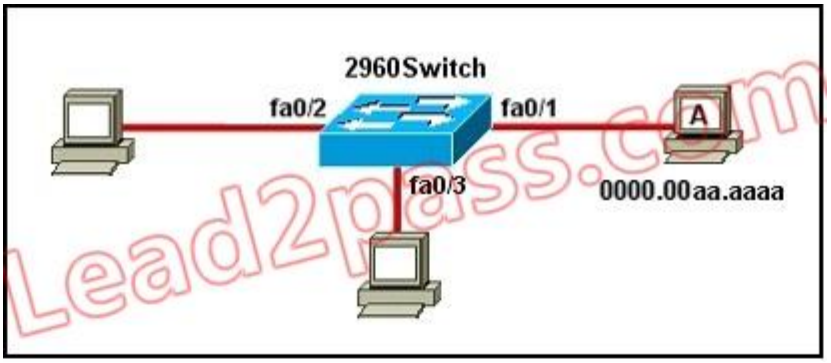
A. This switch has more than one interface connected to the root network segment in VLAN 2.
B. This switch is running RSTP while the elected designated switch is running 802.1d Spanning Tree.
C. This switch interface has a higher path cost to the root bridge than another in the topology.
D. This switch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

Answer: C

QUESTION 377
Refer to the exhibit. This command is executed on 2960Switch:

```
2960Switch(config)# mac-address-table static 0000.00aa.aaaa vlan 10
interface fa0/1
```

Which two of these statements correctly identify results of executing the command? (Choose two.)



A. Port security is implemented on the fa0/1 interface.
B. MAC address 0000.00aa.aaaa does not need to be learned by this switch.
C. Only MAC address 0000.00aa.aaaa can source frames on the fa0/1 segment.
D. Frames with a Layer 2 source address of 0000.00aa.aaaa will be forwarded out fa0/1.
E. MAC address 0000.00aa.aaaa will be listed in the MAC address table for interface fa0/1 only.

Answer: BE

QUESTION 378
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: ADE

QUESTION 379
What are two characteristics of Telnet? (Choose two.)

A. It sends data in clear text format.
B. It is no longer supported on Cisco network devices.
C. It is more secure than SSH.
D. It requires an enterprise license in order to be implemented.
E. It requires that the destination device be configured to support Telnet connections.

Answer: AE

QUESTION 380
What are two security appliances that can be installed in a network? (Choose two.)

A. ATM
B. IDS

C. IOS
D. IOX
E. IPS
F. SDM

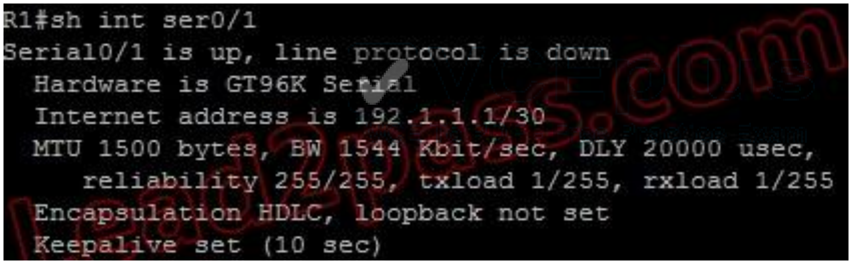
Answer: BE

QUESTION 381
Assuming a subnet mask of 255.255.248.0, three of the following addresses are valid host addresses. Which are these addresses? (Choose three.)

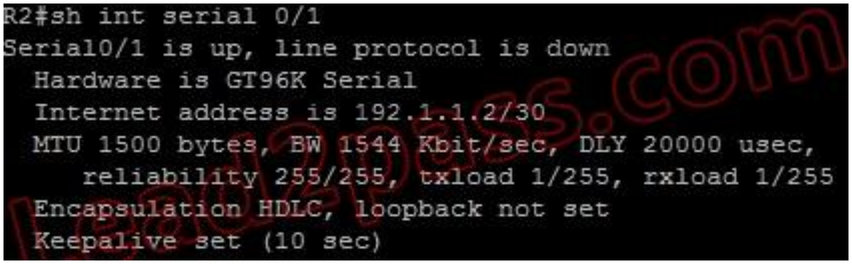
A. 172.16.9.0
B. 172.16.8.0
C. 172.16.31.0
D. 172.16.20.0

Answer: ACD

QUESTION 382
Refer to the exhibit. A network technician is unable to ping from R1 to R2.
What will help correct the problem?



```
R1#sh int ser0/1
Serial0/1 is up, line protocol is down
  Hardware is GT96K Serial
  Internet address is 192.1.1.1/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
```

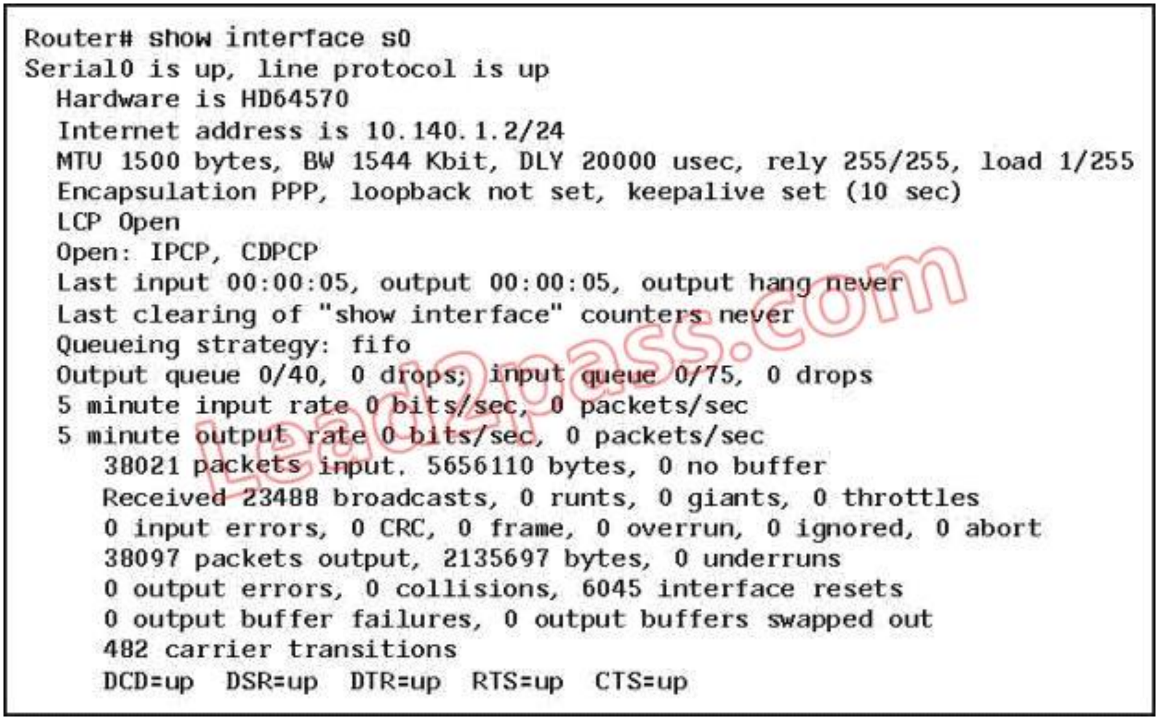


```
R2#sh int serial 0/1
Serial0/1 is up, line protocol is down
  Hardware is GT96K Serial
  Internet address is 192.1.1.2/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
```

A. Ensure that the serial cable is correctly plugged in to the interfaces.
B. Apply the clock rate 56000 configuration command to the serial0/1 interface of R1.
C. Configure the serial0/1 interfaces on R1 and R2 with the no shutdown command.
D. Change the address of the serial0/1 interface of R1 to 192.1.1.4.
E. Change the subnet masks of both interfaces to 255.255.255.240.

Answer: A

QUESTION 383
Refer to the exhibit. Which two statements are true of the interface configuration? (Choose two.)

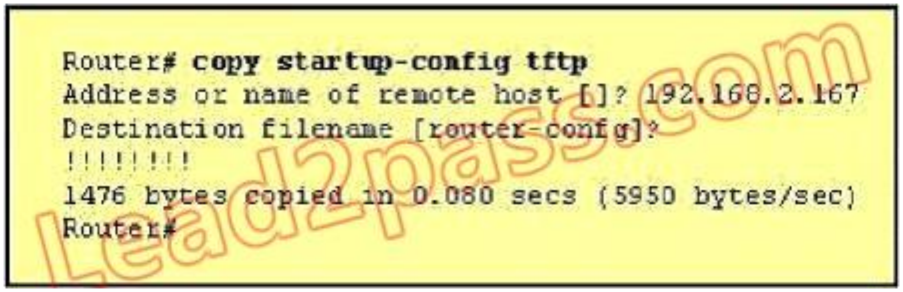


```
Router# show interface s0
Serial0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 10.140.1.2/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive set (10 sec)
  LCP Open
  Open: IPCP, CDPCP
  Last input 00:00:05, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     38021 packets input, 5656110 bytes, 0 no buffer
     Received 23488 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     38097 packets output, 2135697 bytes, 0 underruns
     0 output errors, 0 collisions, 6045 interface resets
     0 output buffer failures, 0 output buffers swapped out
     482 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

A. The encapsulation in use on this interface is PPP.
B. The default serial line encapsulation is in use on this interface.
C. The address mask of this interface is 255.255.255.0.
D. This interface is connected to a LAN.
E. The interface is not ready to forward packets.

Answer: AC

QUESTION 384
Refer to the exhibit. What does the address 192.168.2.167 represent?



```
Router# copy startup-config tftp
Address or name of remote host []? 192.168.2.167
Destination filename [router-confg]?
!!!!!!!!
1476 bytes copied in 0.080 secs (5950 bytes/sec)
Router#
```

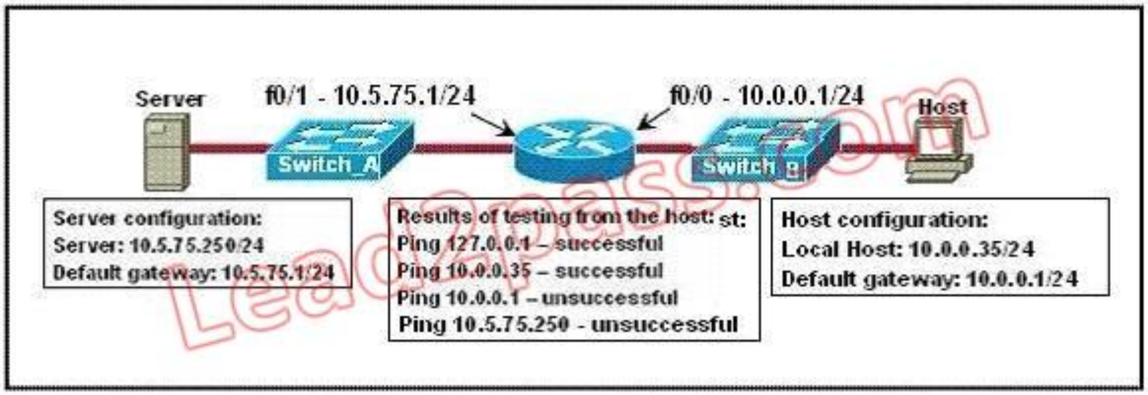
A. the TFTP server from which the file startup-config is being transferred
B. the router from which the file startup-config is being transferred
C. the TFTP server from which the file router-confg is being transferred
D. the TFTP server to which the file router-confg is being transferred
E. the router to which the file router-confg is being transferred
F. the router to which the file startup-config is being transferred

Answer: D

QUESTION 385

Refer to the exhibit. A technician is troubleshooting a host connectivity problem. The host is unable to ping a server connected to Switch_A.

Based on the results of the testing, what could be the problem?


Server
f0/1 - 10.5.75.1/24
f0/0 - 10.0.0.1/24
Host
Switch_A
Switch_B
Server configuration:
Server: 10.5.75.250/24
Default gateway: 10.5.75.1/24
Results of testing from the host: st:
Ping 127.0.0.1 – successful
Ping 10.0.0.35 – successful
Ping 10.0.0.1 – unsuccessful
Ping 10.5.75.250 - unsuccessful
Host configuration:
Local Host: 10.0.0.35/24
Default gateway: 10.0.0.1/24
Lead2pass.com

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

Answer: D

QUESTION 386

In which situation would the use of a static route be appropriate?

A. To configure a route to the first Layer 3 device on the network segment.
B. To configure a route from an ISP router into a corporate network.
C. To configure a route when the administrative distance of the current routing protocol is too low.
D. To reach a network is more than 15 hops away.
E. To provide access to the Internet for enterprise hosts.

Answer: B

QUESTION 387

An administrator issues the show ip interface s0/0 command and the output displays that interface Serial0/0 is up, line protocol is up What does "line protocol is up" specifically indicate about the interface?

A. The cable is attached properly.
B. CDP has discovered the connected device.
C. Keepalives are being received on the interface.
D. A carrier detect signal has been received from the connected device.
E. IP is correctly configured on the interface.

Answer: C

QUESTION 388
Which three statements are correct about RIP version 2? (Choose three)

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

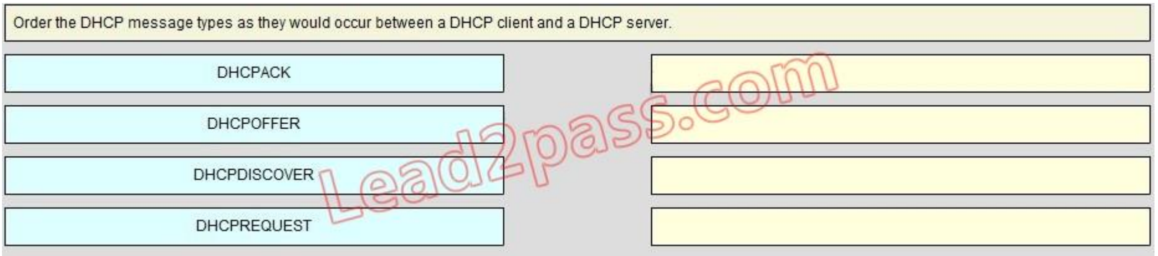
Answer: BCE

QUESTION 389
How can an administrator determine if a router has been configured when it is first powered up?

A. A configured router prompts for a password.
B. A configured router goes to the privileged mode prompt.
C. An unconfigured router goes into the setup dialog.
D. An unconfigured router goes to the enable mode prompt.

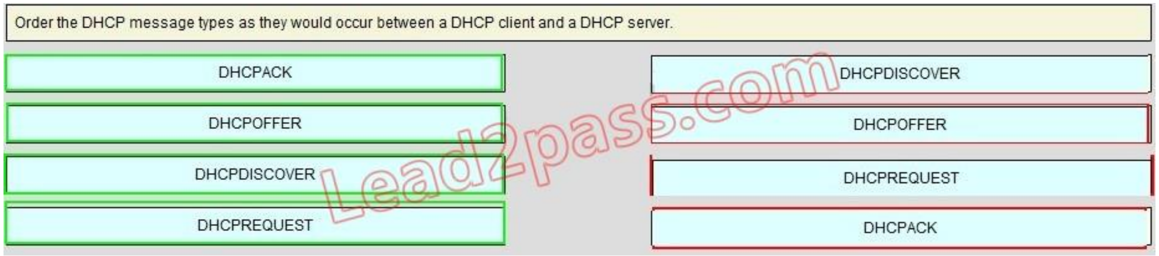
Answer: C

QUESTION 390
Drag and Drop Question


Order the DHCP message types as they would occur between a DHCP client and a DHCP server.

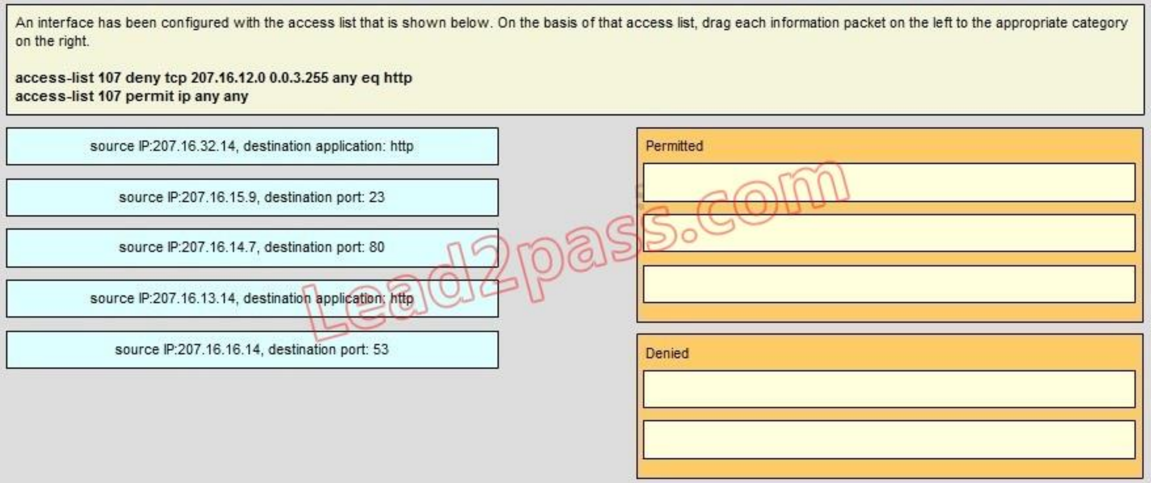
DHCPACK
DHCPOFFER
DHCPDISCOVER
DHCPREQUEST

Answer:


Order the DHCP message types as they would occur between a DHCP client and a DHCP server.

DHCPACK	DHCPDISCOVER
DHCPOFFER	DHCPOFFER
DHCPDISCOVER	DHCPREQUEST
DHCPREQUEST	DHCPACK

QUESTION 391
Drag and Drop Question

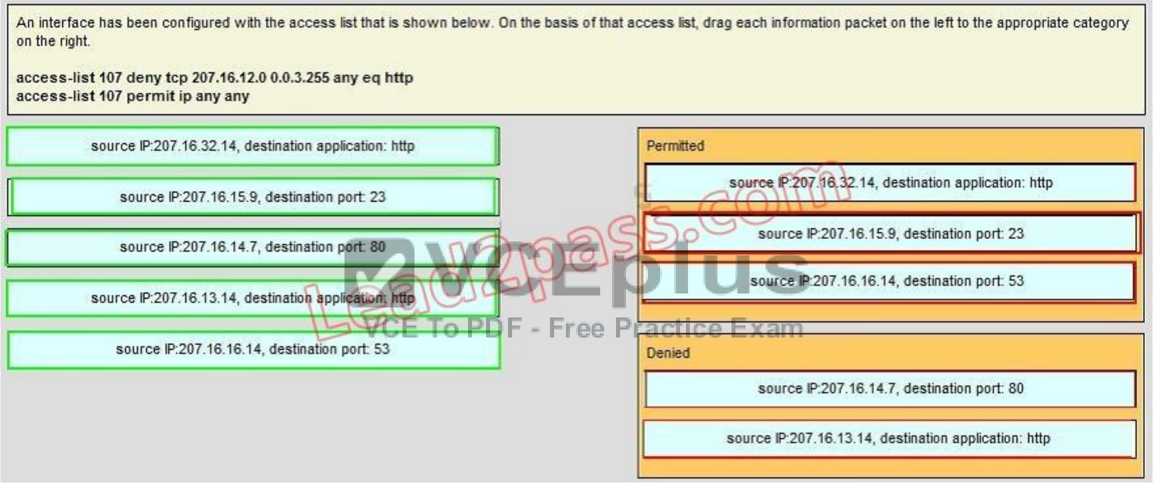


An interface has been configured with the access list that is shown below. On the basis of that access list, drag each information packet on the left to the appropriate category on the right.

```
access-list 107 deny tcp 207.16.12.0 0.0.3.255 any eq http
access-list 107 permit ip any any
```

- source IP:207.16.32.14, destination application: http
- source IP:207.16.15.9, destination port: 23
- source IP:207.16.14.7, destination port: 80
- source IP:207.16.13.14, destination application: http
- source IP:207.16.16.14, destination port: 53

Answer:



An interface has been configured with the access list that is shown below. On the basis of that access list, drag each information packet on the left to the appropriate category on the right.

```
access-list 107 deny tcp 207.16.12.0 0.0.3.255 any eq http
access-list 107 permit ip any any
```

- source IP:207.16.32.14, destination application: http
- source IP:207.16.15.9, destination port: 23
- source IP:207.16.14.7, destination port: 80
- source IP:207.16.13.14, destination application: http
- source IP:207.16.16.14, destination port: 53

Permitted
- source IP:207.16.32.14, destination application: http
- source IP:207.16.15.9, destination port: 23
- source IP:207.16.16.14, destination port: 53

Denied
- source IP:207.16.14.7, destination port: 80
- source IP:207.16.13.14, destination application: http

QUESTION 392
A network administrator receives an error message while trying to configure the Ethernet interface of a router with IP address 10.24.24.24/29. Which statement explains the reason for this issue?

A. This address is a broadcast address.
B. VLSM-capable routing protocols must be enabled first on the router.
C. The Ethernet interface is faulty.
D. This address is a network address.

Answer: D

QUESTION 393
Which address is the IPv6 all-RIP-routers multicast group address that is used by RIPng as the destination address for RIP updates?

A. FF02::9

B. FF02::6
C. FF05::101
D. FF02::A

Answer: A

QUESTION 394
If all OSPF routers in a single area are configured with the same priority value, what value does a router use for the OSPF router ID in the absence of a loopback interface?

A. the IP address of the first Fast Ethernet interface
B. the IP address of the console management interface
C. the highest IP address among its active interfaces
D. the lowest IP address among its active interfaces
E. the priority value until a loopback interface is configured

Answer: C

QUESTION 395
The OSPF Hello protocol performs which of the following tasks? (Choose two.)

A. It provides dynamic neighbor discovery.
B. It detects unreachable neighbors in 90 second intervals.
C. It maintains neighbor relationships.
D. It negotiates correctness parameters between neighboring interfaces.
E. It uses timers to elect the router with the fastest links as the designated router.
F. It broadcasts hello packets throughout the internetwork to discover all routers that are running OSPF.

Answer: AC

QUESTION 396
The network administrator of the Oregon router adds the following command to the router configuration: ip route 192.168.12.0 255.255.255.0 172.16.12.1. What are the results of adding this command? (Choose two.)

A. The command establishes a static route.
B. The command invokes a dynamic routing protocol for 192.168.12.0.
C. Traffic for network 192.168.12.0 is forwarded to 172.16.12.1.
D. Traffic for all networks is forwarded to 172.16.12.1.
E. This route is automatically propagated throughout the entire network.
F. Traffic for network 172.16.12.0 is forwarded to the 192.168.12.0 network.

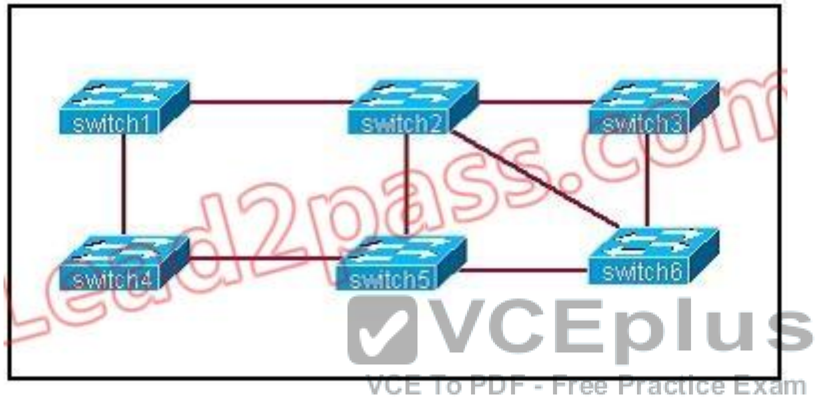
Answer: AC

QUESTION 397
A network administrator is planning a network installation for a large organization. The design requires 100 separate subnetworks, so the company has acquired a Class B network address. What subnet mask will provide the 100 subnetworks required, if 500 usable host addresses are required per subnet?

A. 255.255.240.0
B. 255.255.248.0
C. 255.255.252.0
D. 255.255.254.0
E. 255.255.255.0
F. 255.255.255.192

Answer: D

QUESTION 398
Refer to Exhibit. 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

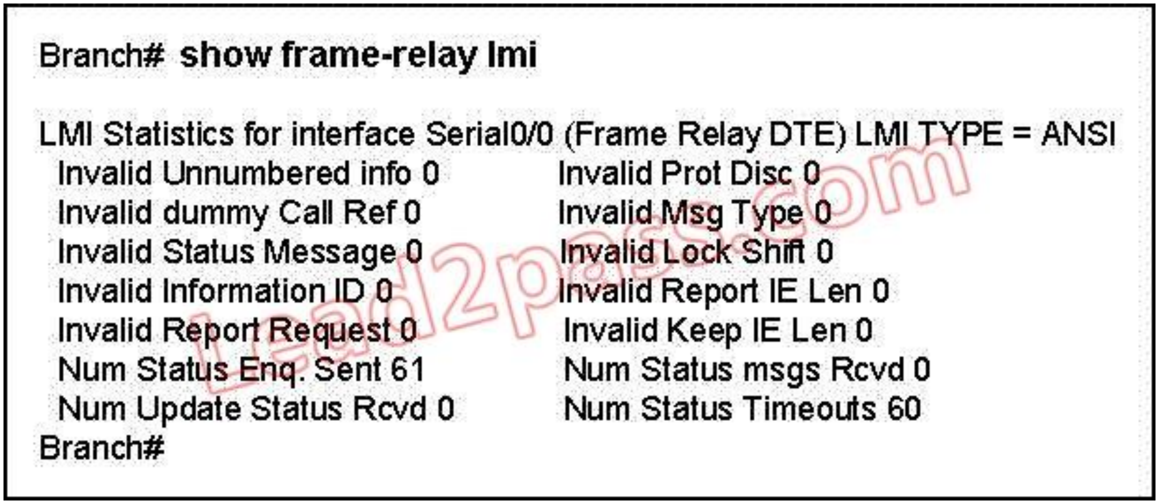
QUESTION 399
Which of the following services use UDP? (Choose three.)

A. Telnet
B. TFTP
C. SNMP
D. DNS
E. SMTP
F. HTTP

Answer: BCD

QUESTION 400

Refer to the exhibit. Which two statements are true based the output of the show frame-relay lmi command issued on the Branch router? (Choose two.)



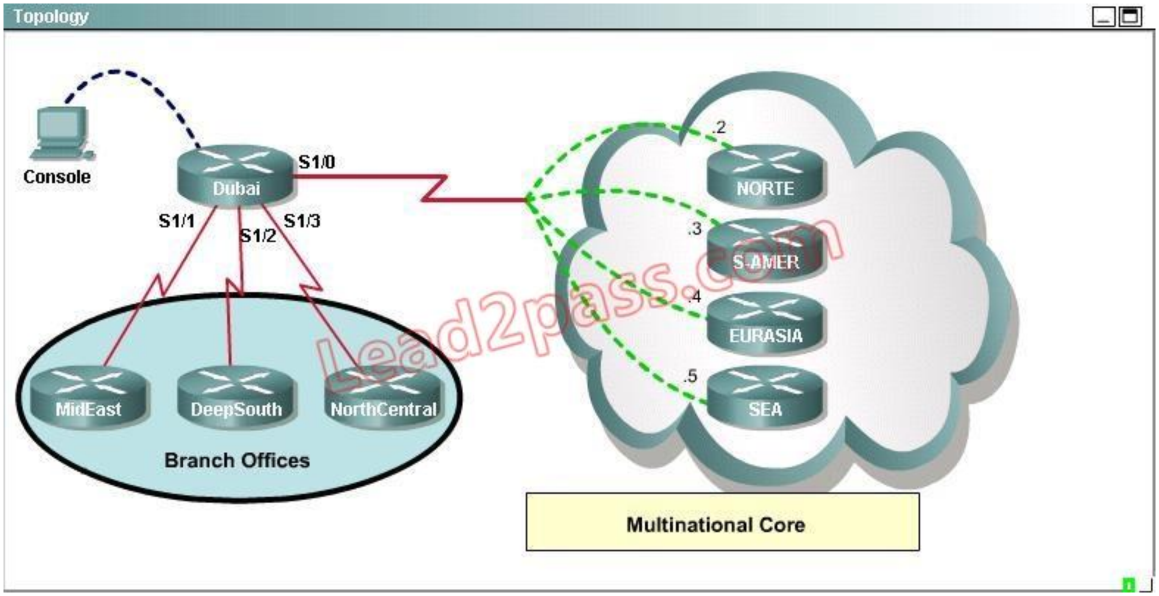
```
Branch# show frame-relay lmi

LMI Statistics for interface Serial0/0 (Frame Relay DTE) LMI TYPE = ANSI
  Invalid Unnumbered info 0          Invalid Prot Disc 0
  Invalid dummy Call Ref 0           Invalid Msg Type 0
  Invalid Status Message 0           Invalid Lock Shift 0
  Invalid Information ID 0           Invalid Report IE Len 0
  Invalid Report Request 0           Invalid Keep IE Len 0
  Num Status Enq. Sent 61            Num Status msgs Rcvd 0
  Num Update Status Rcvd 0           Num Status Timeouts 60
Branch#
```

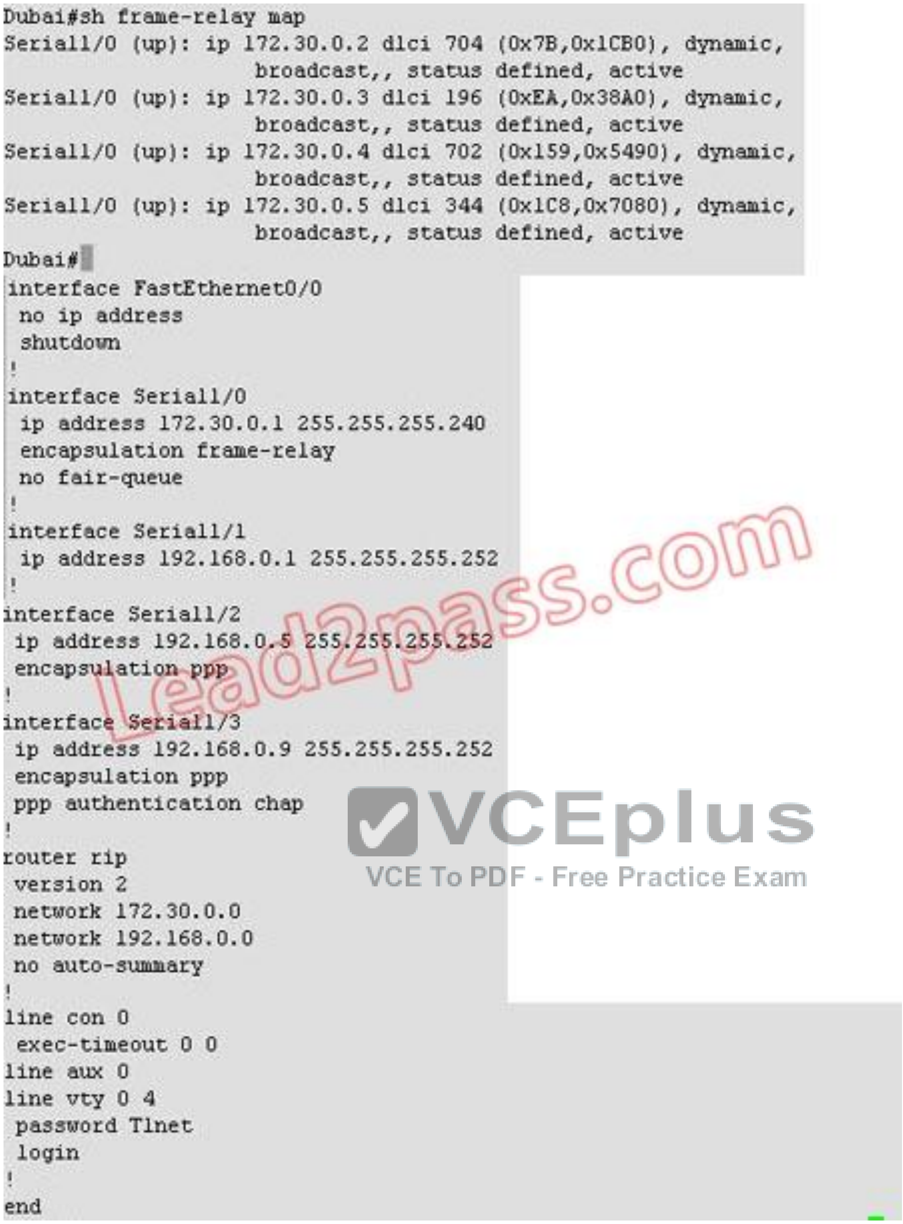
A. LMI messages are being sent on DLCI 1023.
B. The LMI exchange between the router and Frame Relay switch is functioning properly.
C. LMI messages are being sent on DLCI 0.
D. The Frame Relay switch is not responding to LMI requests from the router.
E. The router is providing a clock signal on Serial0/0 on the circuit to the Frame Relay switch.
F. Interface Serial0/0 is not configured to encapsulate Frame Relay.

Answer: CD

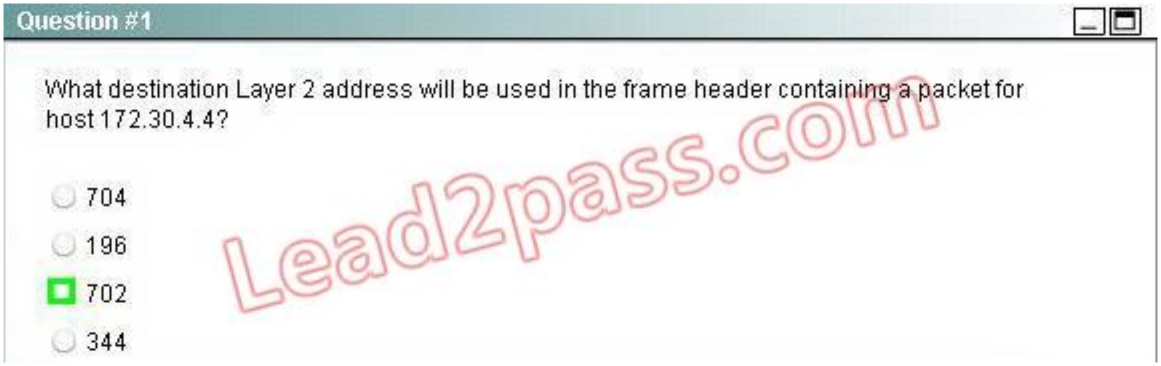
QUESTION 401

Hotspot Question





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



Question #1

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

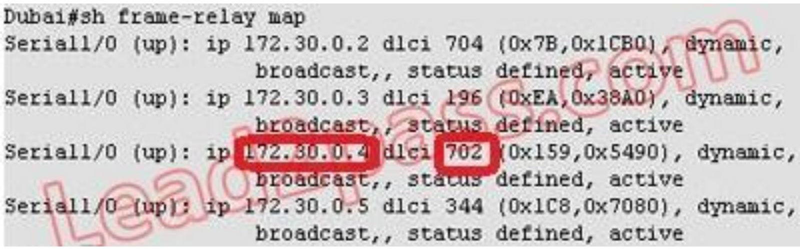
○ 704

○ 196

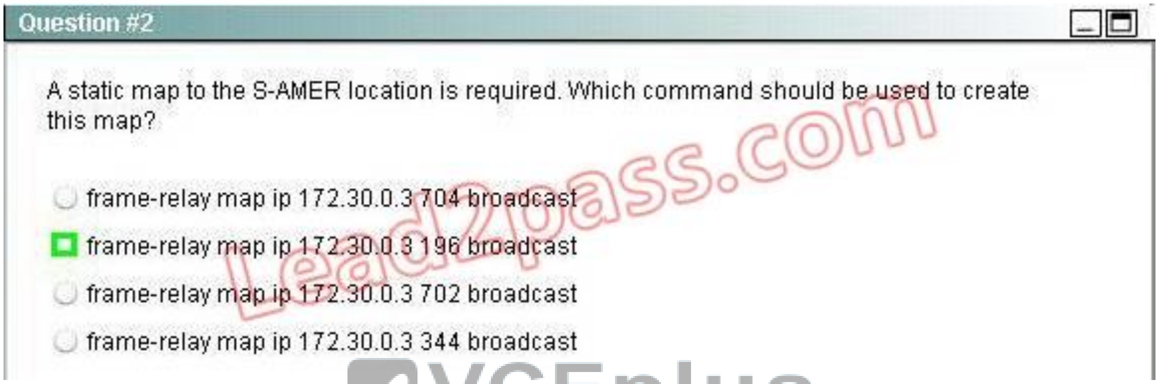
● 702

○ 344

Answer: 702
Explanation:
The output of the above show command displays that the local DLCI number corresponding to the sub-interface of s1/0 whose IP address is 172.30.0.4 is 702.



```
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
```

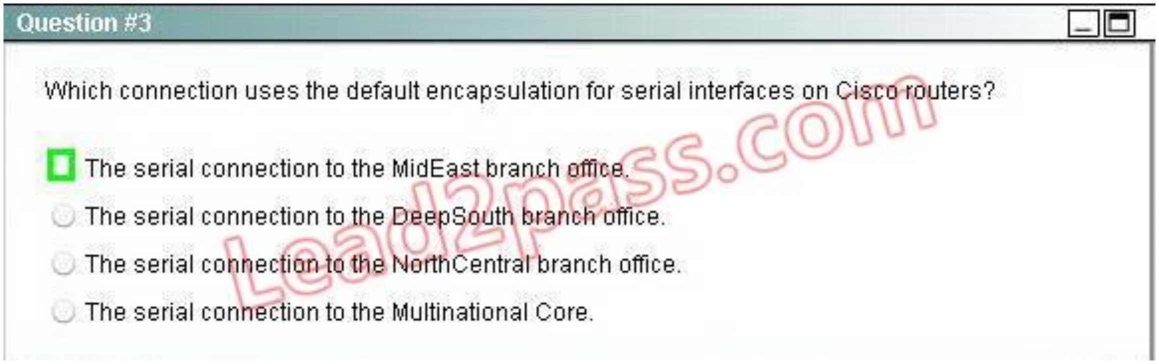


Question #2

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

Answer: frame-relay map ip 172.30.0.3 196 broadcast
Explanation:
Based on the output of the command **"show frame-relay map"**, we know that DLCI mapped to the router S-AMER is 196. (.3 In the above network topology, the complete Layer 3 IP address is 172.30.0.3)



Question #3

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

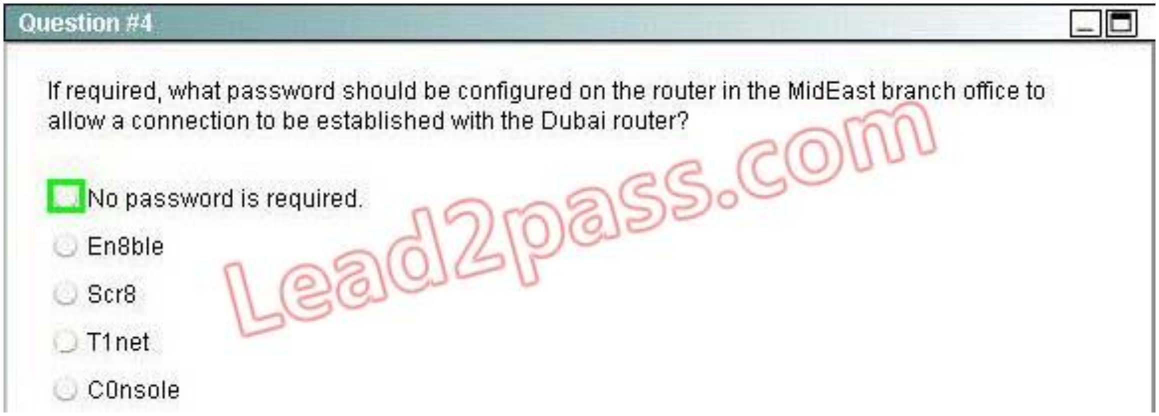
● The serial connection to the MidEast branch office.
○ The serial connection to the DeepSouth branch office.
○ The serial connection to the NorthCentral branch office.
○ The serial connection to the Multinational Core.

Answer: The serial connection to the MidEast branch office.
Explanation:
On the basis of the configuration on Dubai provided in the exhibit, we know that the encapsulation types of different interfaces are as follows:

```
Serial 1/0 : encapsulation frame-relay
Serial 1/2 and Serial 1/3 : both interfaces are encapsulated PPP
Serial 1/1: There is no related encapsulation information displayed, so
its default encapsulation type is HDLC .
```

Based on the network topology provided in the exhibit, the interface Serial 1/1 is connected to the router MidEast of the branch office, so the encapsulation type of the router MidEast is by default. The default encapsulation on a serial interface is HDLC. The original HDLC encapsulation was defined by the International Organization for Standards (ISO), those same folks who developed the OSI model. The ISO version of HDLC had one shortcoming, however; it had no options to support multiple Layer 3 routed protocols. As a result, most vendors have created their own form of HDLC. Cisco is no exception because it has its own proprietary form of HDLC to support various Layer 3 protocols such as IPX, IP, and AppleTalk.
The Serial connection to the Dub<i branch office using the default encapsulation type. You can change using:

```
* encapsulation <type> command on interface
```



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?

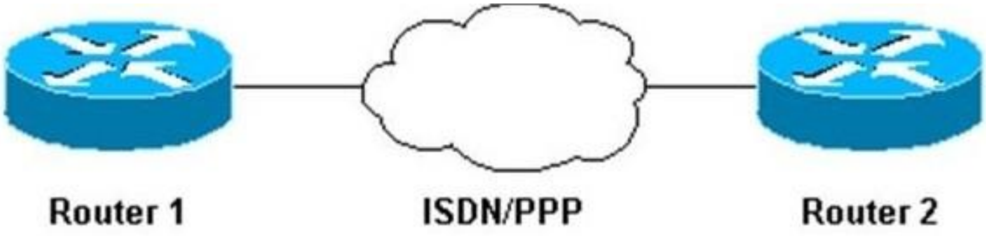
☑ No password is required.
○ En8ble
○ Scr8
○ T1net
○ C0nsole

Answer: Enable
Explanation:
In the diagram, DeepSouth is connected to Dubai's S1/2 interface and is configured as follows:

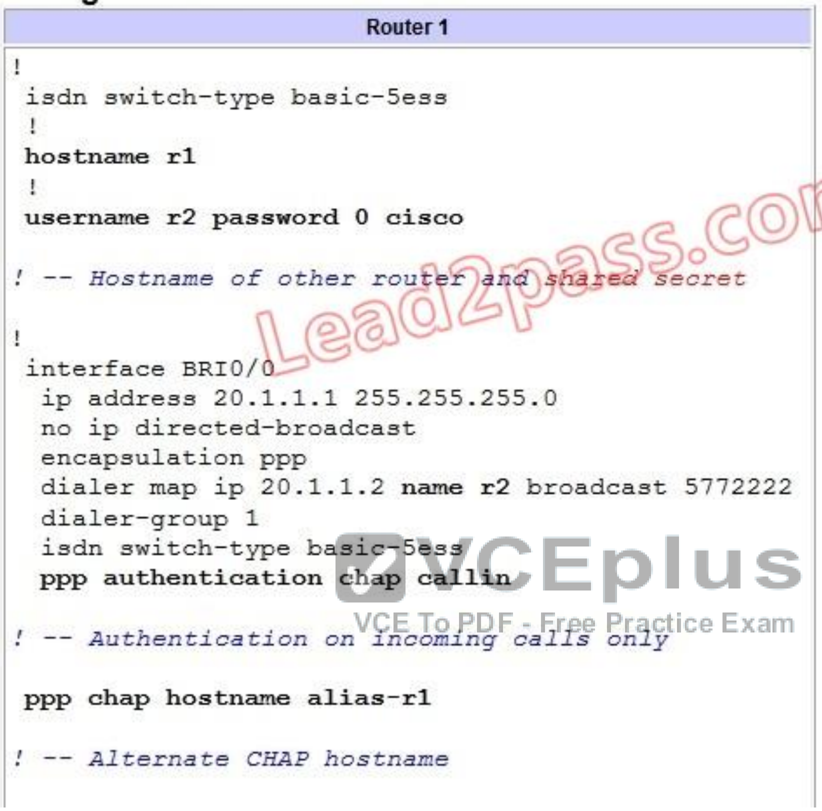
```
Interface Serial1/2
IP address 192.168.0.5 255.255.255.252
Encapsulalation PPP ; Encapsulation for this interface is PPP
```

Check out the following Cisco Link:
http://www.cisco.com/en/US/tech/tk713/tk507/technologies_configuration_example09186a008009 4333.shtml#configuringausernamedifferentfromtheroutersname

Here is a snipit of an example:
If Router 1 initiates a call to Router 2, Router 2 would challenge Router 1, but Router 1 would not challenge Router 2. This occurs because the ppp authentication chap callin command is configured on Router 1. This is an example of a unidirectional authentication. In this setup, the ppp chap hostname alias-r1 command is configured on Router 1. Router 1 uses "alias-r1" as its hostname for CHAP authentication instead of "r1." The Router 2 dialer map name should match Router 1's ppp chap hostname; otherwise, two B channels are established, one for each direction.



Configurations



Router 1

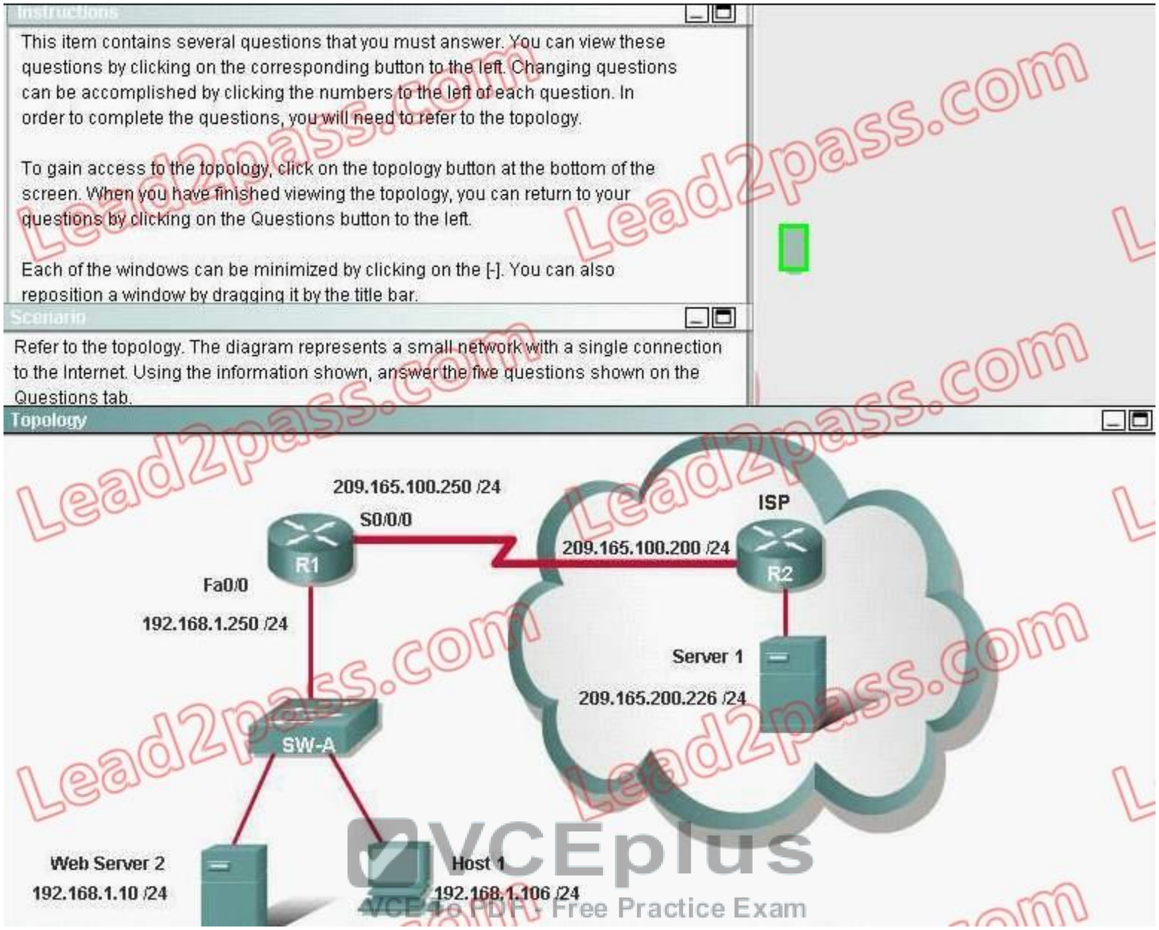
```
!
 isdn switch-type basic-5ess
 !
 hostname r1
 !
 username r2 password 0 cisco

! -- Hostname of other router and shared secret

!
 interface BRI0/0
  ip address 20.1.1.1 255.255.255.0
  no ip directed-broadcast
  encapsulation ppp
  dialer map ip 20.1.1.2 name r2 broadcast 5772222
  dialer-group 1
  isdn switch-type basic-5ess
  ppp authentication chap callin

! -- Authentication on incoming calls only

 ppp chap hostname alias-r1

! -- Alternate CHAP hostname
```

QUESTION 402
What are two recommended ways of protecting network device configuration files from outside network security threats? (Choose two.)

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

Answer: BD

QUESTION 403
Hotspot Question



Instructions

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

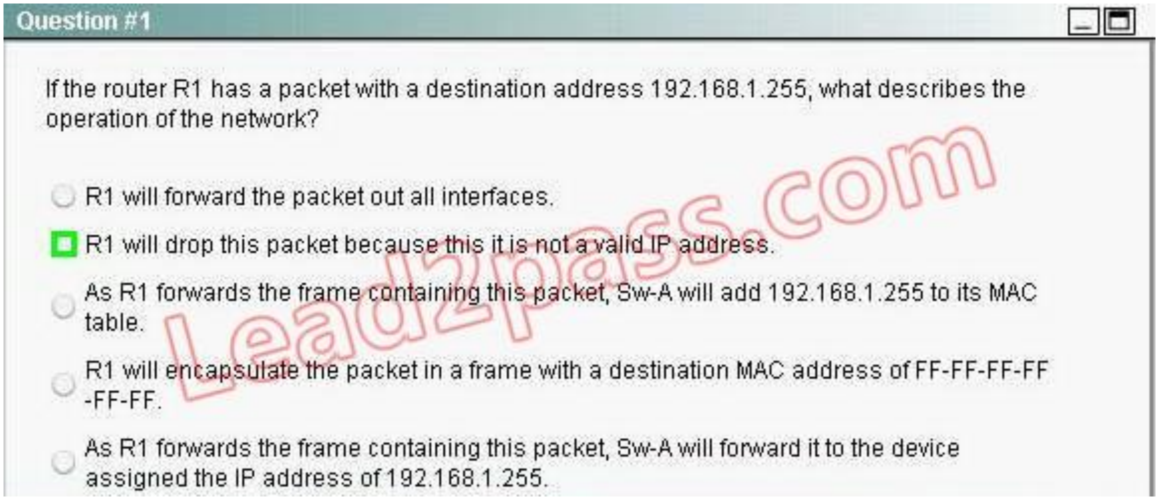
To gain access to the topology, click on the topology button at the bottom of the screen. When you have finished viewing the topology, you can return to your questions by clicking on the Questions button to the left.

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

Scenario

Refer to the topology. 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.

Topology



Question #1

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.

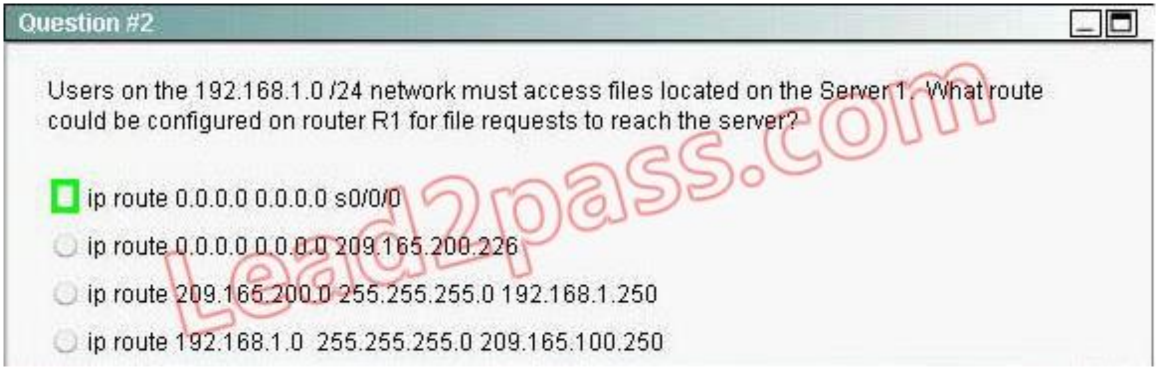
☑ R1 will drop this packet because this it is not a valid IP address.

○ 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.

Answer: R1 will drop this packet because this is not a valid IP address.



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

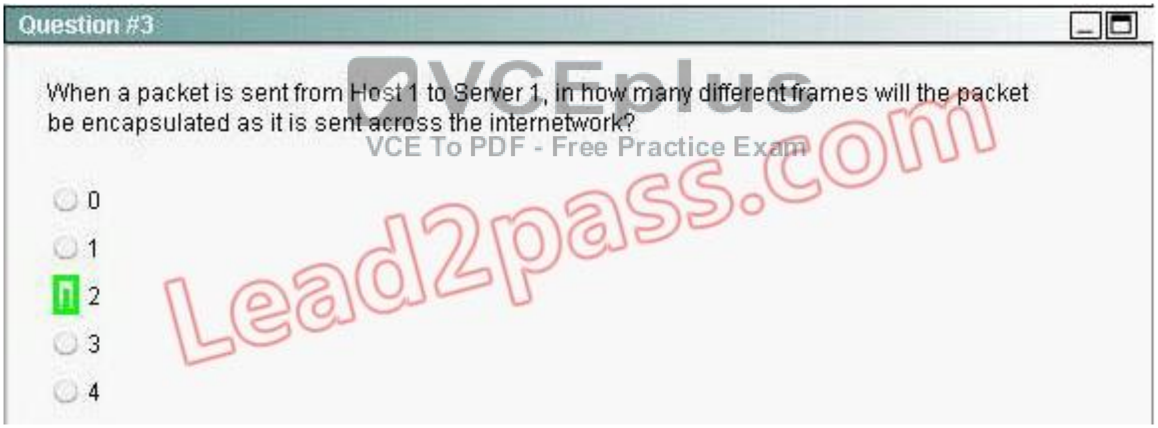
○ ip route 192.168.1.0 255.255.255.0 209.165.100.250

Answer: ip route 0.0.0.0 0.0.0.0 s0/0/0
Explanation:
In order to allow the network of 192.168.1.0/24 to access Server 1, we need to establish a default route. The format of this default route is as follows:

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

Based on the request of this subject, we need to configure the correct route as follows:

```
ip route 0.0.0.0 0.0.0.0 s0/0/0
```



Question #3

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

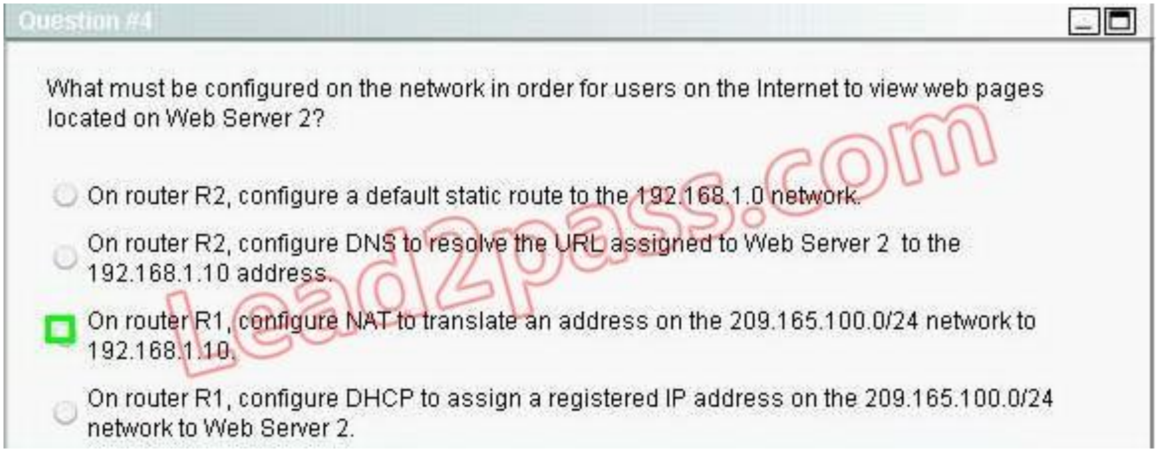
○ 1

● 2

○ 3

○ 4

Answer: 3
Explanation:
We believe the correct answer is 3 because the packet will be encapsulated in one more frame sent between routers R1 and R2. Source MAC is interface S0/0/0 on router R1 and destination is the serialinterface on router R2.



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.

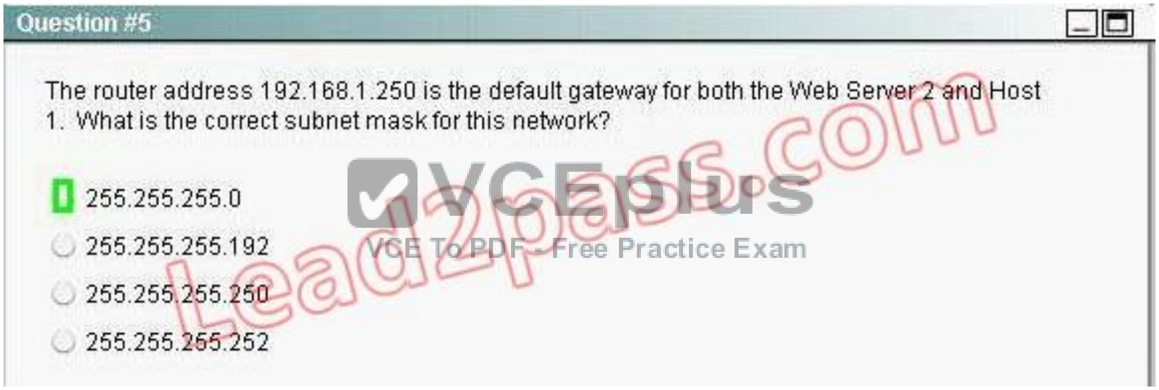
☑ On router R1, configure NAT to translate an address on the 209.165.100.0/24 network to 192.168.1.10.

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

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

Explanation:

In order to allow internet users to access Web Server 2, we need to configure NAT address translation on router R1.



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

Answer: 255.255.255.0

Explanation:

1. Based on the information provided in the exhibit, we know that the IP address of the interface Fa0/0 is 192.168.1.250/24, that is to say the subnet mask is 255.255.255.0??

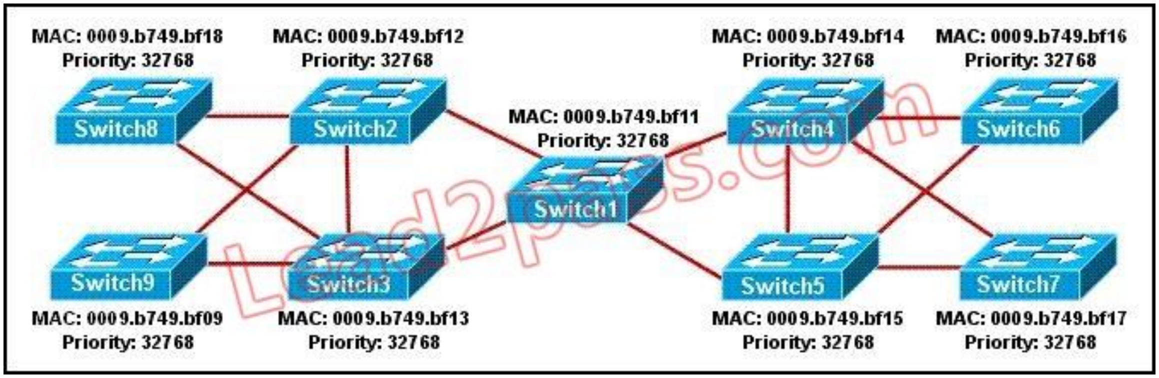
2. When configuring the correct IP address and not wasting IP address, the network of 192.168.1.0 needs to contain the following three IP addresses of interfaces:

```
R1(fa 0/0) : 192.168.1.250
Host 1: 192.168.1.106/24
Web server 2: 192.168.1.10/24
```

The correct mask is 255.255.255.0.

QUESTION 404

Refer to the exhibit. The switches on a campus network have been interconnected as shown. All of the switches are running Spanning Tree Protocol with its default settings. Unusual traffic patterns are observed and it is discovered that Switch9 is the root bridge. Which change will ensure that Switch1 will be selected as the root bridge instead of Switch9?



A. Raise the bridge priority on Switch1.
B. Lower the bridge priority on Switch9.
C. Raise the bridge priority on Switch9.
D. Physically replace Switch9 with Switch1 in the topology.
E. Disable spanning tree on Switch9.
F. Lower the bridge priority on Switch1.

Answer: F

QUESTION 405
The Company WAN is migrating from RIPv1 to RIPv2.
Which three statements are correct about RIP version 2? (Choose three)

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

Answer: ACE

QUESTION 406
If a router has four interfaces and each interface is connected to four switches, how many broadcast domains are present on the router?

A. 1
B. 2
C. 4
D. 8

Answer: C

QUESTION 407
Which command can you use to set the hostname on a switch?

A. switch-mdf-c1(config)#hostname switch-mdf1

B. switch-mdf-c1>hostname switch-mdf1
C. switch-mdf-c1#hostname switch-mdf1
D. switch-mdf-c1(config-if)#hostname switch-mdf1

Answer: A

QUESTION 408
If the primary root bridge experiences a power loss, which switch takes over?

A. switch 0004.9A1A.C182
B. switch 00E0.F90B.6BE3
C. switch 00E0.F726.3DC6
D. switch 0040.0BC0.90C5

Answer: A

QUESTION 409
Which IPv6 header field is equivalent to the TTL?

A. Hop Limit
B. Flow Label
C. TTD
D. Hop Count
E. Scan Timer

Answer: A

QUESTION 410
Which two statements about the tunnel mode ipv6ip command are true? (Choose two.)

A. It enables the transmission of IPv6 packets within the configured tunnel.
B. It specifies IPv4 as the encapsulation protocol.
C. It specifies IPv6 as the encapsulation protocol.
D. It specifies IPv6 as the transport protocol.
E. It specifies that the tunnel is a Teredo tunnel.

Answer: AB

QUESTION 411
What is the correct routing match to reach 172.16.1.5/32?

A. 172.16.1.0/26
B. 172.16.1.0/25
C. 172.16.1.0/24
D. the default route

Answer: A

QUESTION 412

Which step in the router boot process searches for an IOS image to load into the router?

A. bootstrap
B. POST
C. mini-IOS
D. ROMMON mode

Answer: A

QUESTION 413

Which command can you enter to route all traffic that is destined for 192.168.0.0/20 to a specific interface?

A. router(config)#ip route 192.168.0.0 255.255.240.0 GigabitEthernet0/1
B. router(config)#ip route 0.0.0.0 255.255.255.0 GigabitEthernet0/1
C. router(config)#ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/1
D. router(config)#ip route 192.168.0.0 255.255.255.0 GigabitEthernet0/1

Answer: A

QUESTION 414

Which technology allows a large number of private IP addresses to be represented by a smaller number of public IP addresses?

A. NAT
B. NTP
C. RFC 1631
D. RFC 1918

Answer: A

QUESTION 415

What is the effect of the overload keyword in a static NAT translation configuration?

A. It enables port address translation.
B. It enables the use of a secondary pool of IP addresses when the first pool is depleted.
C. It enables the inside interface to receive traffic.
D. It enables the outside interface to forward traffic.

Answer: A

QUESTION 416

Which protocol advertises a virtual IP address to facilitate transparent failover of a Cisco routing device?

A. FHRP
B. DHCP
C. RSMLT

D. ESRP

Answer: A

QUESTION 417
What are three broadband wireless technologies? (Choose three.)

A. WiMax
B. satellite Internet
C. municipal Wi-Fi
D. site-to-site VPN
E. DSLAM
F. CMTS

Answer: ABC

QUESTION 418
Which condition indicates that service password-encryption is enabled?

A. The local username password is encrypted in the configuration.
B. The enable secret is encrypted in the configuration.
C. The local username password is in clear text in the configuration.
D. The enable secret is in clear text in the configuration.

Answer: A

QUESTION 419
Which two spanning-tree port states does RSTP combine to allow faster convergence? (Choose two.)

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

Answer: AB

QUESTION 420
Which technology can enable multiple VLANs to communicate with one another?

A. inter-VLAN routing using a Layer 3 switch
B. inter-VLAN routing using a Layer 2 switch
C. intra-VLAN routing using router on a stick
D. intra-VLAN routing using a Layer 3 switch

Answer: A

QUESTION 421

In which three ways is an IPv6 header simpler than an IPv4 header? (Choose three.)

A. Unlike IPv4 headers, IPv6 headers have a fixed length.
B. IPv6 uses an extension header instead of the IPv4 Fragmentation field.
C. IPv6 headers eliminate the IPv4 Checksum field.
D. IPv6 headers use the Fragment Offset field in place of the IPv4 Fragmentation field.
E. IPv6 headers use a smaller Option field size than IPv4 headers.
F. IPv6 headers use a 4-bit TTL field, and IPv4 headers use an 8-bit TTL field.

Answer: ABC

QUESTION 422

Which feature builds a FIB and an adjacency table to expedite packet forwarding?

A. Cisco Express Forwarding
B. process switching
C. fast switching
D. cut-through

Answer: A

QUESTION 423

What is the purpose of the POST operation on a router?

A. determine whether additional hardware has been added
B. locate an IOS image for booting
C. enable a TFTP server
D. set the configuration register

Answer: A

QUESTION 424

Which command can you enter to set the default route for all traffic to an interface?

A. router(config)#ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/1
B. router(config)#ip route 0.0.0.0 255.255.255.255 GigabitEthernet0/1
C. router(config-router)#default-information originate
D. router(config-router)#default-information originate always

Answer: A

QUESTION 425

Which two types of NAT addresses are used in a Cisco NAT device? (Choose two.)

A. inside local
B. inside global
C. inside private

D. outside private
E. external global
F. external local

Answer: AB

QUESTION 426
What is the danger of the permit any entry in a NAT access list?

A. It can lead to overloaded resources on the router.
B. It can cause too many addresses to be assigned to the same interface.
C. It can disable the overload command.
D. It prevents the correct translation of IP addresses on the inside network.

Answer: A

QUESTION 427
Which protocol is the Cisco proprietary implementation of FHRP?

A. HSRP
B. VRRP
C. GLBP
D. CARP

Answer: A

QUESTION 428
Which two statements about late collisions are true? (Choose two.)

A. They may indicate a duplex mismatch.
B. By definition, they occur after the 512th bit of the frame has been transmitted.
C. They indicate received frames that did not pass the FCS match.
D. They are frames that exceed 1518 bytes.
E. They occur when CRC errors and interference occur on the cable.

Answer: AB

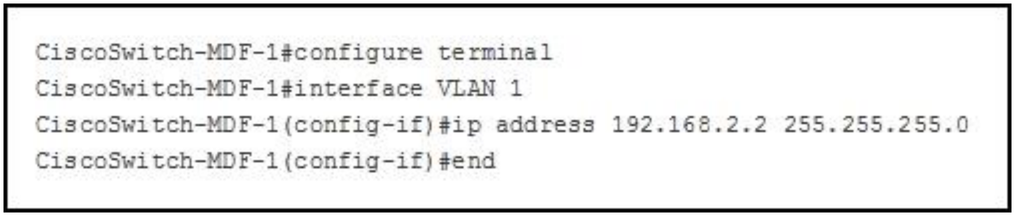
QUESTION 429
Which three characteristics are representative of a link-state routing protocol? (Choose three.)

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: ACD

QUESTION 430

Refer to the exhibit. What is the effect of the given configuration?



```
CiscoSwitch-MDF-1#configure terminal
CiscoSwitch-MDF-1#interface VLAN 1
CiscoSwitch-MDF-1(config-if)#ip address 192.168.2.2 255.255.255.0
CiscoSwitch-MDF-1(config-if)#end
```

A. It configures an inactive switch virtual interface.
B. It configures an active management interface.
C. It configures the native VLAN.
D. It configures the default VLAN.

Answer: A

QUESTION 431

Which command can you enter to view the ports that are assigned to VLAN 20?

A. Switch#show vlan id 20
B. Switch#show ip interface brief
C. Switch#show interface vlan 20
D. Switch#show ip interface vlan 20

Answer: A

QUESTION 432

If primary and secondary root switches with priority 16384 both experience catastrophic losses, which tertiary switch can take over?

A. a switch with priority 20480
B. a switch with priority 8192
C. a switch with priority 4096
D. a switch with priority 12288

Answer: A

QUESTION 433

Which two statements about IPv6 and routing protocols are true? (Choose two.)

A. Link-local addresses are used to form routing adjacencies.
B. OSPFv3 was developed to support IPv6 routing.
C. EIGRP, OSPF, and BGP are the only routing protocols that support IPv6.
D. Loopback addresses are used to form routing adjacencies.
E. EIGRPv3 was developed to support IPv6 routing.

Answer: AB

QUESTION 434

Which two features can dynamically assign IPv6 addresses? (Choose two.)

A. IPv6 stateless autoconfiguration
B. DHCP
C. NHRP
D. IPv6 stateful autoconfiguration
E. ISATAP tunneling

Answer: AB

QUESTION 435

Which command can you enter to configure a local username with an encrypted password and EXEC mode user privileges?

A. Router(config)#username jdone privilege 1 password 7 08314D5D1A48
B. Router(config)#username jdone privilege 1 password 7 PASSWORD1
C. Router(config)#username jdone privilege 15 password 0 08314D5D1A48
D. Router(config)#username jdone privilege 15 password 0 PASSWORD1

Answer: A

QUESTION 436

Which three commands can you use to set a router boot image? (Choose three.)

A. Router(config)# boot system flash c4500-p-mz.121-20.bin
B. Router(config)# boot system tftp c7300-js-mz.122-33.SB8a.bin
C. Router(config)#boot system rom c7301-advipservicesk9-mz.124-24.T4.bin
D. Router> boot flash:c180x-adventerprisek9-mz-124-6T.bin
E. Router(config)#boot flash:c180x-adventerprisek9-mz-124-6T.bin
F. Router(config)#boot bootldr bootflash:c4500-jk9s-mz.122-23f.bin

Answer: ABC

QUESTION 437

Which three statements about static routing are true? (Choose three.)

A. It uses consistent route determination.
B. It is best used for small-scale deployments.
C. Routing is disrupted when links fail.
D. It requires more resources than other routing methods.
E. It is best used for large-scale deployments.
F. Routers can use update messages to reroute when links fail.

Answer: ABC

QUESTION 438

Which type of address is the public IP address of a NAT device?

A. outside global
B. outside local
C. inside global
D. inside local
E. outside public
F. inside public

Answer: C

QUESTION 439
Which command can you enter to display the hits counter for NAT traffic?

A. show ip nat statistics
B. debug ip nat
C. show ip debug nat
D. clear ip nat statistics

Answer: A

QUESTION 440
Which standards-based First Hop Redundancy Protocol is a Cisco supported alternative to Hot Standby Router Protocol?

A. VRRP
B. GLBP
C. TFTP
D. DHCP

Answer: A

QUESTION 441
What are two reasons that duplex mismatches can be difficult to diagnose? (Choose two.)

A. The interface displays a connected (up/up) state even when the duplex settings are mismatched.
B. The symptoms of a duplex mismatch may be intermittent.
C. Autonegotiation is disabled.
D. Full-duplex interfaces use CSMA/CD logic, so mismatches may be disguised by collisions.
E. 1-Gbps interfaces are full-duplex by default.

Answer: AB

QUESTION 442
Which command can you execute to set the user inactivity timer to 10 seconds?

A. SW1(config-line)#exec-timeout 0 10
B. SW1(config-line)#exec-timeout 10
C. SW1(config-line)#absolute-timeout 0 10

D. SW1(config-line)#absolute-timeout 10

Answer: A

QUESTION 443
Which command sequence can you enter to create VLAN 20 and assign it to an interface on a switch?

A. Switch(config)#vlan 20
Switch(config)#Interface gig x/y
Switch(config-if)#switchport access vlan 20
B. Switch(config)#Interface gig x/y
Switch(config-if)#vlan 20
Switch(config-vlan)#switchport access vlan 20
C. Switch(config)#vlan 20
Switch(config)#Interface vlan 20
Switch(config-if)#switchport trunk native vlan 20
D. Switch(config)#vlan 20
Switch(config)#Interface vlan 20
Switch(config-if)#switchport access vlan 20
E. Switch(config)#vlan 20
Switch(config)#Interface vlan 20
Switch(config-if)#switchport trunk allowed vlan 20

Answer: A

QUESTION 444
Which spanning-tree protocol rides on top of another spanning-tree protocol?

A. MSTP
B. RSTP
C. PVST+
D. Mono Spanning Tree

Answer: A

QUESTION 445
Which two statements about IPv6 router advertisement messages are true? (Choose two.)

A. They use ICMPv6 type 134.
B. The advertised prefix length must be 64 bits.
C. The advertised prefix length must be 48 bits.
D. They are sourced from the configured IPv6 interface address.
E. Their destination is always the link-local address of the neighboring node.

Answer: AB

QUESTION 446
Which three statements about IPv6 prefixes are true? (Choose three.)

A. FF00:/8 is used for IPv6 multicast.
B. FE80::/10 is used for link-local unicast.
C. FC00::/7 is used in private networks.
D. 2001::1/127 is used for loopback addresses.
E. FE80::/8 is used for link-local unicast.
F. FEC0::/10 is used for IPv6 broadcast.

Answer: ABC

QUESTION 447
After you configure the Loopback0 interface, which command can you enter to verify the status of the interface and determine whether fast switching is enabled?

A. Router#show ip interface loopback 0
B. Router#show run
C. Router#show interface loopback 0
D. Router#show ip interface brief

Answer: A

QUESTION 448
Which three statements about link-state routing are true? (Choose three.)

A. Routes are updated when a change in topology occurs.
B. Updates are sent to a multicast address by default.
C. OSPF is a link-state protocol.
D. Updates are sent to a broadcast address.
E. RIP is a link-state protocol.
F. It uses split horizon.

Answer: ABC

QUESTION 449
Which NAT function can map multiple inside addresses to a single outside address?

A. PAT
B. SFTP
C. RARP
D. ARP
E. TFTP

Answer: A

QUESTION 450
What is the first step in the NAT configuration process?

A. Define inside and outside interfaces.

B. Define public and private IP addresses.
C. Define IP address pools.
D. Define global and local interfaces.

Answer: A

QUESTION 451
What are two requirements for an HSRP group? (Choose two.)

A. exactly one active router
B. one or more standby routers
C. one or more backup virtual routers
D. exactly one standby active router
E. exactly one backup virtual router

Answer: AB

QUESTION 452
Which two commands can you enter to verify that a configured NetFlow data export is operational? (Choose two.)

A. show ip flow export
B. show ip cache flow
C. ip flow ingress
D. ip flow egress
E. interface ethernet 0/0
F. ip flow-export destination

Answer: AB

QUESTION 453
What are three characteristics of satellite Internet connections? (Choose three.)

A. Their upload speed is about 10 percent of their download speed.
B. They are frequently used by rural users without access to other high-speed connections.
C. They are usually at least 10 times faster than analog modem connections.
D. They are usually faster than cable and DSL connections.
E. They require a WiMax tower within 30 miles of the user location.
F. They use radio waves to communicate with cellular phone towers.

Answer: ABC

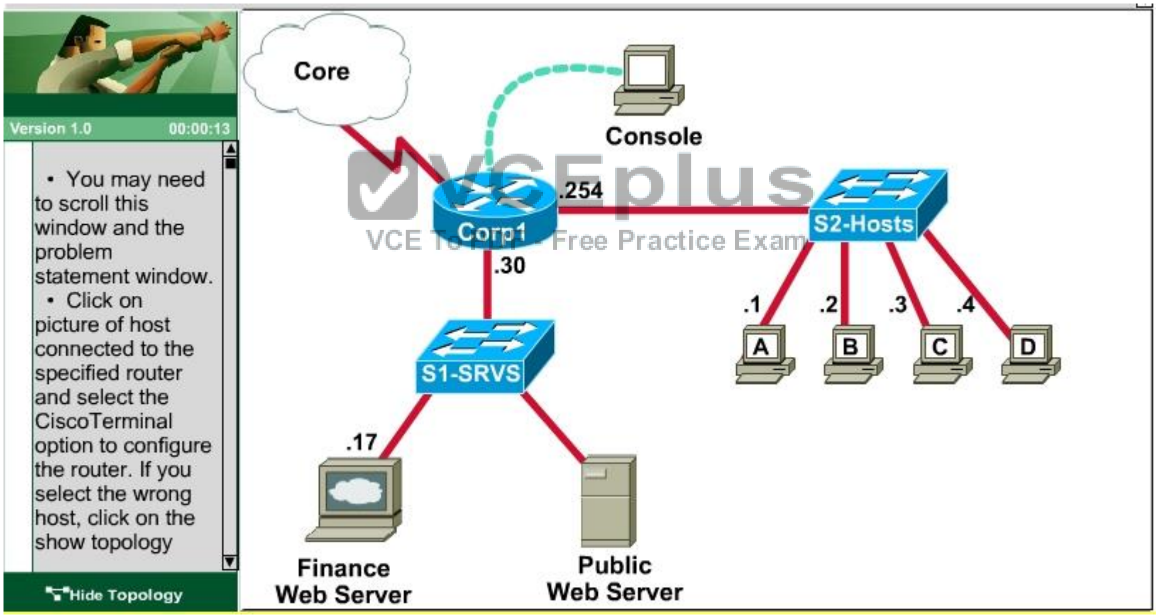
QUESTION 454
Lab Simulation Question - ACL-5
A corporation wants to add security to its network. The requirements are:

```
- Host C should be able to use a web browser (HTTP) to access the
Finance Web Server.
- Other types of access from host C to the Finance Web Server should be
```

blocked.
- All access from hosts in the Core or local LAN to the Finance Web Server should be blocked.
- All hosts in the Core and on local LAN should be able to access the Public Web Server.

You have been tasked to create and apply a numbered access list to a single outbound interface. This access list can contain no more than three statements that meet these requirements. Access to the router CLI can be gained by clicking on the appropriate host.

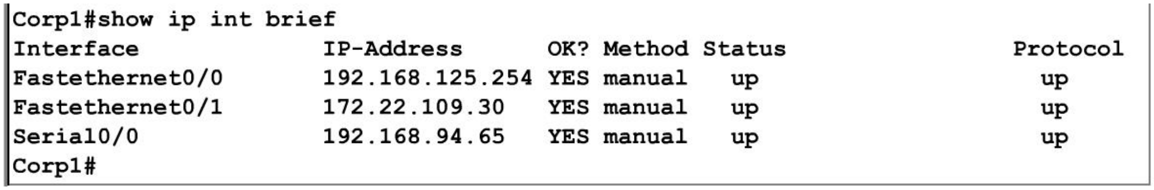
- All passwords have been temporarily set to "cisco".
- The Core connection uses an IP address of 198.18.209.65.
- The computers in the Hosts LAN have been assigned addresses of 192.168.78.1 - 192.168.78.254.
- host A 192.168.78.1
- host B 192.168.78.2
- host C 192.168.78.3
- host D 192.168.78.4
- The Finance Web Server has been assigned an address of 172.22.146.17.
- The Public Web Server in the Server LAN has been assigned an address of 172.22.146.18.



- 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

Answer:
Please see below explanation part for details answer steps:

We should create an access-list and apply it to the interface that is connected to the Server LAN because it can filter out traffic from both S2 and Core networks. To see which interface this is, use the “show ip int brief” command:



```
Corp1#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
Fastethernet0/0        192.168.125.254 YES manual   up                    up
Fastethernet0/1        172.22.109.30   YES manual   up                    up
Serial0/0              192.168.94.65   YES manual   up                    up
Corp1#
```

From this, we know that the servers are located on the fa0/1 interface, so we will place our numbered access list here in the outbound direction.

Corp1#configure terminal

Our access-list needs to allow host C – 192.168125.3 to the Finance Web Server 172.22.109.17 via HTTP (port 80), so our first line is this:

Corp1(config)#access-list 100 permit tcp host 192.168.125.3 host 172.22.109.17 eq 80

Then, our next two instructions are these:

- Other types of access from host C to the Finance Web Server should be blocked.
- All access from hosts in the Core or local LAN to the Finance Web Server should be blocked.

This can be accomplished with one command (which we need to do as our ACL needs to be no more than 3 lines long), blocking all other access to the finance web server:

Corp1(config)#access-list 100 deny ip any host 172.22.109.17

Our last instruction is to allow all hosts in the Core and on the local LAN access to the Public Web Server (172.22.109.18)

Corp1(config)#access-list 100 permit ip host 172.22.109.18 any

Finally, 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.
To verify, just click on host C to open its web browser. In the address box type **http://172.22.109.17** 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. Then, repeat to make sure they can reach the public server at 172.22.109.18. Finally, save the configuration

Corp1(config-if)#end
Corp1#copy running-config startup-config

QUESTION 455

Which command sets and automatically encrypts the privileged enable mode password?

A. Enable password c1sc0
B. Secret enable c1sc0
C. Password enable c1sc0
D. Enable secret c1sc0

Answer: D

QUESTION 456

The enable secret command is used to secure access to which CLI mode?

A. global configuration mode
B. privileged EXEC mode
C. user EXEC mode
D. auxiliary setup mode

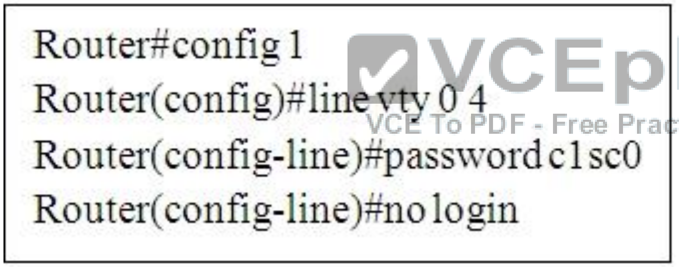
Answer: B

QUESTION 457
The enable secret command is used to secure access to which CLI mode?

A. global configuration mode
B. privileged EXEC mode
C. user EXEC mode
D. auxiliary setup mode

Answer: B

QUESTION 458
Refer to the exhibit. What is the result of setting the no login command?



```
Router#config 1
Router(config)#line vty 0 4
Router(config-line)#password c1sc0
Router(config-line)#no login
```

A. Telnet access is denied.
B. Telnet access requires a new password at the first login.
C. Telnet access requires a new password.
D. no password is required for telnet access.

Answer: D

QUESTION 459
Which option describes a difference between EIGRP for IPv4 and IPv6?

A. Only EIGRP for IPv6 advertises all connected networks.
B. Only EIGRP for IPv6 requires a router ID to be configured under the routing process-
C. AS numbers are configured in EIGRP but not in EIGRPv3.
D. Only EIGRP for IPv6 is enabled in the global configuration mode.

Answer: B
Explanation:
Router ID - Both EIGRP for IPv4 and EIGRP for IPv6 use a 32-bit number for the EIGRP router

ID. The 32-bit router ID is represented in dotted-decimal notation and is commonly referred to as an IPv4 address. If the EIGRP for IPv6 router has not been configured with an IPv4 address, the eigrp router-id command must be used to configure a 32-bit router ID. The process for determining the router ID is the same for both EIGRP for IPv4 and IPv6.

QUESTION 460
What is the best way to verify that a host has a path to other hosts in different networks?

A. Ping the loopback address.
B. Ping the default gateway.
C. Ping the local interface address.
D. Ping the remote network.

Answer: D
Explanation:
Ping is a tool that helps to verify IP-level connectivity; PathPing is a tool that detects packet loss over multiple-hop trips. When troubleshooting, the ping command is used to send an ICMP Echo Request to a target host name or IP address. Use Ping whenever you want to verify that a host computer can send IP packets to a destination host. You can also use the Ping tool to isolate network hardware problems and incompatible configurations. If you call ipconfig /all and receive a response, there is no need to ping the loopback address and your own IP address -- Ipconfig has already done so in order to generate the report.
It is best to verify that a route exists between the local computer and a network host by first using ping and the IP address of the network host to which you want to connect. The command syntax is:
ping < IP address >
Perform the following steps when using Ping:
Ping the loopback address to verify that TCP/IP is installed and configured correctly on the local computer.
ping 127.0.0.1
If the loopback step fails, the IP stack is not responding. This might be because the TCP drivers are corrupted, the network adapter might not be working, or another service is interfering with IP.
Ping the IP address of the local computer to verify that it was added to the network correctly. Note that if the routing table is correct, this simply forwards the packet to the loopback address of 127.0.0.1.
ping < IP address of local host >
Ping the IP address of the default gateway to verify that the default gateway is functioning and that you can communicate with a local host on the local network.
ping < IP address of default gateway >
Ping the IP address of a remote host to verify that you can communicate through a router.
ping < IP address of remote host >
Ping the host name of a remote host to verify that you can resolve a remote host name.
ping < Host name of remote host >
Run a PathPing analysis to a remote host to verify that the routers on the way to the destination are operating correctly.
pathping < IP address of remote host >

QUESTION 461
If host Z needs to send data through router R1 to a storage server, which destination MAC address does host Z use to transmit packets?

A. the host Z MAC address
B. the MAC address of the interface on R1 that connects to the storage server

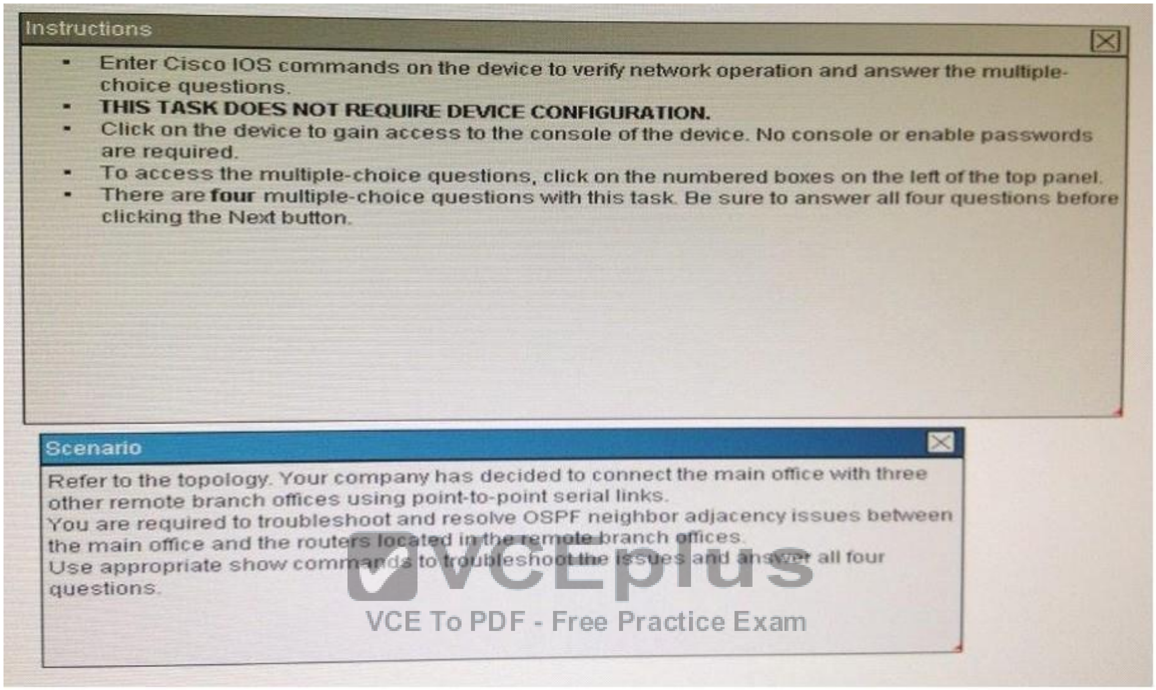
C. the MAC address of the interface on R1 that connects to host Z

D. the MAC address of the storage server interface

Answer: C

QUESTION 462

Hotspot Questions

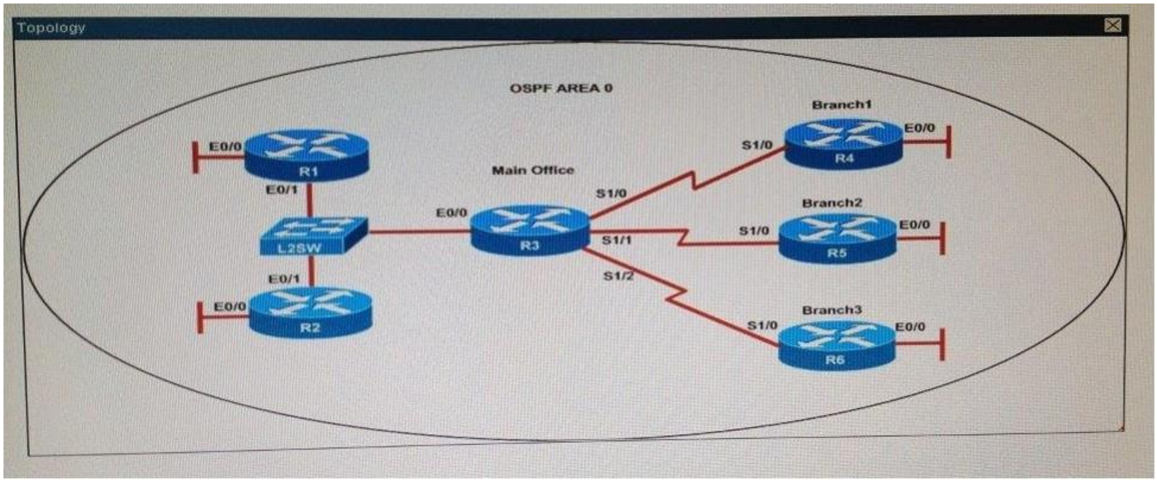


Instructions

- Enter Cisco IOS commands on the device to verify network operation and answer the multiple-choice questions.
- **THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.**
- Click on the device to gain access to the console of the device. No console or enable passwords are required.
- To access the multiple-choice questions, click on the numbered boxes on the left of the top panel.
- There are **four** multiple-choice questions with this task. Be sure to answer all four questions before clicking the Next button.

Scenario

Refer to the topology. Your company has decided to connect the main office with three other remote branch offices using point-to-point serial links.
You are required to troubleshoot and resolve OSPF neighbor adjacency issues between the main office and the routers located in the remote branch offices.
Use appropriate show commands to troubleshoot the issues and answer all four questions.



```
R1# show running-config
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 10.10.230.1 255.255.255.0
ip ospf hello-interval 25
ip ospf 1 area 0
!
log-adjacency-changes


R2# show running-config
R2
!
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**
ip address 10.10.230.2 255.255.255.0
ip ospf 2 area 0
!
router ospf 2
log-adjacency-changes

R3# show running-config
R3
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
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# show running-config

```
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
!
router ospf 4
log-adjacency-changes
```

R5# show running-config

```
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
!
router ospf 5
log-adjacency-changes
```

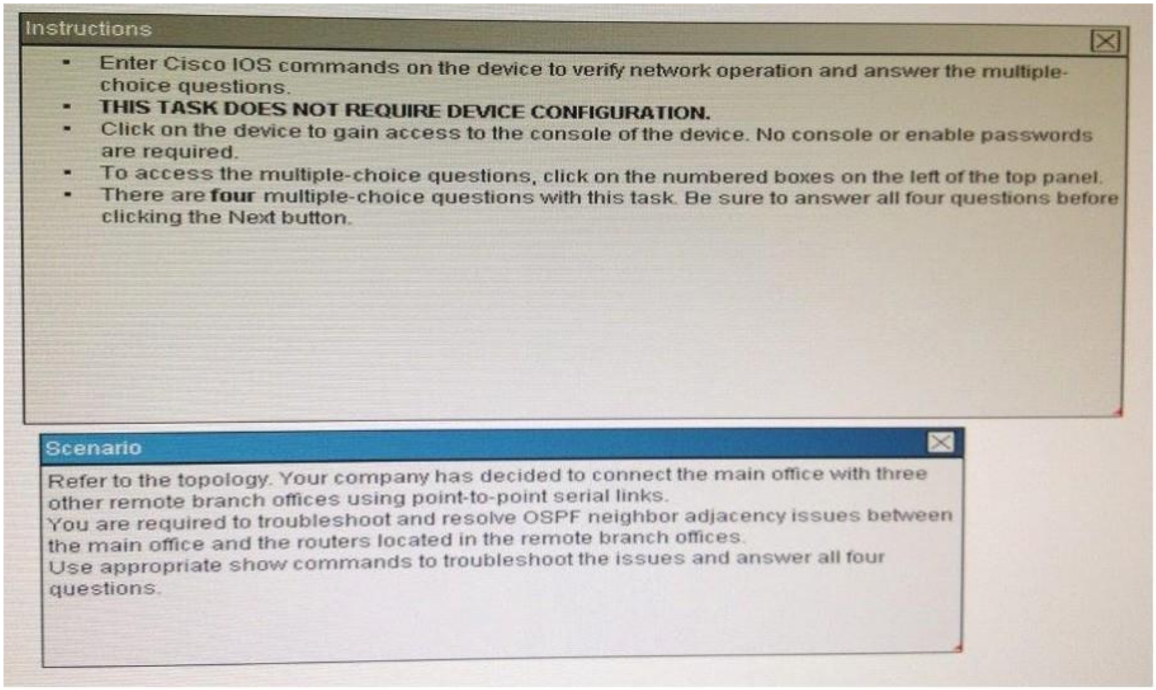
```
R6# show running-config
R6
username R3 password CISCO36
!
interface Loopback0
description **Loopback**
ip address 192.168.6.6 255.255.255.255
ip ospf 6 area 0
!
interface Ethernet0/0
ip address 172.16.115.1 255.255.255.0
ip ospf 6 area 0
!
interface Serial1/0
description **Connected to R3-Main Branch office**
ip address 10.10.240.10 255.255.255.252
encapsulation ppp
ip ospf 6 area 0
ppp authentication chap
!
router ospf 6
router-id 192.168.3.3
!
```

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

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

Answer: D

QUESTION 463
Hotspot Questions

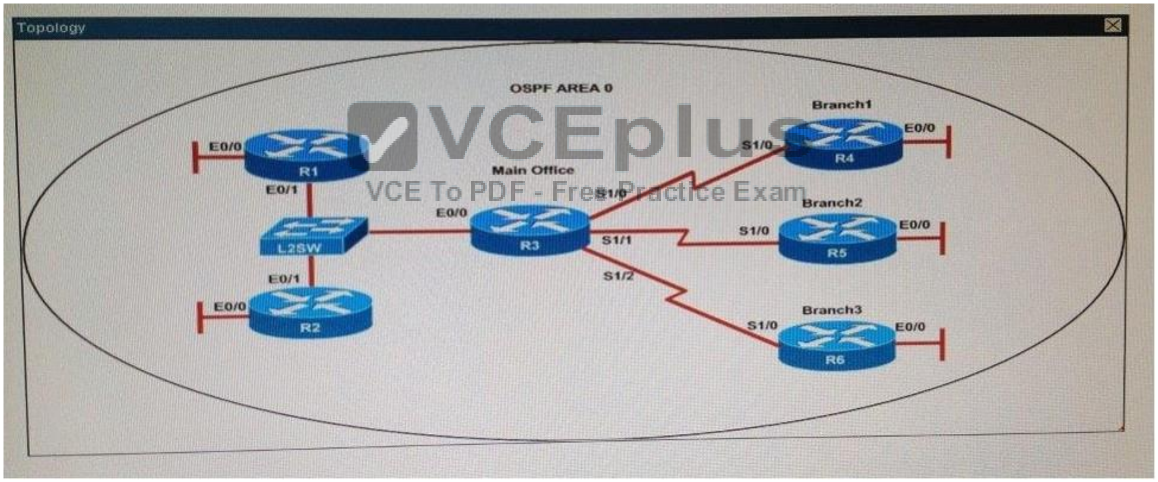


Instructions

- Enter Cisco IOS commands on the device to verify network operation and answer the multiple-choice questions.
- **THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.**
- Click on the device to gain access to the console of the device. No console or enable passwords are required.
- To access the multiple-choice questions, click on the numbered boxes on the left of the top panel.
- There are **four** multiple-choice questions with this task. Be sure to answer all four questions before clicking the Next button.

Scenario

Refer to the topology. Your company has decided to connect the main office with three other remote branch offices using point-to-point serial links.
You are required to troubleshoot and resolve OSPF neighbor adjacency issues between the main office and the routers located in the remote branch offices.
Use appropriate show commands to troubleshoot the issues and answer all four questions.



```
R1# show running-config
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 10.10.230.1 255.255.255.0
ip ospf hello-interval 25
ip ospf 1 area 0
```

```
!
log-adjacency-changes


R2# show running-config
R2
!
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**
ip address 10.10.230.2 255.255.255.0
ip ospf 2 area 0
!
router ospf 2
log-adjacency-changes

R3# show running-config
R3
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
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# show running-config
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
!
router ospf 4
log-adjacency-changes

R5# show running-config
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
!
router ospf 5
log-adjacency-changes

R6# show running-config
R6
username R3 password CISCO36
!
interface Loopback0
description **Loopback**
ip address 192.168.6.6 255.255.255.255
ip ospf 6 area 0
!
```

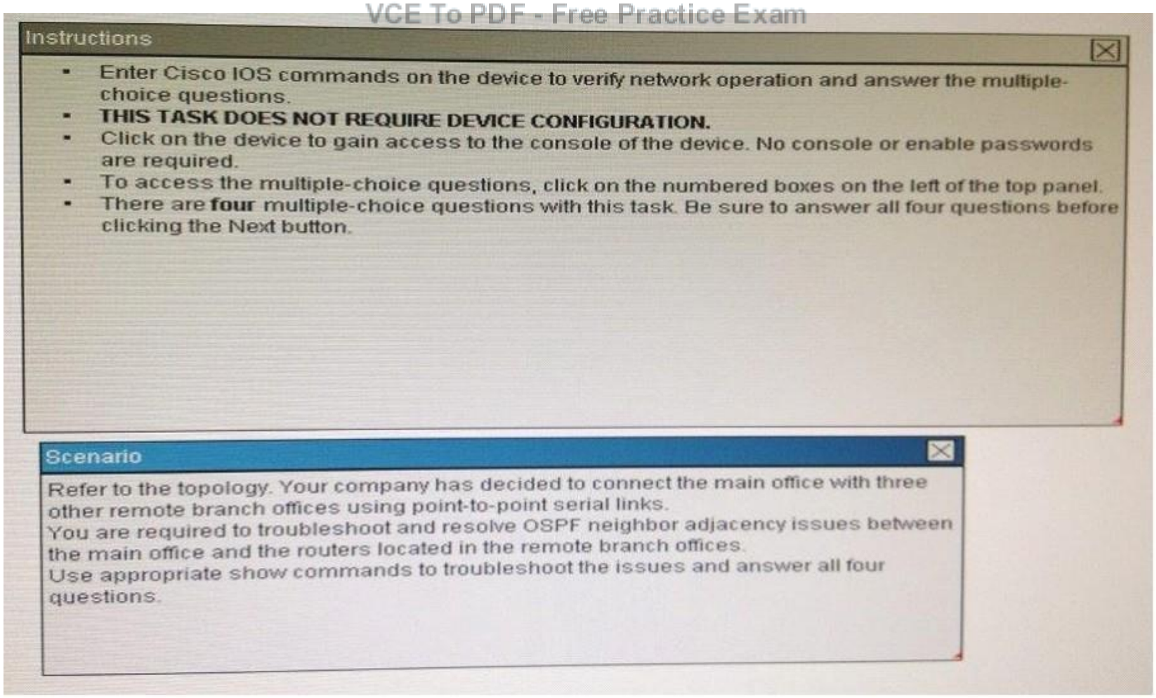
```
interface Ethernet0/0
ip address 172.16.115.1 255.255.255.0
ip ospf 6 area 0
!
interface Serial1/0
description **Connected to R3-Main Branch office**
ip address 10.10.240.10 255.255.255.252
encapsulation ppp
ip ospf 6 area 0
ppp authentication chap
!
router ospf 6
router-id 192.168.3.3
!
```

An OSPF neighbor adjacency is not formed between R3 in the main office and R4 in the Branch1 office. What is causing the problem?

A. There is an area ID mismatch.
B. There is a Layer 2 issue; an encapsulation mismatch on serial links.
C. There is an OSPF hello and dead interval mismatch.
D. The R3 router ID is configured on R4.

Answer: A

QUESTION 464
Hotspot Questions

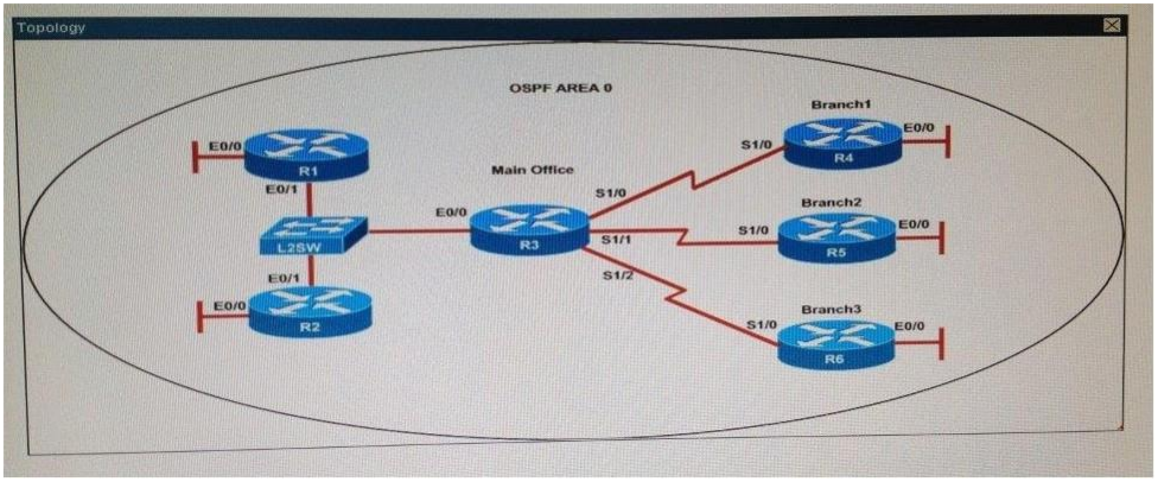


Instructions

- Enter Cisco IOS commands on the device to verify network operation and answer the multiple-choice questions.
- **THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.**
- Click on the device to gain access to the console of the device. No console or enable passwords are required.
- To access the multiple-choice questions, click on the numbered boxes on the left of the top panel.
- There are **four** multiple-choice questions with this task. Be sure to answer all four questions before clicking the Next button.

Scenario

Refer to the topology. Your company has decided to connect the main office with three other remote branch offices using point-to-point serial links.
You are required to troubleshoot and resolve OSPF neighbor adjacency issues between the main office and the routers located in the remote branch offices.
Use appropriate show commands to troubleshoot the issues and answer all four questions.



```
R1# show running-config
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 10.10.230.1 255.255.255.0
ip ospf hello-interval 25
ip ospf 1 area 0
!
log-adjacency-changes
```

```
R2# show running-config
R2
!
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**
ip address 10.10.230.2 255.255.255.0
ip ospf 2 area 0
!
router ospf 2
log-adjacency-changes
```

R3# show running-config

```
R3
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
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# show running-config

```
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
!
```

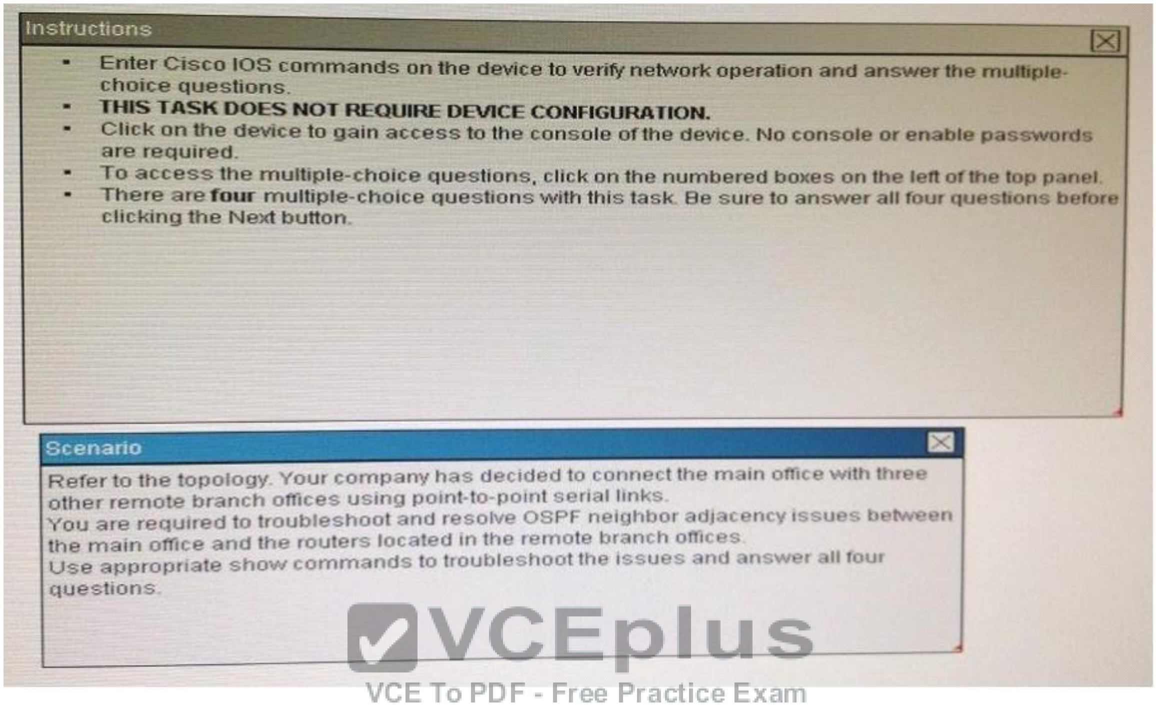
```
router ospf 4
log-adjacency-changes

R5# show running-config
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
!
router ospf 5
log-adjacency-changes

R6# show running-config
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
ip ospf 6 area 0
ppp authentication chap
!
router ospf 6
router-id 192.168.3.3
!
```

R1 does not form an OSPF neighbor adjacency with R2. Which option would fix the issue?

A. R1 ethernet0/1 is shutdown. Configure the no shutdown command.
B. R1 ethernet0/1 configured with a non-default OSPF hello interval of 25, configure no ip ospf hello interval 25
C. R2 ethernet0/1 and R3 ethernet0/0 are configured with a non-default OSPF hello interval of 25; configure no ip ospf hello interval 25
D. Enable OSPF for R1 ethernet0/1; configure ip ospf 1 area 0 command under ethernet0/1

Answer: B

QUESTION 465
Hotspot Questions

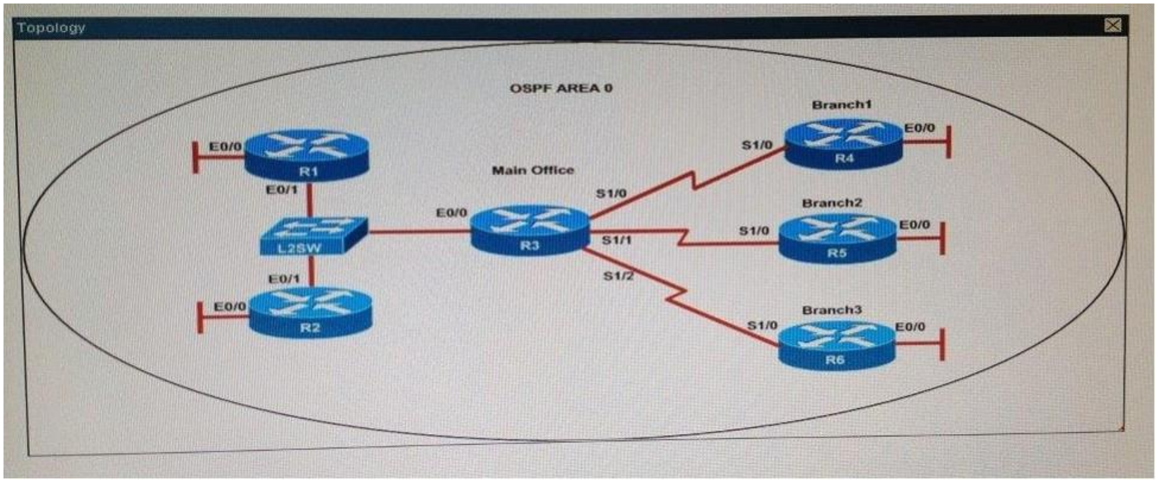


Instructions

- Enter Cisco IOS commands on the device to verify network operation and answer the multiple-choice questions.
- **THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.**
- Click on the device to gain access to the console of the device. No console or enable passwords are required.
- To access the multiple-choice questions, click on the numbered boxes on the left of the top panel.
- There are **four** multiple-choice questions with this task. Be sure to answer all four questions before clicking the Next button.

Scenario

Refer to the topology. Your company has decided to connect the main office with three other remote branch offices using point-to-point serial links.
You are required to troubleshoot and resolve OSPF neighbor adjacency issues between the main office and the routers located in the remote branch offices.
Use appropriate show commands to troubleshoot the issues and answer all four questions.



```
R1# show running-config
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 10.10.230.1 255.255.255.0
ip ospf hello-interval 25
ip ospf 1 area 0
!
log-adjacency-changes
```

R2# show running-config

```
R2
!
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**
ip address 10.10.230.2 255.255.255.0
ip ospf 2 area 0
!
router ospf 2
log-adjacency-changes
```

R3# show running-config

```
R3
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
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# show running-config

```
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
!
router ospf 4
log-adjacency-changes
```

R5# show running-config

```
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
!
router ospf 5
log-adjacency-changes
```

R6# show running-config

```
R6
```

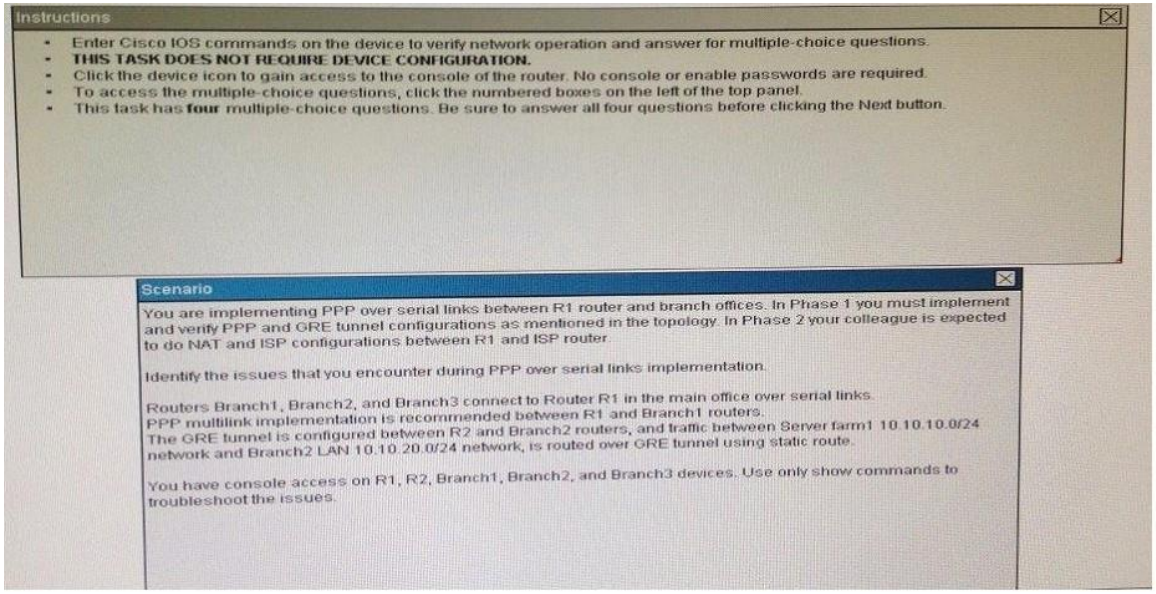
```
username R3 password CISCO36
!
interface Loopback0
description **Loopback**
ip address 192.168.6.6 255.255.255.255
ip ospf 6 area 0
!
interface Ethernet0/0
ip address 172.16.115.1 255.255.255.0
ip ospf 6 area 0
!
interface Serial1/0
description **Connected to R3-Main Branch office**
ip address 10.10.240.10 255.255.255.252
encapsulation ppp
ip ospf 6 area 0
ppp authentication chap
!
router ospf 6
router-id 192.168.3.3
!
```

An OSPF neighbor adjacency is not formed between R3 in the main office and R5 in the Branch2 office. What is causing the problem?

A. There is an area ID mismatch.
B. There is a PPP authentication issue; a password mismatch.
C. There is an OSPF hello and dead interval mismatch.
D. There is a missing network command in the OSPF process on R5.

Answer: C

QUESTION 466
Hotspot Questions



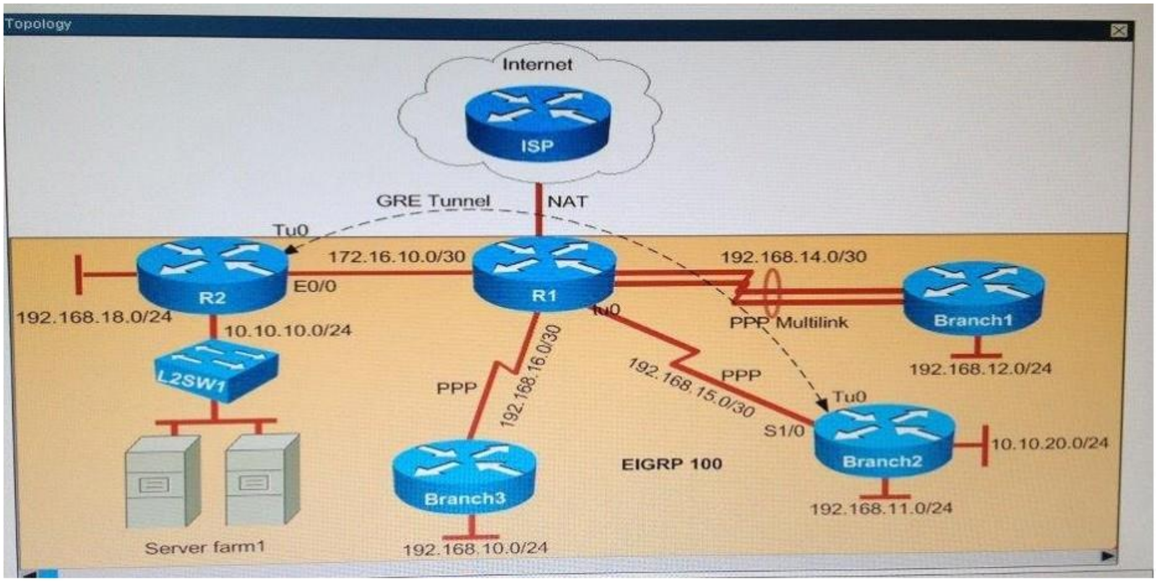
- Enter Cisco IOS commands on the device to verify network operation and answer for multiple-choice questions.
- **THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.**
- Click the device icon to gain access to the console of the router. No console or enable passwords are required.
- To access the multiple-choice questions, click the numbered boxes on the left of the top panel.
- This task has **four** multiple-choice questions. Be sure to answer all four questions before clicking the Next button.

You are implementing PPP over serial links between R1 router and branch offices. In Phase 1 you must implement and verify PPP and GRE tunnel configurations as mentioned in the topology. In Phase 2 your colleague is expected to do NAT and ISP configurations between R1 and ISP router.

Identify the issues that you encounter during PPP over serial links implementation.

Routers Branch1, Branch2, and Branch3 connect to Router R1 in the main office over serial links.
PPP multilink implementation is recommended between R1 and Branch1 routers.
The GRE tunnel is configured between R2 and Branch2 routers, and traffic between Server farm1 10.10.10.0/24 network and Branch2 LAN 10.10.20.0/24 network, is routed over GRE tunnel using static route.

You have console access on R1, R2, Branch1, Branch2, and Branch3 devices. Use only show commands to troubleshoot the issues.

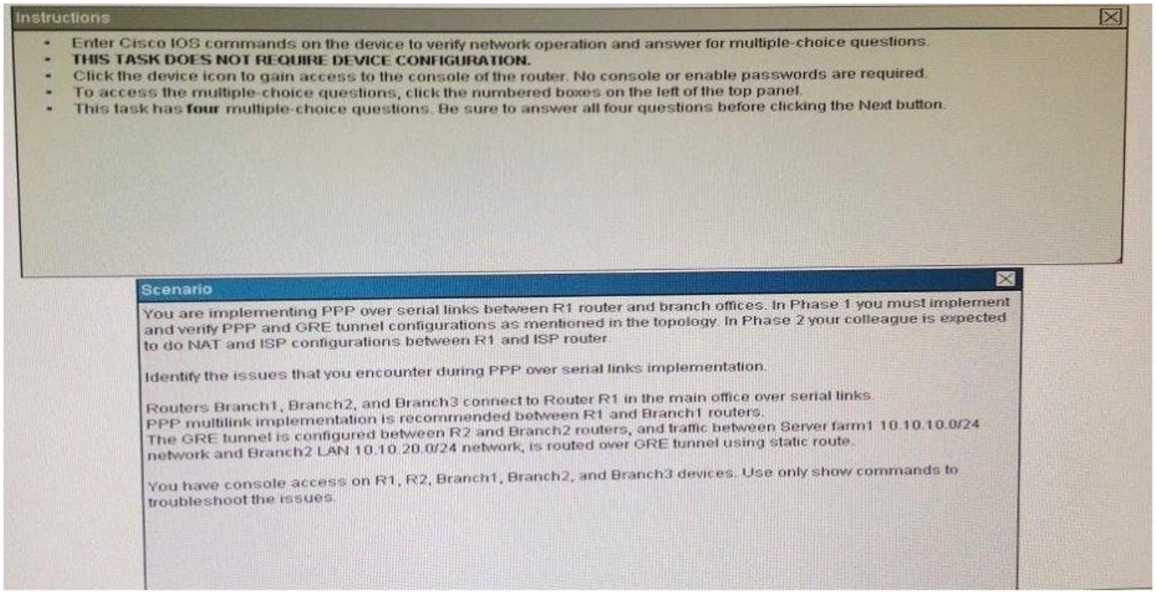


Why is the Branch2 network 10.1 0.20.0/24 unable to communicate with the Server farm1 network 10.1 0.10.0/24 over the GRE tunnel?

A. The GRE tunnel destination is not configured on the R2 router.
B. The GRE tunnel destination is not configured on the Branch2 router.
C. The static route points to the tunnel0 interface that is misconfigured on the Branch2 router.
D. The static route points to the tunnel0 interface that is misconfigured on the R2 router.

Answer: C

QUESTION 467
Hotspot Questions


Instructions

- Enter Cisco IOS commands on the device to verify network operation and answer for multiple-choice questions.
- **THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.**
- Click the device icon to gain access to the console of the router. No console or enable passwords are required.
- To access the multiple-choice questions, click the numbered boxes on the left of the top panel.
- This task has **four** multiple-choice questions. Be sure to answer all four questions before clicking the Next button.

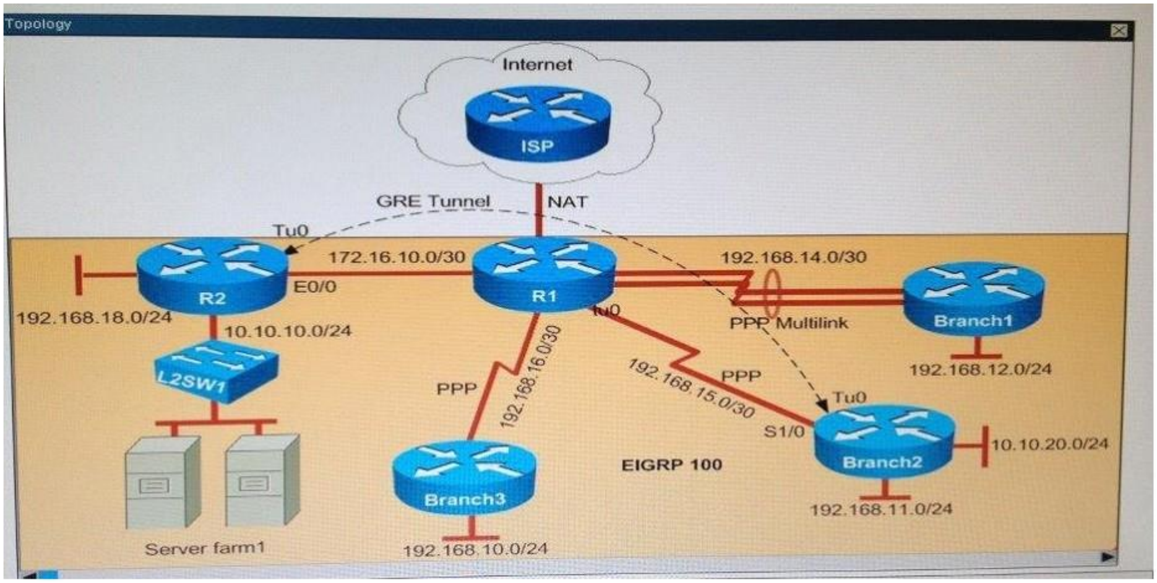
Scenario

You are implementing PPP over serial links between R1 router and branch offices. In Phase 1 you must implement and verify PPP and GRE tunnel configurations as mentioned in the topology. In Phase 2 your colleague is expected to do NAT and ISP configurations between R1 and ISP router.

Identify the issues that you encounter during PPP over serial links implementation.

Routers Branch1, Branch2, and Branch3 connect to Router R1 in the main office over serial links.
PPP multilink implementation is recommended between R1 and Branch1 routers.
The GRE tunnel is configured between R2 and Branch2 routers, and traffic between Server farm1 10.10.10.0/24 network and Branch2 LAN 10.10.20.0/24 network, is routed over GRE tunnel using static route.

You have console access on R1, R2, Branch1, Branch2, and Branch3 devices. Use only show commands to troubleshoot the issues.

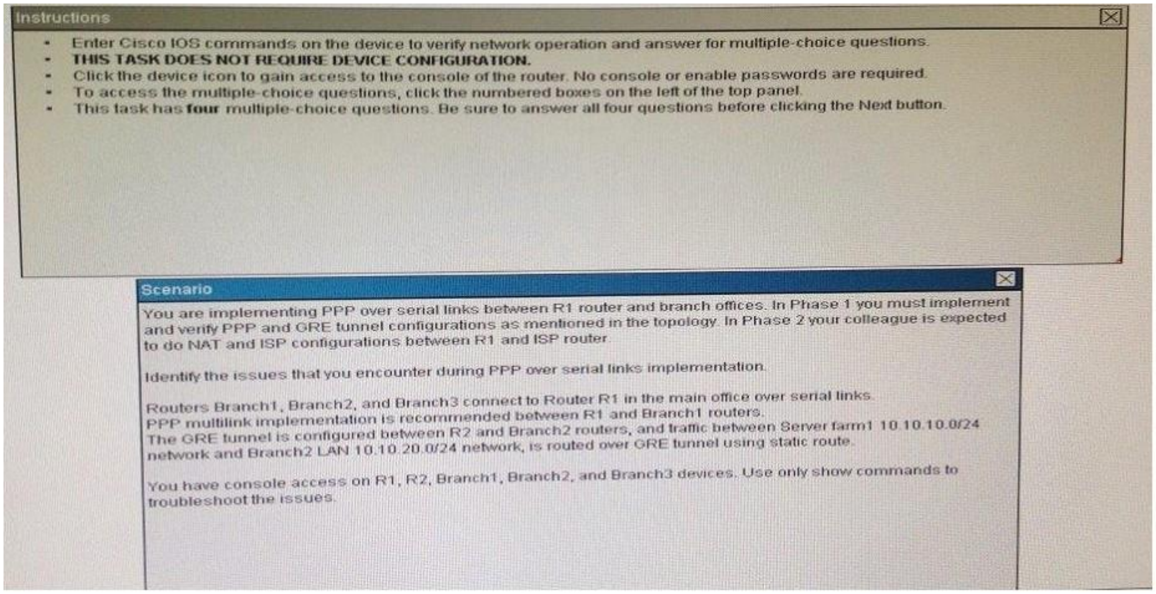


Why has the Branch3 router lost connectivity with R1?
Use only show commands to troubleshoot because usage of the debug command is restricted on the Branch3 and R1 routers.

A. A PPP chap hostname mismatch is noticed between Branch3 and R1.
B. A PPP chap password mismatch is noticed between Branch3 and R1.
C. PPP encapsulation is not configured on Branch3.
D. The PPP chap hostname and PPP chap password commands are missing on the Branch3 router.

Answer: A

QUESTION 468
Hotspot Questions


Instructions

- Enter Cisco IOS commands on the device to verify network operation and answer for multiple-choice questions.
- **THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.**
- Click the device icon to gain access to the console of the router. No console or enable passwords are required.
- To access the multiple-choice questions, click the numbered boxes on the left of the top panel.
- This task has **four** multiple-choice questions. Be sure to answer all four questions before clicking the Next button.

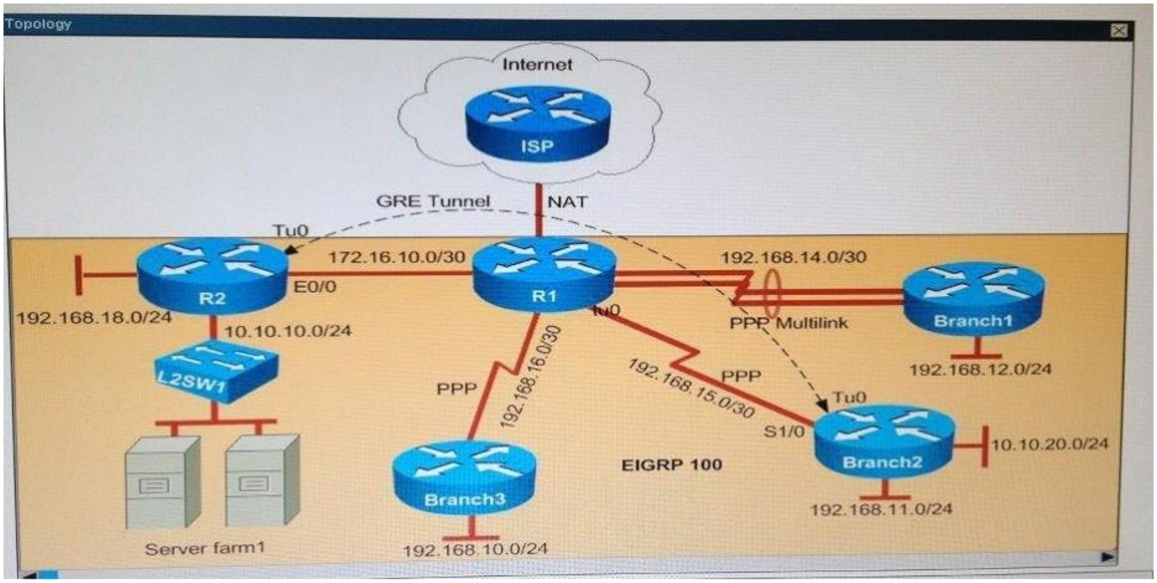
Scenario

You are implementing PPP over serial links between R1 router and branch offices. In Phase 1 you must implement and verify PPP and GRE tunnel configurations as mentioned in the topology. In Phase 2 your colleague is expected to do NAT and ISP configurations between R1 and ISP router.

Identify the issues that you encounter during PPP over serial links implementation.

Routers Branch1, Branch2, and Branch3 connect to Router R1 in the main office over serial links.
PPP multilink implementation is recommended between R1 and Branch1 routers.
The GRE tunnel is configured between R2 and Branch2 routers, and traffic between Server farm1 10.10.10.0/24 network and Branch2 LAN 10.10.20.0/24 network, is routed over GRE tunnel using static route.

You have console access on R1, R2, Branch1, Branch2, and Branch3 devices. Use only show commands to troubleshoot the issues.

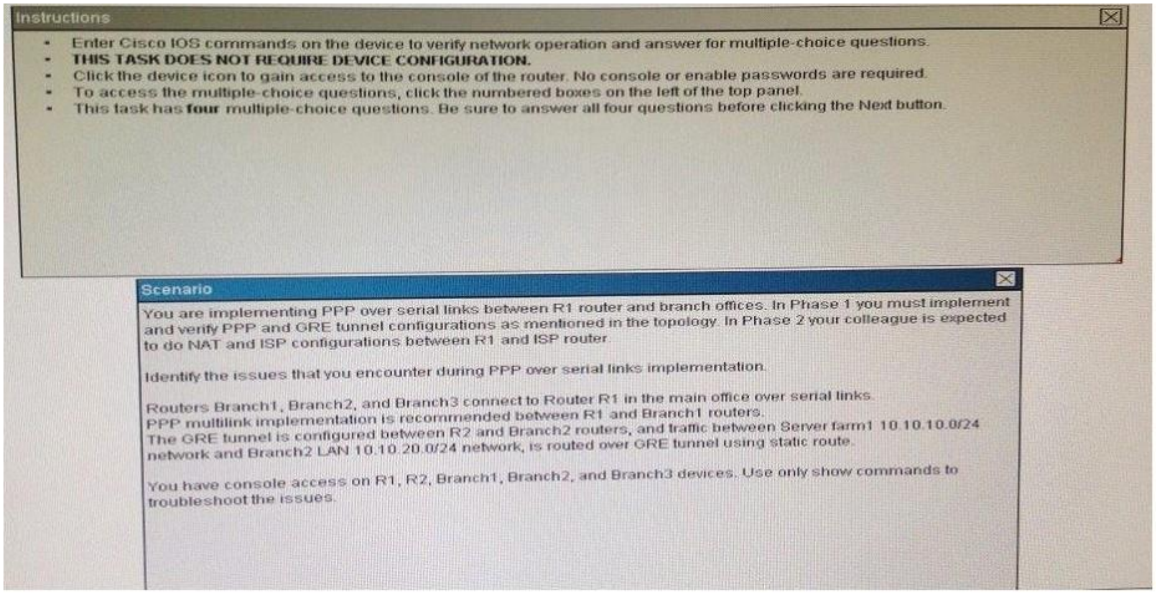


Which statement about the router configurations is correct?

A. PPP PAP is authentication configured between Branch2 and R1.
B. Tunnel keepalives are not configured for the tunnel0 interface on Branch2 and R2.
C. The Branch2 LAN network 192.168.11 0/24 is not advertised into the EIGRP network.
D. The Branch3 LAW network 192.168.10.0/24 is not advertised into the EIGRP network.
E. PPP CHAP is authentication configured between Branch1 and R1.

Answer: D

QUESTION 469
Hotspot Questions


Instructions

- Enter Cisco IOS commands on the device to verify network operation and answer for multiple-choice questions.
- **THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.**
- Click the device icon to gain access to the console of the router. No console or enable passwords are required.
- To access the multiple-choice questions, click the numbered boxes on the left of the top panel.
- This task has **four** multiple-choice questions. Be sure to answer all four questions before clicking the Next button.

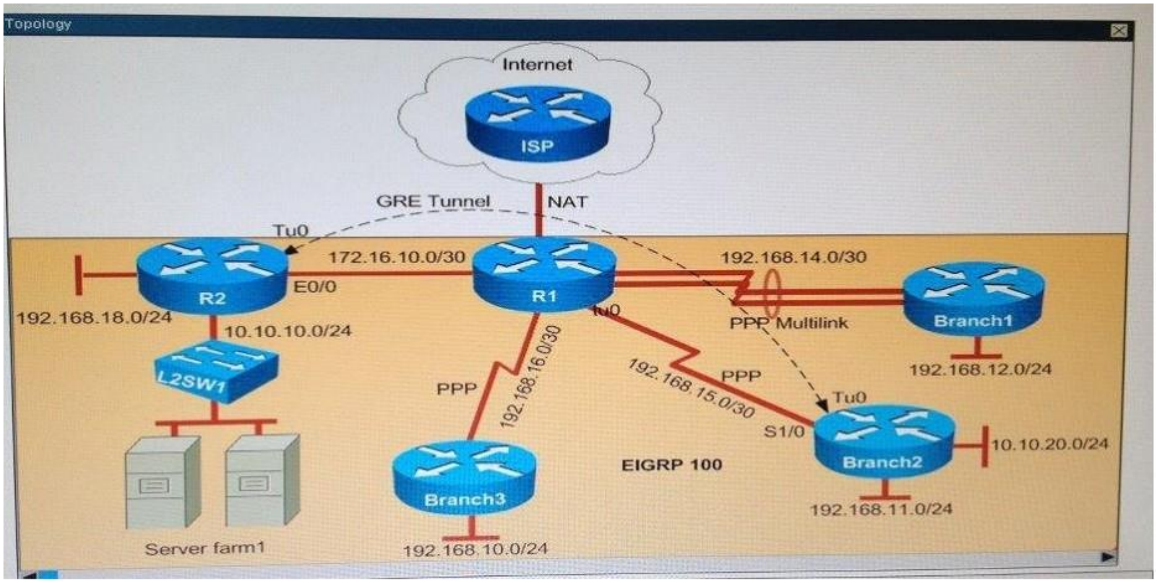
Scenario

You are implementing PPP over serial links between R1 router and branch offices. In Phase 1 you must implement and verify PPP and GRE tunnel configurations as mentioned in the topology. In Phase 2 your colleague is expected to do NAT and ISP configurations between R1 and ISP router.

Identify the issues that you encounter during PPP over serial links implementation.

Routers Branch1, Branch2, and Branch3 connect to Router R1 in the main office over serial links.
PPP multilink implementation is recommended between R1 and Branch1 routers.
The GRE tunnel is configured between R2 and Branch2 routers, and traffic between Server farm1 10.10.10.0/24 network and Branch2 LAN 10.10.20.0/24 network, is routed over GRE tunnel using static route.

You have console access on R1, R2, Branch1, Branch2, and Branch3 devices. Use only show commands to troubleshoot the issues.



Why did Branch1 router lose WAN connectivity with R1 router?

A. The IP address is misconfigured on PPP multilink interface on the Branch1 router.
B. The PPP multilink group is misconfigured on the anch1 serial interfaces.
C. The PPP multilink group is misconfigured on the R1 serial interfaces.
D. The Branch1 serial interfaces are placed in a shutdown condition.

Answer: A

QUESTION 470

While you were troubleshooting a connection issue, a ping from one VLAN to another VLAN on the same switch failed. Which command verifies that IP routing is enabled on interfaces and the local VLANs are up?

A. show ip interface brief
B. show ip nat statistics
C. show ip statistics
D. show ip route

Answer: A

Explanation:

Initiate a ping from an end device in one VLAN to the interface VLAN on another VLAN in order to verify that the switch routes between VLANs. In this example, ping from VLAN 2 (10.1.2.1) to Interface VLAN 3 (10.1.3.1) or Interface VLAN 10 (10.1.10.1). If the ping fails, verify that IP routing is enabled and that the VLAN interfaces status is up with the show ip interface brief command.

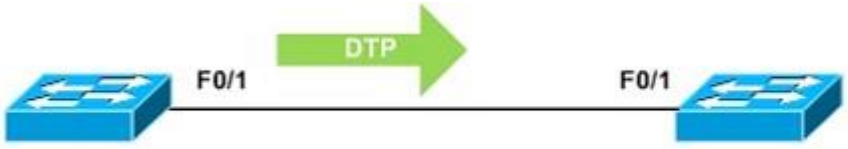
QUESTION 471

Which statement about DTP is true?

A. It uses the native VLAN.
B. It negotiates a trunk link after VTP has been configured.

C. It uses desirable mode by default.
D. It sends data on VLAN 1.

Answer: D
Explanation:
Disabling Dynamic Trunking Protocol (DTP)
Cisco's Dynamic Trunking Protocol can facilitate the automatic creation of trunks between two switches. When two connected ports are configured in dynamic mode, and at least one of the ports is configured as desirable, the two switches will negotiate the formation of a trunk across the link. DTP isn't to be confused with VLAN Trunking Protocol (VTP), although the VTP domain does come into play.



```
interface FastEthernet0/1                  interface FastEthernet0/1
 switchport mode dynamic desirable          switchport mode dynamic auto
```

DTP on the wire is pretty simple, essentially only advertising the VTP domain, the status of the interface, and it's DTP type. These packets are transmitted in the native (or access) VLAN every 60 seconds both natively and with ISL encapsulation (tagged as VLAN 1) when DTP is enabled.

QUESTION 472
Which feature can you use to monitor traffic on a switch by replicating it to another port or ports on the same switch?

A. copy run start
B. traceroute
C. the ICMP Echo IP SLA
D. SPAN

Answer: D
Explanation:
A source port, also called a monitored port, is a switched or routed port that you monitor for network traffic analysis. In a single local SPAN session or RSPAN source session, you can monitor source port traffic, such as received (Rx), transmitted (Tx), or bidirectional (both). The switch supports any number of source ports (up to the maximum number of available ports on the switch) and any number of source VLANs.
A source port has these characteristics:
It can be any port type, such as EtherChannel, Fast Ethernet, Gigabit Ethernet, and so forth.
It can be monitored in multiple SPAN sessions.
It cannot be a destination port.
Each source port can be configured with a direction (ingress, egress, or both) to monitor. For EtherChannel sources, the monitored direction applies to all physical ports in the group.
Source ports can be in the same or different VLANs. For VLAN SPAN sources, all active ports in the source VLAN are included as source ports.

QUESTION 473
Which two circumstances can cause collision domain issues on VLAN domain? (Choose two.)

A. duplex mismatches on Ethernet segments in the same VLAN
B. multiple errors on switchport interfaces
C. congestion on the switch inband path
D. a failing NIC in an end device
E. an overloaded shared segment

Answer: AC
Explanation:
Collision Domains
A collision domain is an area of a single LAN where end stations contend for access to the network because all end stations are connected to a shared physical medium. If two connected devices transmit onto the media at the same time, a collision occurs. When a collision occurs, a JAM signal is sent on the network, indicating that a collision has occurred and that devices should ignore any fragmented data associated with the collision. Both sending devices back off sending their data for a random amount and then try again if the medium is free for transmission. Therefore, collisions effectively delay transmission of data, lowering the effective throughput available to a device. The more devices that are attached to a collision domain, the greater the chances of collisions; this results in lower bandwidth and performance for each device attached to the collision domain. Bridges and switches terminate the physical signal path of a collision domain, allowing you to segment separate collision domains, breaking them up into multiple smaller pieces to provide more bandwidth per user within the new collision domains formed.

QUESTION 474
What is a difference between TACACS+ and RADIUS in AAA?

A. Only TACACS+ allows for separate authentication.
B. Only RADIUS encrypts the entire access-request packet.
C. Only RADIUS uses TCP.
D. Only TACACS+ couples authentication and authorization.

Answer: A
Explanation: Authentication and Authorization
RADIUS combines authentication and authorization. The access-accept packets sent by the RADIUS server to the client contain authorization information. This makes it difficult to decouple authentication and authorization.
TACACS+ uses the AAA architecture, which separates AAA. This allows separate authentication solutions that can still use TACACS+ for authorization and accounting. For example, with TACACS+, it is possible to use Kerberos authentication and TACACS+ authorization and accounting. After a NAS authenticates on a Kerberos server, it requests authorization information from a TACACS+ server without having to re-authenticate. The NAS informs the TACACS+ server that it has successfully authenticated on a Kerberos server, and the server then provides authorization information. During a session, if additional authorization checking is needed, the access server checks with a TACACS+ server to determine if the user is granted permission to use a particular command. This provides greater control over the commands that can be executed on the access server while decoupling from the authentication mechanism.

QUESTION 475
Which version of SNMP first allowed user-based access?

A. SNMPv3 with RBAC
B. SNMPv3
C. SNMPv1

D. SNMPv2

Answer: B

QUESTION 476
Which IEEE standard does PVST+ use to tunnel information?

A. 802.1x
B. 802 1q
C. 802.1w
D. 802.1s

Answer: B

QUESTION 477
Which option describes the purpose of traffic policing?

A. It prioritizes routing protocol traffic.
B. It remarks traffic that is below the CIR
C. It drops traffic that exceeds the CIR.
D. It queues and then transmits traffic that exceeds the CIR.

Answer: C
Explanation:
Traffic policing allows you to control the maximum rate of traffic transmitted or received on an interface. Traffic policing is often configured on interfaces at the edge of a network to limit traffic into or out of the network. In most Traffic Policing configurations, traffic that falls within the rate parameters is transmitted, whereas traffic that exceeds the parameters is dropped or transmitted with a different priority.

QUESTION 478
Which component of the Cisco SDN solution serves as the centralized management system?

A. Cisco OpenDaylight
B. Cisco ACI
C. Cisco APIC
D. Cisco IWAN

Answer: B
Explanation:
Cisco ACI is a comprehensive SDN architecture. This policy-based automation solution supports a business-relevant application policy language, greater scalability through a distributed enforcement system, and greater network visibility. These benefits are achieved through the integration of physical and virtual environments under one policy model for networks, servers, storage, services, and security.

QUESTION 479
What are two drawbacks of implementing a link-state routing protocol? (Choose two.)

A. the sequencing and acknowledgment of link-state packets

B. the high volume of link-state advertisements in a converged network
C. the requirement for a hierarchical IP addressing scheme for optimal functionality
D. the high demand on router resources to run the link-state routing algorithm
E. the large size of the topology table listing all advertised routes in the converged network

Answer: CD

QUESTION 480
Which part of the PPPoE server configuration contains the information used to assign an IP address to a PPPoE client?

A. virtual-template interface
B. DHCP
C. dialer interface
D. AAA authentication

Answer: C
Explanation:
PPPoE is configured as a point to point connection between two Ethernet ports. As a tunneling protocol, PPPoE is used as an effective foundation for the transport of IP packets at the network layer. IP is overlaid over a PPP connection and uses PPP as a virtual dial up connection between points on the network. From the user's perspective, a PPPoE session is initiated by using connection software on the client machine or router. PPPoE session initiation involves the identification of the Media Access Control (MAC) address of the remote device. This process, also known as PPPoE discovery

QUESTION 481
Which process is associated with spanning-tree convergence?

A. determining the path cost
B. electing designated ports
C. learning the sender bridge ID
D. assigning the port ID

Answer: B
Explanation:
Spanning Tree Protocol (STP) convergence (Layer 2 convergence) happens when bridges and switches have transitioned to either the forwarding or blocking state. When layer 2 is converged, Root Switch is elected and Root Ports, Designated Ports and Non-Designated ports in all switches are selected. At Converged condition, the Root Ports and the Designated ports are in forwarding state, and all other ports are in blocking state.

QUESTION 482
Which option is the benefit of implementing an intelligent DNS for a cloud computing solution?

A. It reduces the need for a backup data center.
B. It can redirect user requests to locations that are using fewer network resources.
C. It enables the ISP to maintain DNS records automatically.
D. It eliminates the need for a GSS.

Answer: B

QUESTION 483
Which protocol supports sharing the VLAN configuration between two or more switches?

A. multicast
B. STP
C. VTP
D. split-horizon

Answer: C
Explanation:
"VTP allows a network manager to configure a switch so that it will propagate VLAN configurations to other switches in the network"
VTP minimizes misconfigurations and configuration inconsistencies that can cause problems, such as duplicate VLAN names or incorrect VLAN-type specifications. VTP helps you simplify management of the VLAN database across multiple switches. VTP is a Cisco-proprietary protocol and is available on most of the Cisco switches.

QUESTION 484
How can you disable DTP on a switch port?

A. Configure the switch port as a trunk.
B. Add an interface on the switch to a channel group.
C. Change the operational mode to static access.
D. Change the administrative mode to access.

Answer: A

QUESTION 485
Which two components are used to identify a neighbor in a BGP configuration? (Choose two.)

A. autonomous system number
B. version number
C. router ID
D. subnet mask
E. IP address

Answer: AE
Explanation:
Use the show ip bgp neighbors (registered customers only) command to display information about the TCP and Border Gateway Protocol (BGP) connections and verify if the BGP peer is established. The output of the show ip bgp neighbors command below shows the BGP state as 'Established', which indicates that the BGP peer relationship has been established successfully.

```
R1-AGS# show ip bgp neighbors | include BGP
BGP neighbor is 10.10.10.2, remote AS 400, internal link BGP version 4, remote router ID 2.2.2.2
BGP state = Established, up for 00:04:20
BGP table version 1, neighbor version 1
R1-AGS#
```

The show ip bgp neighbors command has been used above with the modifier | include BGP. This makes the output more readable by filtering the the command output and displaying the relevant

parts only.
In addition, the show ip bgp summary (registered customers only) command can also be used to display the status of all BGP connections, as shown below.
R1-AGS(9)# show ip bgp summary
BGP router identifier 10.1.1.2, local AS number 400 BGP table version is 1, main routing table version 1
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd 10.10.10.2 4 400 3 3 1 0 0 00:00:26 0

QUESTION 486
Which type of interface can negotiate an IP address for a PPPoE client?

A. Ethernet
B. dialer
C. serial
D. Frame Relay

Answer: B

QUESTION 487
What is the default VLAN on an access port?

A. 0
B. 1
C. 10
D. 1024

Answer: B

QUESTION 488
Which statement about QoS default behavior is true?

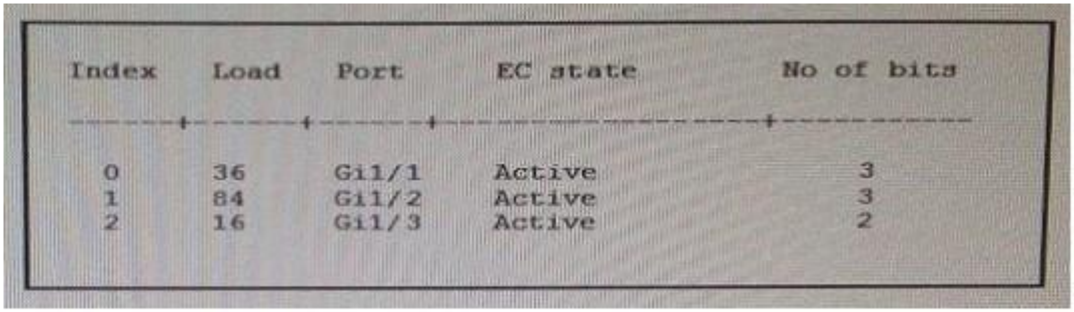
A. Ports are untrusted by default.
B. VoIP traffic is passed without being tagged.
C. Video traffic is passed with a well-known DSCP value of 46.
D. Packets are classified internally with an environment.
E. Packets that arrive with a tag are untagged at the edge of an administrative domain.

Answer: E
Explanation:
Frames received from users in the administratively-defined VLANs are classified or tagged for transmission to other devices. Based on rules that you define, a unique identifier (the tag) is inserted in each frame header before it is forwarded. The tag is examined and understood by each device before any broadcasts or transmissions to other switches, routers, or end stations. When the frame reaches the last switch or router, the tag is removed before the frame is sent to the target end station. VLANs that are assigned on trunk or access ports without identification or a tag are called native or untagged frames. For IEEE 802.1Q frames with tag information, the priority value from the header frame is used. For native frames, the default priority of the input port is used. Each port on the switch has a single receive queue buffer (the ingress port) for incoming traffic. When an untagged frame arrives, it is assigned the value of the port as its port default priority. You assign this value by using the CLI or CMS. A tagged frame continues to use

its assigned CoS value when it passes through the ingress port.

QUESTION 489

Refer to the exhibit. While troubleshooting a switch, you executed the show interface port-channel 1 etherchannel command and it returned this output.
Which information is provided by the Load value?



```
Index   Load   Port    EC state        No of bits
------+------+------+------------------+-----------
  0     36     Gi1/1   Active              3
  1     84     Gi1/2   Active              3
  2     16     Gi1/3   Active              2
```

A. the percentage of use of the link
B. the preference of the link
C. the session count of the link
D. the number source-destination pairs on the link

Answer: D

QUESTION 490

Which spanning-tree feature places a port immediately into a forwarding stated?

A. BPDU guard
B. PortFast
C. loop guard
D. UDLD
E. Uplink Fast

Answer: B

Explanation:

PortFast causes a switch or trunk port to enter the spanning tree forwarding state immediately, bypassing the listening and learning states. You can use PortFast on switch or trunk ports that are connected to a single workstation, switch, or server to allow those devices to connect to the network immediately, instead of waiting for the port to transition from the listening and learning states to the forwarding state.

QUESTION 491

Which protocol authenticates connected devices before allowing them to access the LAN?

A. 802.1d
B. 802.11
C. 802.1w
D. 802.1x

Answer: D

Explanation:
802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN. The term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator. The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols.
The authenticator acts like a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant's identity has been validated and authorized. An analogy to this is providing a valid visa at the airport's arrival immigration before being allowed to enter the country. With 802.1X port-based authentication, the supplicant provides credentials, such as user name/password or digital certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the supplicant (client device) is allowed to access resources located on the protected side of the network.

QUESTION 492
Which identification number is valid for an extended ACL?

A. 1
B. 64
C. 99
D. 100
E. 299
F. 1099

Answer: D

QUESTION 493
Which two pieces of information are provided by the show controllers serial 0 command? (Choose two.)

A. the type of cable that is connected to the interface.
B. The uptime of the interface
C. the status of the physical layer of the interface
D. the full configuration of the interface
E. the interface's duplex settings

Answer: AC
Explanation:
The show controller command provides hardware-related information useful to troubleshoot and diagnose issues with Cisco router interfaces. The Cisco 12000 Series uses a distributed architecture with a central command-line interface (CLI) at the Gigabit Route Processor (GRP) and a local CLI at each line card.

QUESTION 494
Which EIGRP for IPv6 command can you enter to view the link-local addresses of the neighbors of a device?

A. show ipv6 eigrp 20 interfaces

B. show ipv6 route eigrp
C. show ipv6 eigrp neighbors
D. show ip eigrp traffic

Answer: C

QUESTION 495
Which configuration can you apply to enable encapsulation on a subinterface?

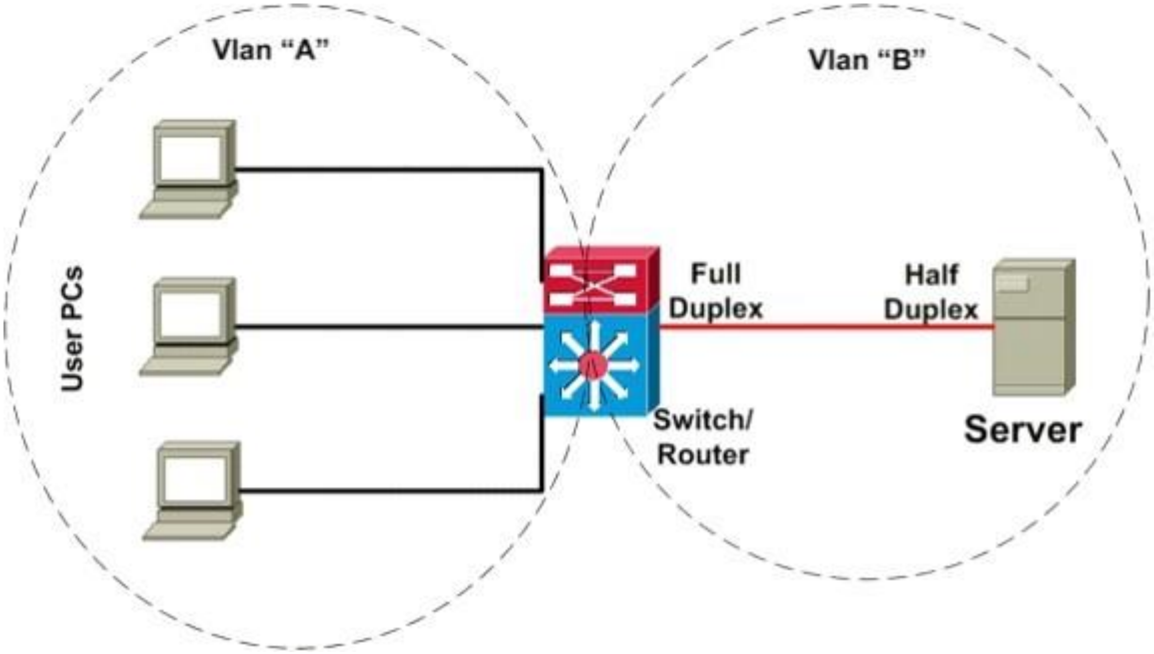
A. interface FastEthernet 0/0
encapsulation dot1Q 30
ip address 10.1.1.30 255.255.255.0
B. interface FastEthernet 0/0.30
ip address 10.1.1.30 255.255.255.0
C. interface FastEthernet 0/0.30
description subinterface vlan 30
D. interface FastEthernet 0/0.30
encapsulation dot1Q 30
ip address 10.1.1.30 255.255.255.0

Answer: D

QUESTION 496
Which statement about slow inter VLAN forwarding is true?

A. The VLAN is experiencing slowness in the point-to-point collisionless connection.
B. The VLANs are experiencing slowness because multiple devices are connected to the same hub.
C. The local VLAN is working normally, but traffic to the alternate VLAN is forwarded slower than expected.
D. The entire VLAN is experiencing slowness.
E. The VLANs are experiencing slowness due to a duplex mismatch.

Answer: E
Explanation:
Common Causes of Slow IntraVLAN and InterVLAN Connectivity The symptoms of slow connectivity on a VLAN can be caused by multiple factors on different network layers. Commonly the network speed issue may be occurring on a lower level, but symptoms can be observed on a higher level as the problem masks itself under the term "slow VLAN". To clarify, this document defines the following new terms: "slow collision domain", "slow broadcast domain" (in other words, slow VLAN), and "slow interVLAN forwarding". These are defined in the section Three Categories of Causes, below.
In the following scenario (illustrated in the network diagram below), there is a Layer 3 (L3) switch performing interVLAN routing between the server and client VLANs. In this failure scenario, one server is connected to a switch, and the port duplex mode is configured half- duplex on the server side and full-duplex on the switch side. This misconfiguration results in a packet loss and slowness, with increased packet loss when higher traffic rates occur on the link where the server is connected. For the clients who communicate with this server, the problem looks like slow interVLAN forwarding because they do not have a problem communicating to other devices or clients on the same VLAN. The problem occurs only when communicating to the server on a different VLAN. Thus, the problem occurred on a single collision domain, but is seen as slow interVLAN forwarding.



Three Categories of Causes

The causes of slowness can be divided into three categories, as follows:

Slow Collision Domain Connectivity

Collision domain is defined as connected devices configured in a half-duplex port configuration, connected to each other or a hub. If a device is connected to a switch port and full-duplex mode is configured, such a point-to-point connection is collisionless. Slowness on such a segment still can occur for different reasons.

Slow Broadcast Domain Connectivity (Slow VLAN)

Slow broadcast domain connectivity occurs when the whole VLAN (that is, all devices on the same VLAN) experiences slowness.

Slow InterVLAN Connectivity (Slow Forwarding Between VLANs) Slow interVLAN connectivity (slow forwarding between VLANs) occurs when there is no slowness on the local VLAN, but traffic needs to be forwarded to an alternate VLAN, and it is not forwarded at the expected rate.

Causes for Network Slowness

Packet Loss

In most cases, a network is considered slow when higher-layer protocols (applications) require extended time to complete an operation that typically runs faster. That slowness is caused by the loss of some packets on the network, which causes higher-level protocols like TCP or applications to time out and initiate retransmission.

Hardware Forwarding Issues

With another type of slowness, caused by network equipment, forwarding (whether Layer 2 [L2] or L3) is performed slowly. This is due to a deviation from normal (designed) operation and switching to slow path forwarding. An example of this is when Multilayer Switching (MLS) on the switch forwards L3 packets between VLANs in the hardware, but due to misconfiguration, MLS is not functioning properly and forwarding is done by the router in the software (which drops the interVLAN forwarding rate significantly).

QUESTION 497

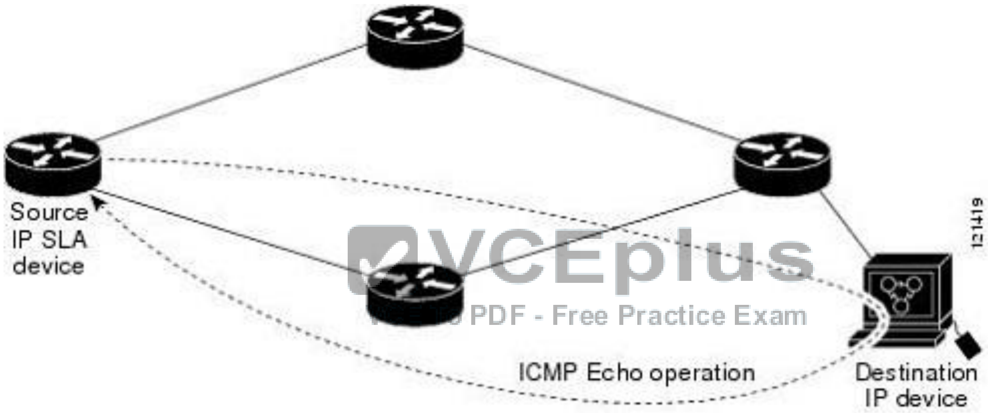
Which statement about the IP SLAs ICMP Echo operation is true?

A. The frequency of the operation .s specified in milliseconds.

B. It is used to identify the best source interface from which to send traffic.

C. It is configured in enable mode.
D. It is used to determine the frequency of ICMP packets.

Answer: D
Explanation:
This module describes how to configure an IP Service Level Agreements (SLAs) Internet Control Message Protocol (ICMP) Echo operation to monitor end-to-end response time between a Cisco router and devices using IPv4 or IPv6. ICMP Echo is useful for troubleshooting network connectivity issues. This module also demonstrates how the results of the ICMP Echo operation can be displayed and analyzed to determine how the network IP connections are performing.
ICMP Echo Operation
The ICMP Echo operation measures end-to-end response time between a Cisco router and any devices using IP. Response time is computed by measuring the time taken between sending an ICMP Echo request message to the destination and receiving an ICMP Echo reply.
In the figure below ping is used by the ICMP Echo operation to measure the response time between the source IP SLAs device and the destination IP device. Many customers use IP SLAs ICMP-based operations, in-house ping testing, or ping-based dedicated probes for response time measurements.



The IP SLAs ICMP Echo operation conforms to the same IETF specifications for ICMP ping testing and the two methods result in the same response times.
Configuring a Basic ICMP Echo Operation on the Source Device SUMMARY STEPS
1. enable
2. configure terminal
3. ip sla operation-number
4. icmp-echo {destination-ip-address | destination-hostname} [source-ip {ip-address | hostname} | source-interface interface-name]
5. frequency seconds 6. end

QUESTION 498
Which option describes how a switch in rapid PVST+ mode responds to a topology change?

A. It immediately deletes dynamic MAC addresses that were learned by all ports on the switch.
B. It sets a timer to delete all MAC addresses that were learned dynamically by ports in the same STP instance.
C. It sets a timer to delete dynamic MAC addresses that were learned by all ports on the switch.
D. It immediately deletes all MAC addresses that were learned dynamically by ports in the same STP instance.

Answer: D

Explanation:

Rapid PVST+This spanning-tree mode is the same as PVST+ except that is uses a rapid convergence based on the IEEE 802.1w standard. To provide rapid convergence, the rapid PVST+ immediately deletes dynamically learned MAC address entries on a per-port basis upon receiving a topology change. By contrast, PVST+ uses a short aging time for dynamically learned MAC address entries.

The rapid PVST+ uses the same configuration as PVST+ (except where noted), and the switch needs only minimal extra configuration. The benefit of rapid PVST+ is that you can migrate a large PVST+ install base to rapid PVST+ without having to learn the complexities of the MSTP configuration and without having to reprovision your network. In rapid-PVST+ mode, each VLAN runs its own spanning-tree instance up to the maximum supported.

QUESTION 499

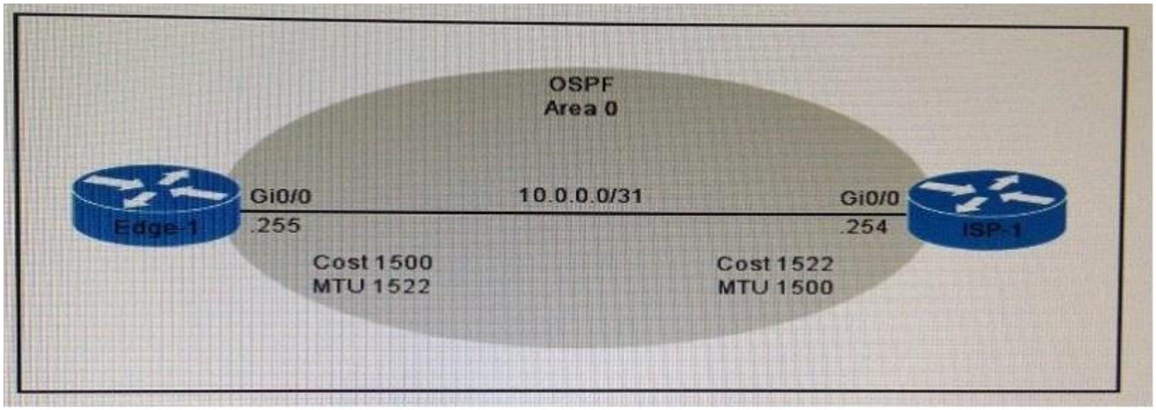
Which type of topology is required by DMVPN?

A. ring
B. full mesh
C. hub-and-spoke
D. partial mesh

Answer: C

QUESTION 500

Refer to the exhibit. Router edge-1 is unable to establish OSPF neighbor adjacency with router ISP-1. Which two configuration changes can you make on edge-1 to allow the two routers to establish adjacency? (Choose two.)



A. Set the subnet mask on edge-1 to 255 255.255.252.
B. Reduce the MTU on edge-1 to 1514.
C. Set the OSPF cost on edge-1 to 1522.
D. Reduce the MTU on edge-1 to 1500.
E. Configure the ip ospf mtu-ignore command on the edge-1 Gi0/0 interface.

Answer: DE

Explanation:

A situation can occur where the interface MTU is at a high value, for example 9000, while the real value of the size of packets that can be forwarded over this interface is 1500.

If there is a mismatch on MTU on both sides of the link where OSPF runs, then the OSPF adjacency will not form because the MTU value is carried in the Database Description (DBD) packets and checked on the other side.

QUESTION 501
Which statement about switch access ports is true?

A. They drop packets with 802.1Q tags.
B. A VLAN must be assigned to an access port before it is created.
C. They can receive traffic from more than one VLAN with no voice support
D. By default, they carry traffic for VLAN 10.

Answer: A
Explanation:
"If an access port receives a packet with an 802.1Q tag in the header other than the access VLAN value, that port drops the packet without learning its MAC source address."

QUESTION 502
Which option is a benefit of switch stacking?

A. It provides redundancy with no impact on resource usage.
B. It simplifies adding and removing hosts.
C. It supports better performance of high-needs applications.
D. It provides higher port density with better resource usage.

Answer: D
Explanation:
A stackable switch is a network switch that is fully functional operating standalone but which can also be set up to operate together with one or more other network switches, with this group of switches showing the characteristics of a single switch but having the port capacity of the sum of the combined switches.

QUESTION 503
What is the first step you perform to configure an SNMPv3 user?

A. Configure server traps.
B. Configure the server group.
C. Configure the server host.
D. Configure the remote engine ID.

Answer: B
Explanation:
The first task in configuring SNMPv3 is to define a view. To simplify things, we'll create a view that allows access to the entire internet subtree:
router(config)#snmp-server view readview internet included This command creates a view called readview. If you want to limit the view to the system tree, for example, replace internet with system. The included keyword states that the specified tree should be included in the view; use excluded if you wanted to exclude a certain subtree.
Next, create a group that uses the new view. The following command creates a group called readonly ; v3 means that SNMPv3 should be used. The auth keyword specifies that the entity should authenticate packets without encrypting them; read readview says that the view named

readview should be used whenever members of the readonly group access the router.
router(config)#snmp-server group readonly v3 auth read readview

QUESTION 504
Which statement about named ACLs is true?

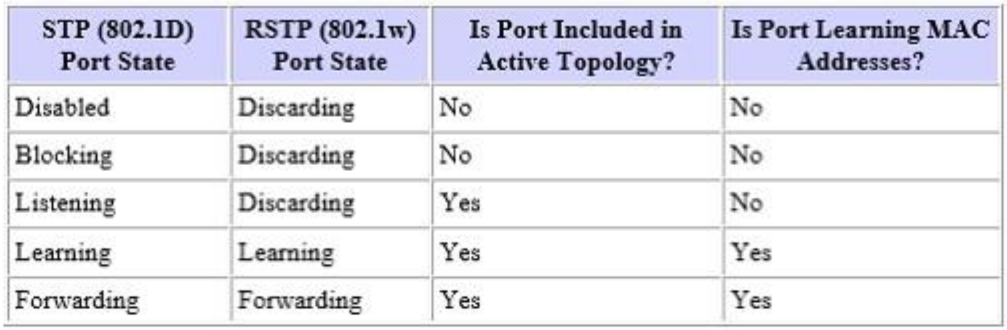
A. They support standard and extended ACLs.
B. They are used to filter usernames and passwords for Telnet and SSH.
C. They are used to filter Layer 7 traffic.
D. They support standard ACLs only.
E. They are used to rate limit traffic destined to targeted networks.

Answer: A
Explanation:
Named Access Control Lists (ACLs) allows standard and extended ACLs to be given names instead of numbers. Unlike in numbered Access Control Lists (ACLs), we can edit Named Access Control Lists. Another benefit of using named access configuration mode is that you can add new statements to the access list, and insert them wherever you like. With the legacy syntax, you must delete the entire access list before reapplying it using the updated rules.

QUESTION 505
Which two switch states are valid for 802.1w? (Choose two.)

A. listening
B. backup
C. disabled
D. learning
E. discarding

Answer: DE
Explanation:
Port States
There are only three port states left in RSTP that correspond to the three possible operational states. The 802.1D disabled, blocking, and listening states are merged into a unique 802.1w discarding state.



STP (802.1D) Port State	RSTP (802.1w) Port State	Is Port Included in Active Topology?	Is Port Learning MAC Addresses?
Disabled	Discarding	No	No
Blocking	Discarding	No	No
Listening	Discarding	Yes	No
Learning	Learning	Yes	Yes
Forwarding	Forwarding	Yes	Yes

QUESTION 506
Which statement about MPLS is true?

A. It operates in Layer 1.
B. It operates between Layer 2 and Layer 3.
C. It operates in Layer 3.
D. it operates in Layer 2.

Answer: B
Explanation:
MPLS belongs to the family of packet-switched networks. MPLS operates at a layer that is generally considered to lie between traditional definitions of OSI Layer 2 (data link layer) and Layer 3 (network layer), and thus is often referred to as a layer 2.5 protocol.

QUESTION 507
Which Cisco platform can verify ACLs?

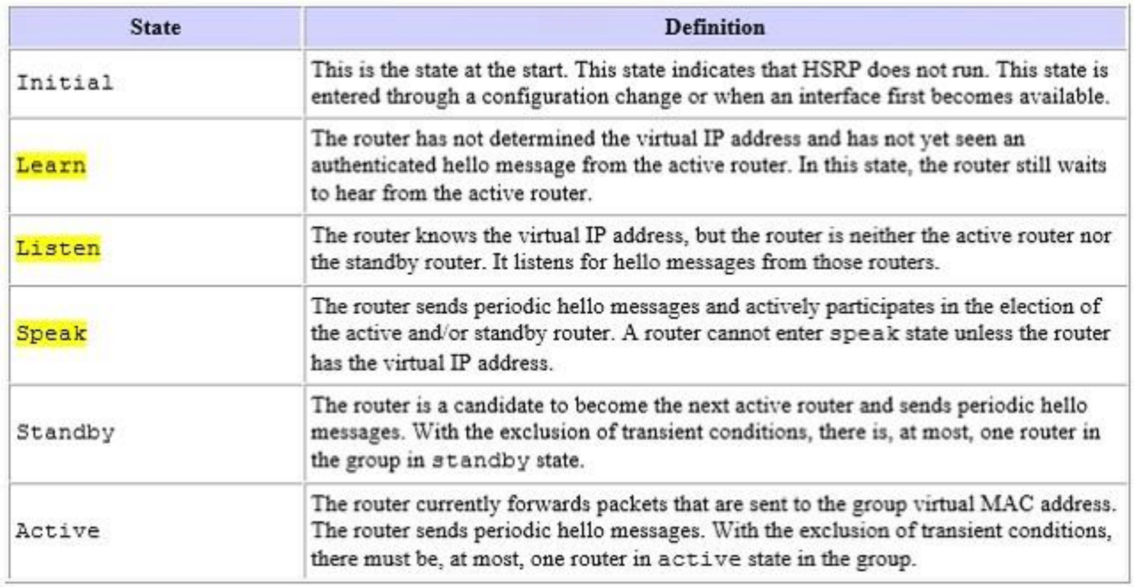
A. Cisco Prime Infrastructure
B. Cisco Wireless LAN Controller
C. Cisco APIC-EM
D. Cisco IOS-XE

Answer: B

QUESTION 508
Which three options are the HSRP states for a router? (Choose three.)

A. initialize
B. learn
C. secondary
D. listen
E. speak
F. primary

Answer: BDE
Explanation:
HSRP States



State	Definition
`Initial`	This is the state at the start. This state indicates that HSRP does not run. This state is entered through a configuration change or when an interface first becomes available.
`Learn`	The router has not determined the virtual IP address and has not yet seen an authenticated hello message from the active router. In this state, the router still waits to hear from the active router.
`Listen`	The router knows the virtual IP address, but the router is neither the active router nor the standby router. It listens for hello messages from those routers.
`Speak`	The router sends periodic hello messages and actively participates in the election of the active and/or standby router. A router cannot enter `speak` state unless the router has the virtual IP address.
`Standby`	The router is a candidate to become the next active router and sends periodic hello messages. With the exclusion of transient conditions, there is, at most, one router in the group in `standby` state.
`Active`	The router currently forwards packets that are sent to the group virtual MAC address. The router sends periodic hello messages. With the exclusion of transient conditions, there must be, at most, one router in `active` state in the group.

QUESTION 509
You enter the show ipv6 route command on an OSPF device and the device displays a route. Which conclusion can you draw about the environment?

A. OSPF is distributing IPv6 routes to BGP.
B. The router is designated as an ABR.
C. The router is designated as totally stubby.
D. OSPFv3 is in use.

Answer: A

QUESTION 510
Which NTP command configures the local device as an NTP reference clock source?

A. ntp peer
B. ntp broadcast
C. ntp master
D. ntp server

Answer: D

QUESTION 511
Which routing protocol has the smallest default administrative distance?

A. IBGP
B. OSPF
C. IS-IS
D. EIGRP
E. RIP

Answer: D

Explanation:

http://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/15986-admin-distance.html

Default Distance Value TableThis table lists the administrative distance default values of the protocols that Cisco supports:

Route Source
Default Distance Values
Connected interface
Static route
Enhanced Interior Gateway Routing Protocol (EIGRP) summary route External Border Gateway Protocol (BGP)
Internal EIGRP
IGRP
OSPF
Intermediate System-to-Intermediate System (IS-IS) Routing Information Protocol (RIP)
Exterior Gateway Protocol (EGP)
On Demand Routing (ODR)
External EIGRP
Internal BGP
Unknown*

QUESTION 512

Which statement about static routes is true?

A. The source interface can be configured to make routing decisions.
B. A subnet mask is entered for the next-hop address.
C. The subnet mask is 255.255 255.0 by default
D. The exit interface can be specified to indicate where the packets will be routed.

Answer: D

Explanation:

Static routing can be used to define an exit point from a router when no other routes are available or necessary. This is called a default route.

QUESTION 513

Under which circumstance should a network administrator implement one-way NAT?

A. when the network must route UDP traffic
B. when traffic that originates outside the network must be routed to internal hosts
C. when traffic that originates inside the network must be routed to internal hosts
D. when the network has few public IP addresses and many private IP addresses require outside access

Answer: B

Explanation:

NAT operation is typically transparent to both the internal and external hosts. Typically the internal host is aware of the true IP address and TCP or UDP port of the external host. Typically the NAT device may function as the default gateway for the internal host. However the external host is only aware of the public IP address for the NAT device and the particular port being used to communicate on behalf of a specific internal host.

NAT and TCP/UDP

"Pure NAT", operating on IP alone, may or may not correctly parse protocols that are totally concerned with IP information, such as ICMP, depending on whether the payload is interpreted by a host on the "inside" or "outside" of translation. As soon as the protocol stack is traversed, even with such basic protocols as TCP and UDP, the protocols will break unless NAT takes action beyond the network layer. IP packets have a checksum in each packet header, which provides error detection only for the header. IP datagrams may become fragmented and it is necessary for a NAT to reassemble these fragments to allow correct recalculation of higher-level checksums and correct tracking of which packets belong to which connection. The major transport layer protocols, TCP and UDP, have a checksum that covers all the data they carry, as well as the TCP/UDP header, plus a "pseudo-header" that contains the source and destination IP addresses of the packet carrying the TCP/UDP header.

For an originating NAT to pass TCP or UDP successfully, it must recompute the TCP/UDP header checksum based on the translated IP addresses, not the original ones, and put that checksum into the TCP/UDP header of the first packet of the fragmented set of packets. The receiving NAT must recompute the IP checksum on every packet it passes to the destination host, and also recognize and recompute the TCP/UDP header using the retranslated addresses and pseudo-header. This is not a completely solved problem. One solution is for the receiving NAT to reassemble the entire segment and then recompute a checksum calculated across all packets.

The originating host may perform Maximum transmission unit (MTU) path discovery to determine the packet size that can be transmitted without fragmentation, and then set the don't fragment (DF) bit in the appropriate packet header field. Of course, this is only a one-way solution, because the responding host can send packets of any size, which may be fragmented before reaching the NAT.

QUESTION 514

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

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

Answer: D

Explanation:

IP Routing Table Entry TypesAn entry in the IP routing table contains the following information in the order presented:

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

Next Hop. The IP address of the next hop.

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

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

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

Remote Network IDs. Routes for network IDs that are not directly attached but are available across other routers. For remote networks, the Next Hop field is the IP address of a local router in between the forwarding node and the remote network. Host Routes. A route to a specific IP address. Host routes allow routing to occur on a per- IP address basis. For host routes, the network ID is the IP address of the specified host and the network mask is 255.255.255.255. Default Route. The default route is designed to be used when a more specific network ID or host route is not found. The default route network ID is 0.0.0.0 with the network mask of 0.0.0.0.

QUESTION 515

When a router makes a routing decision for a packet that is received from one network and destined to another, which portion of the packet does if replace?

A. Layer 2 frame header and trailer
B. Layer 3 IP address
C. Layer 5 session
D. Layer 4 protocol

Answer: A

Explanation:

Router Switching Function (1.2.1.1)A primary function of a router is to forward packets toward their destination. This is accomplished by using a switching function, which is the process used by a router to accept a packet on one interface and forward it out of another interface. A key responsibility of the switching function is to encapsulate packets in the appropriate data link frame type for the outgoing data link.

NOTE:

In this context, the term "switching" literally means moving packets from source to destination and should not be confused with the function of a Layer 2 switch. After the router has determined the exit interface using the path determination function, the router must encapsulate the packet into the data link frame of the outgoing interface. What does a router do with a packet received from one network and destined for another network? The router performs the following three major steps:

Step 1. De-encapsulates the Layer 3 packet by removing the Layer 2 frame header and trailer.

Step 2. Examines the destination IP address of the IP packet to find the best path in the routing table.

Step 3. If the router finds a path to the destination, it encapsulates the Layer 3 packet into a new Layer 2 frame and forwards the frame out the exit interface.

QUESTION 516

On which type of device is every port in the same collision domain?

A. a router
B. a Layer 2 switch
C. a hub

Answer: C

Explanation:

Collision domainA collision domain is, as the name implies, a part of a network where packet collisions can occur. A collision occurs when two devices send a packet at the same time on the shared network segment. The packets collide and both devices must send the packets again, which reduces network efficiency. Collisions are often in a hub environment, because each port on a hub is in the same collision domain. By contrast, each port on a bridge, a switch or a router is in a separate collision domain.

QUESTION 517

Which statement about routing protocols is true?

A. Link-state routing protocols choose a path by the number of hops to the destination.

B. OSPF is a link-state routing protocol.
C. Distance-vector routing protocols use the Shortest Path First algorithm.
D. IS-IS is a distance-vector routing protocol.

Answer: A
Explanation:
Link State Routing Protocols
Link state protocols are also called shortest-path-first protocols. Link state routing protocols have a complete picture of the network topology. Hence they know more about the whole network than any distance vector protocol.
Three separate tables are created on each link state routing enabled router. One table is used to hold details about directly connected neighbors, one is used to hold the topology of the entire internetwork and the last one is used to hold the actual routing table. Link state protocols send information about directly connected links to all the routers in the network. Examples of Link state routing protocols include OSPF - Open Shortest Path First and IS-IS - Intermediate System to Intermediate System. There are also routing protocols that are considered to be hybrid in the sense that they use aspects of both distance vector and link state protocols. EIGRP - Enhanced Interior Gateway Routing Protocol is one of those hybrid routing protocols.

QUESTION 518
Which technology supports the stateless assignment of IPv6 addresses?

A. DNS
B. DHCPv6
C. DHCP
D. autoconfiguration

Answer: B
Explanation:
DHCPv6 Technology Overview
IPv6 Internet Address Assignment Overview
IPv6 has been developed with Internet Address assignment dynamics in mind. Being aware that IPv6 Internet addresses are 128 bits in length and written in hexadecimals makes automation of address-assignment an important aspect within network design. These attributes make it inconvenient for a user to manually assign IPv6 addresses, as the format is not naturally intuitive to the human eye. To facilitate address assignment with little or no human intervention, several methods and technologies have been developed to automate the process of address and configuration parameter assignment to IPv6 hosts. The various IPv6 address assignment methods are as follows:
1. Manual Assignment
An IPv6 address can be statically configured by a human operator. However, manual assignment is quite open to errors and operational overhead due to the 128 bit length and hexadecimal attributes of the addresses, although for router interfaces and static network elements and resources this can be an appropriate solution.
2. Stateless Address Autoconfiguration (RFC2462)
Stateless Address Autoconfiguration (SLAAC) is one of the most convenient methods to assign Internet addresses to IPv6 nodes. This method does not require any human intervention at all from an IPv6 user. If one wants to use IPv6 SLAAC on an IPv6 node, it is important that this IPv6 node is connected to a network with at least one IPv6 router connected. This router is configured by the network administrator and sends out Router Advertisement announcements onto the link. These announcements can allow the on-link connected IPv6 nodes to configure themselves with IPv6 address and routing parameters, as specified in RFC2462, without further human intervention.
3. Stateful DHCPv6

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) has been standardized by the IETF through RFC3315. DHCPv6 enables DHCP servers to pass configuration parameters, such as IPv6 network addresses, to IPv6 nodes. It offers the capability of automatic allocation of reusable network addresses and additional configuration flexibility. This protocol is a stateful counterpart to "IPv6 Stateless Address Autoconfiguration" (RFC 2462), and can be used separately, or in addition to the stateless autoconfiguration to obtain configuration parameters.

4. DHCPv6-PD

DHCPv6 Prefix Delegation (DHCPv6-PD) is an extension to DHCPv6, and is specified in RFC3633. Classical DHCPv6 is typically focused upon parameter assignment from a DHCPv6 server to an IPv6 host running a DHCPv6 protocol stack. A practical example would be the stateful address assignment of "2001:db8::1" from a DHCPv6 server to a DHCPv6 client. DHCPv6-PD however is aimed at assigning complete subnets and other network and interface parameters from a DHCPv6-PD server to a DHCPv6-PD client. This means that instead of a single address assignment, DHCPv6-PD will assign a set of IPv6 "subnets". An example could be the assignment of "2001:db8::/60" from a DHCPv6-PD server to a DHCPv6-PD client. This will allow the DHCPv6-PD client (often a CPE device) to segment the received address IPv6 address space, and assign it dynamically to its IPv6 enabled interfaces.

5. Stateless DHCPv6

Stateless DHCPv6 is a combination of "stateless Address Autoconfiguration" and "Dynamic Host Configuration Protocol for IPv6" and is specified by RFC3736. When using stateless- DHCPv6, a device will use Stateless Address Auto-Configuration (SLAAC) to assign one or more IPv6 addresses to an interface, while it utilizes DHCPv6 to receive "additional parameters" which may not be available through SLAAC. For example, additional parameters could include information such as DNS or NTP server addresses, and are provided in a stateless manner by DHCPv6. Using stateless DHCPv6 means that the DHCPv6 server does not need to keep track of any state of assigned IPv6 addresses, and there is no need for state refreshment as result. On network media supporting a large number of hosts associated to a single DHCPv6 server, this could mean a significant reduction in DHCPv6 messages due to the reduced need for address state refreshments. From Cisco IOS 12.4(15)T onwards the client can also receive timing information, in addition to the "additional parameters" through DHCPv6. This timing information provides an indication to a host when it should refresh its DHCPv6 configuration data. This behavior (RFC4242) is particularly useful in unstable environments where changes are likely to occur.

QUESTION 519

Which feature allows a device to use a switch port that is configured for half-duplex to access the network?

A. CSMA/CD
B. IGMP
C. port security
D. split horizon

Answer: A

Explanation:

Ethernet began as a local area network technology that provided a half-duplex shared channel for stations connected to coaxial cable segments linked with signal repeaters. In this appendix, we take a detailed look at the half-duplex shared-channel mode of operation, and at the CSMA/CD mechanism that makes it work.

In the original half-duplex mode, the CSMA/CD protocol allows a set of stations to compete for access to a shared Ethernet channel in a fair and equitable manner. The protocol's rules determine the behavior of Ethernet stations, including when they are allowed to transmit a frame onto a shared Ethernet channel, and what to do when a collision occurs. Today, virtually all devices are connected to Ethernet switch ports over full-duplex media, such as twisted-pair cables. On this type of connection, assuming that both devices can support the full-duplex mode of operation and that Auto-Negotiation (AN) is enabled, the AN protocol will automatically select the highest-performance mode of operation supported by the devices at each end of the link. That will result in full-duplex mode for the vast majority of Ethernet connections with modern interfaces that support full duplex and AN.

QUESTION 520
Which function enables an administrator to route multiple VLANs on a router?

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

Answer: D

QUESTION 521
Which dynamic routing protocol uses only the hop count to determine the best path to a destination?

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

Answer: C

QUESTION 522
What is one requirement for interfaces to run IPv6?

A. An IPv6 address must be configured on the interface.
B. An IPv4 address must be configured.
C. Stateless autoconfiguration must be enabled after enabling IPv6 on the interface.
D. IPv6 must be enabled with the ipv6 enable command in global configuration mode.

Answer: A
Explanation:
To use IPv6 on your router, you must, at a minimum, enable the protocol and assign IPv6 addresses to your interfaces.

QUESTION 523
Which destination IP address can a host use to send one message to multiple devices across different subnets?

A. 172.20.1.0
B. 127.0.0.1
C. 192.168.0.119
D. 239.255.0.1

Answer: D

Explanation:
Multicast is a networking protocol where one host can send a message to a special multicast IP address and one or more network devices can listen for and receive those messages.
Multicast works by taking advantage of the existing IPv4 networking infrastructure, and it does so in something of a weird fashion. As you read, keep in mind that things are a little confusing because multicast was "shoe-horned" in to an existing technology. For the rest of this article, let's use the multicast IP address of 239.255.0.1. We'll not worry about port numbers yet, but make a mental note that they are used in multicast. We'll discuss that later.

QUESTION 524
Which MTU size can cause a baby giant error?

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

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

QUESTION 525
Which entity assigns IPv6 addresses to end users?

A. ICANN
B. APNIC
C. RIR
D. ISPs

Answer: C

QUESTION 526
Which option is the default switch port port-security violation mode?

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

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

QUESTION 527
Which statement about the inside interface configuration in a NAT deployment is true?

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

Answer: B
Explanation:
This module describes how to configure Network Address Translation (NAT) for IP address conservation and how to configure inside and outside source addresses. This module also provides information about the benefits of configuring NAT for IP address conservation.
NAT enables private IP internetworks that use nonregistered IP addresses to connect to the Internet. NAT operates on a device, usually connecting two networks, and translates the private (not globally unique) addresses in the internal network into legal addresses before packets are forwarded onto another network. NAT can be configured to advertise to the outside world only one address for the entire network. This ability provides additional security by effectively hiding the entire internal network behind that one address. NAT is also used at the enterprise edge to allow internal users access to the Internet and to allow Internet access to internal devices such as mail servers.

QUESTION 528
Which value is indicated by the next hop in a routing table?

A. preference of the route source
B. IP address of the remote router for forwarding the packets
C. how the route was learned
D. exit interface IP address for forwarding the packets

Answer: D
Explanation:
The routing table contains network/next hop associations. These associations tell a router that a particular destination can be optimally reached by sending the packet to a specific router that represents the "next hop" on the way to the final destination. The next hop association can also be the outgoing or exit interface to the final destination.

QUESTION 529
Which option is a valid hostname for a switch?

A. Switch-Cisco
B. Switch-Cisco!
C. SwitchCisco
D. SwitchCisc0

Answer: C

QUESTION 530
Which component of the routing table ranks routing protocols according to their preferences?

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

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

QUESTION 531
Which statement about unicast frame forwarding on a switch is true?

A. The TCAM table stores destination MAC addresses
B. If the destination MAC address is unknown, the frame is flooded to every port that is configured in the same VLAN except on the port that it was received on.
C. The CAM table is used to determine whether traffic is permitted or denied on a switch
D. The source address is used to determine the switch port to which a frame is forwarded

Answer: B

QUESTION 532
Which statement about native VLAN traffic is true?

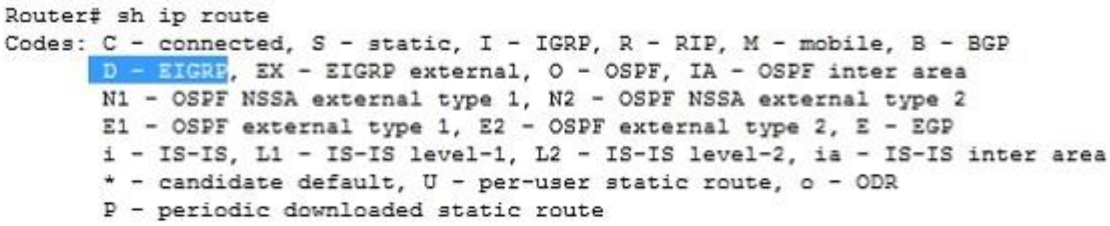
A. Cisco Discovery Protocol traffic travels on the native VLAN by default
B. Traffic on the native VLAN is tagged with 1 by default
C. Control plane traffic is blocked on the native VLAN.
D. The native VLAN is typically disabled for security reasons

Answer: B

QUESTION 533
Which route source code represents the routing protocol with a default administrative distance of 90 in the routing table?

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

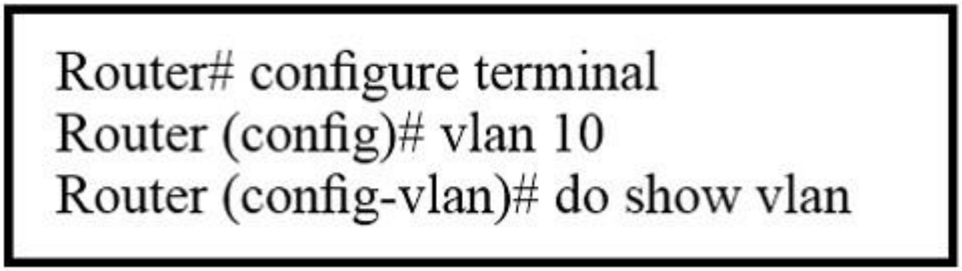
Answer: C
Explanation:
SStatic
EEGP
DEIGRP
RRIP
OOSPF
Default Administrative distance of EIGRP protocol is 90 then answer is C.



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

Default Distance Value TableThis table lists the administrative distance default values of the protocols that Cisco supports:
Route Source
Default Distance Values
Connected interface
Static route
Enhanced Interior Gateway Routing Protocol (EIGRP) summary route External Border Gateway Protocol (BGP)
Internal EIGRP
IGRP
OSPF
Intermediate System-to-Intermediate System (IS-IS) Routing Information Protocol (RIP)
Exterior Gateway Protocol (EGP)
On Demand Routing (ODR)
External EIGRP
Internal BGP
Unknown*

QUESTION 534
Refer to the exhibit. Which statement describes the effect of this configuration?



```
Router# configure terminal
Router (config)# vlan 10
Router (config-vlan)# do show vlan
```

A. The VLAN 10 VTP configuration is displayed.
B. VLAN 10 spanning-tree output is displayed.
C. The VLAN 10 configuration is saved when the router exits VLAN configuration mode.
D. VLAN 10 is added to the VLAN database.

Answer: D

QUESTION 535
When enabled, which feature prevents routing protocols from sending hello messages on an interface'?

A. virtual links

B. passive-interface
C. directed neighbors
D. OSPF areas

Answer: B
Explanation:
You can use the passive-interface command in order to control the advertisement of routing information. The command enables the suppression of routing updates over some interfaces while it allows updates to be exchanged normally over other interfaces. With most routing protocols, the passive-interface command restricts outgoing advertisements only.
But, when used with Enhanced Interior Gateway Routing Protocol (EIGRP), the effect is slightly different. This document demonstrates that use of the passive-interface command in EIGRP suppresses the exchange of hello packets between two routers, which results in the loss of their neighbor relationship. This stops not only routing updates from being advertised, but it also suppresses incoming routing updates. This document also discusses the configuration required in order to allow the suppression of outgoing routing updates, while it also allows incoming routing updates to be learned normally from the neighbor.

QUESTION 536
Which device allows users to connect to the network using a single or double radio?

A. access point
B. switch
C. wireless controller
D. firewall

Answer: A

QUESTION 537
Two hosts are attached to a switch with the default configuration. Which statement about the configuration is true?

A. IP routing must be enabled to allow the two hosts to communicate.
B. The two hosts are in the same broadcast domain.
C. The switch must be configured with a VLAN to allow the two hosts to communicate.
D. Port security prevents the hosts from connecting to the switch.

Answer: A
Explanation:
IP routing must be enables to allow the two hosts to communicate with each other with default configuration.
http://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlan-routing/41860-howto-L3-intervlanrouting.html

QUESTION 538
By default, how many MAC addresses are permitted to be learned on a switch port with port security enabled?

A. 8
B. 2
C. 1

D. 0

Answer: C

QUESTION 539

Which statement about a router on a stick is true?

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

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

QUESTION 540

Which network topology allows all traffic to flow through a central hub?

A. bus
B. star
C. mesh
D. ring

Answer: B

QUESTION 541

Which NAT type is used to translate a single inside address to a single outside address?

A. dynamic NAT
B. NAT overload
C. PAT
D. static NAT

Answer: D
Explanation:
Network address translation (NAT) is the process of modifying IP address information in IP packet headers while in transit across a traffic routing device.
There are two different types of NAT:
NAT
PAT

QUESTION 542

What is the default lease time for a DHCP binding?

A. 24 hours
B. 12 hours

C. 48 hours
D. 36 hours

Answer: A
Explanation:
By default, each IP address assigned by a DHCP Server comes with a one- day lease, which is the amount of time that the address is valid. To change the lease value for an IP address, use the following command in DHCP pool configuration mode:

QUESTION 543
Which RFC was created to alleviate the depletion of IPv4 public addresses?

A. RFC 4193
B. RFC 1519
C. RFC 1518
D. RFC 1918

Answer: C

QUESTION 544
Which method does a connected trunk port use to tag VLAN traffic?

A. IEEE 802 1w
B. IEEE 802 1D
C. IEEE 802 1Q
D. IEEE 802 1p

Answer: C
Explanation:
http://www.cisco.com/c/en/us/support/docs/lan-switching/8021q/17056-741-4.html

QUESTION 545
Configuration of which option is required on a Cisco switch for the Cisco IP phone to work?

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

Answer: B
Explanation:
Configure the Switch Port to Carry Both Voice and Data TrafficWhen you connect an IP phone to a switch using a trunk link, it can cause high CPU utilization in the switches. As all the VLANs for a particular interface are trunked to the phone, it increases the number of STP instances the switch has to manage. This increases the CPU utilization. Trunking also causes unnecessary broadcast / multicast / unknown unicast traffic to hit the phone link. In order to avoid this, remove the trunk configuration and keep the voice and access VLAN configured along with Quality of Service (QoS). Technically, it is still a trunk, but it is called a Multi-VLAN Access Port (MVAP). Because voice and data traffic can travel through the same port, you should specify a different VLAN for each type of traffic. You can configure a switch port to forward voice and data traffic on different VLANs. Configure IP phone ports with a voice VLAN configuration. This configuration

creates a pseudo trunk, but does not require you to manually prune the unnecessary VLANs.
The voice VLAN feature enables access ports to carry IP voice traffic from an IP phone.
The voice VLAN feature is disabled by default. The Port Fast feature is automatically enabled when voice VLAN is configured. When you disable voice VLAN, the Port Fast feature is not automatically disabled.

QUESTION 510
Which NTP command configures the local device as an NTP reference clock source?

A. ntp peer
B. ntp broadcast
C. ntp master
D. ntp server

Answer: D

QUESTION 511
Which routing protocol has the smallest default administrative distance?

A. IBGP
B. OSPF
C. IS-IS
D. EIGRP
E. RIP

Answer: D
Explanation:
http://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/15986-admin-distance.html
Default Distance Value TableThis table lists the administrative distance default values of the protocols that Cisco supports:
Route Source
Default Distance Values
Connected interface
Static route
Enhanced Interior Gateway Routing Protocol (EIGRP) summary route External Border Gateway Protocol (BGP)
Internal EIGRP
IGRP
OSPF
Intermediate System-to-Intermediate System (IS-IS) Routing Information Protocol (RIP)
Exterior Gateway Protocol (EGP)
On Demand Routing (ODR)
External EIGRP
Internal BGP
Unknown*

QUESTION 512
Which statement about static routes is true?

A. The source interface can be configured to make routing decisions.

B. A subnet mask is entered for the next-hop address.
C. The subnet mask is 255.255 255.0 by default
D. The exit interface can be specified to indicate where the packets will be routed.

Answer: D
Explanation:
Static routing can be used to define an exit point from a router when no other routes are available or necessary. This is called a default route.

QUESTION 513
Under which circumstance should a network administrator implement one-way NAT?

A. when the network must route UDP traffic
B. when traffic that originates outside the network must be routed to internal hosts
C. when traffic that originates inside the network must be routed to internal hosts
D. when the network has few public IP addresses and many private IP addresses require outside access

Answer: B
Explanation:
NAT operation is typically transparent to both the internal and external hosts. Typically the internal host is aware of the true IP address and TCP or UDP port of the external host. Typically the NAT device may function as the default gateway for the internal host. However the external host is only aware of the public IP address for the NAT device and the particular port being used to communicate on behalf of a specific internal host.
NAT and TCP/UDP
"Pure NAT", operating on IP alone, may or may not correctly parse protocols that are totally concerned with IP information, such as ICMP, depending on whether the payload is interpreted by a host on the "inside" or "outside" of translation. As soon as the protocol stack is traversed, even with such basic protocols as TCP and UDP, the protocols will break unless NAT takes action beyond the network layer. IP packets have a checksum in each packet header, which provides error detection only for the header. IP datagrams may become fragmented and it is necessary for a NAT to reassemble these fragments to allow correct recalculation of higher-level checksums and correct tracking of which packets belong to which connection. The major transport layer protocols, TCP and UDP, have a checksum that covers all the data they carry, as well as the TCP/UDP header, plus a "pseudo-header" that contains the source and destination IP addresses of the packet carrying the TCP/UDP header.
For an originating NAT to pass TCP or UDP successfully, it must recompute the TCP/UDP header checksum based on the translated IP addresses, not the original ones, and put that checksum into the TCP/UDP header of the first packet of the fragmented set of packets. The receiving NAT must recompute the IP checksum on every packet it passes to the destination host, and also recognize and recompute the TCP/UDP header using the retranslated addresses and pseudo-header. This is not a completely solved problem. One solution is for the receiving NAT to reassemble the entire segment and then recompute a checksum calculated across all packets.
The originating host may perform Maximum transmission unit (MTU) path discovery to determine the packet size that can be transmitted without fragmentation, and then set the don't fragment (DF) bit in the appropriate packet header field. Of course, this is only a one-way solution, because the responding host can send packets of any size, which may be fragmented before reaching the NAT.

QUESTION 514
Which component of a routing table entry represents the subnet mask?

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

Answer: D
Explanation:
IP Routing Table Entry TypesAn entry in the IP routing table contains the following information in the order presented:
Network ID. The network ID or destination corresponding to the route. The network ID can be class-based, subnet, or supernet network ID, or an IP address for a host route. Network Mask. The mask that is used to match a destination IP address to the network ID.
Next Hop. The IP address of the next hop.
Interface. An indication of which network interface is used to forward the IP packet. Metric.
A number used to indicate the cost of the route so the best route among possible multiple routes to the same destination can be selected. A common use of the metric is to indicate the number of hops (routers crossed) to the network ID. Routing table entries can be used to store the following types of routes:
Directly Attached Network IDs. Routes for network IDs that are directly attached. For directly attached networks, the Next Hop field can be blank or contain the IP address of the interface on that network.
Remote Network IDs. Routes for network IDs that are not directly attached but are available across other routers. For remote networks, the Next Hop field is the IP address of a local router in between the forwarding node and the remote network. Host Routes. A route to a specific IP address. Host routes allow routing to occur on a per- IP address basis. For host routes, the network ID is the IP address of the specified host and the network mask is 255.255.255.255.
Default Route. The default route is designed to be used when a more specific network ID or host route is not found. The default route network ID is 0.0.0.0 with the network mask of 0.0.0.0.

QUESTION 515
When a router makes a routing decision for a packet that is received from one network and destined to another, which portion of the packet does if replace?

A. Layer 2 frame header and trailer
B. Layer 3 IP address
C. Layer 5 session
D. Layer 4 protocol

Answer: A
Explanation:
Router Switching Function (1.2.1.1)A primary function of a router is to forward packets toward their destination. This is accomplished by using a switching function, which is the process used by a router to accept a packet on one interface and forward it out of another interface. A key responsibility of the switching function is to encapsulate packets in the appropriate data link frame type for the outgoing data link.
NOTE:
In this context, the term "switching" literally means moving packets from source to destination and should not be confused with the function of a Layer 2 switch. After the router has determined the exit interface using the path determination function, the router must encapsulate the packet into the data link frame of the outgoing interface. What does a router do with a packet received from one network and destined for another network? The router performs the following three major steps:
Step 1. De-encapsulates the Layer 3 packet by removing the Layer 2 frame header and trailer.

Step 2. Examines the destination IP address of the IP packet to find the best path in the routing table.
Step 3. If the router finds a path to the destination, it encapsulates the Layer 3 packet into a new Layer 2 frame and forwards the frame out the exit interface.

QUESTION 516
On which type of device is every port in the same collision domain?

A. a router
B. a Layer 2 switch
C. a hub

Answer: C
Explanation:
Collision domainA collision domain is, as the name implies, a part of a network where packet collisions can occur. A collision occurs when two devices send a packet at the same time on the shared network segment. The packets collide and both devices must send the packets again, which reduces network efficiency. Collisions are often in a hub environment, because each port on a hub is in the same collision domain. By contrast, each port on a bridge, a switch or a router is in a separate collision domain.

QUESTION 517
Which statement about routing protocols is true?

A. Link-state routing protocols choose a path by the number of hops to the destination.
B. OSPF is a link-state routing protocol.
C. Distance-vector routing protocols use the Shortest Path First algorithm.
D. IS-IS is a distance-vector routing protocol.

Answer: A
Explanation:
Link State Routing Protocols
Link state protocols are also called shortest-path-first protocols. Link state routing protocols have a complete picture of the network topology. Hence they know more about the whole network than any distance vector protocol.
Three separate tables are created on each link state routing enabled router. One table is used to hold details about directly connected neighbors, one is used to hold the topology of the entire internetwork and the last one is used to hold the actual routing table. Link state protocols send information about directly connected links to all the routers in the network. Examples of Link state routing protocols include OSPF - Open Shortest Path First and IS-IS - Intermediate System to Intermediate System. There are also routing protocols that are considered to be hybrid in the sense that they use aspects of both distance vector and link state protocols. EIGRP - Enhanced Interior Gateway Routing Protocol is one of those hybrid routing protocols.

QUESTION 518
Which technology supports the stateless assignment of IPv6 addresses?

A. DNS
B. DHCPv6
C. DHCP
D. autoconfiguration

Answer: B
Explanation:
DHCPv6 Technology Overview
IPv6 Internet Address Assignment Overview
IPv6 has been developed with Internet Address assignment dynamics in mind. Being aware that IPv6 Internet addresses are 128 bits in length and written in hexadecimals makes automation of address-assignment an important aspect within network design. These attributes make it inconvenient for a user to manually assign IPv6 addresses, as the format is not naturally intuitive to the human eye. To facilitate address assignment with little or no human intervention, several methods and technologies have been developed to automate the process of address and configuration parameter assignment to IPv6 hosts. The various IPv6 address assignment methods are as follows:
1. Manual Assignment
An IPv6 address can be statically configured by a human operator. However, manual assignment is quite open to errors and operational overhead due to the 128 bit length and hexadecimal attributes of the addresses, although for router interfaces and static network elements and resources this can be an appropriate solution.
2. Stateless Address Autoconfiguration (RFC2462)
Stateless Address Autoconfiguration (SLAAC) is one of the most convenient methods to assign Internet addresses to IPv6 nodes. This method does not require any human intervention at all from an IPv6 user. If one wants to use IPv6 SLAAC on an IPv6 node, it is important that this IPv6 node is connected to a network with at least one IPv6 router connected. This router is configured by the network administrator and sends out Router Advertisement announcements onto the link. These announcements can allow the on-link connected IPv6 nodes to configure themselves with IPv6 address and routing parameters, as specified in RFC2462, without further human intervention.
3. Stateful DHCPv6
The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) has been standardized by the IETF through RFC3315. DHCPv6 enables DHCP servers to pass configuration parameters, such as IPv6 network addresses, to IPv6 nodes. It offers the capability of automatic allocation of reusable network addresses and additional configuration flexibility. This protocol is a stateful counterpart to "IPv6 Stateless Address Autoconfiguration" (RFC 2462), and can be used separately, or in addition to the stateless autoconfiguration to obtain configuration parameters.
4. DHCPv6-PD
DHCPv6 Prefix Delegation (DHCPv6-PD) is an extension to DHCPv6, and is specified in RFC3633. Classical DHCPv6 is typically focused upon parameter assignment from a DHCPv6 server to an IPv6 host running a DHCPv6 protocol stack. A practical example would be the stateful address assignment of "2001:db8::1" from a DHCPv6 server to a DHCPv6 client. DHCPv6-PD however is aimed at assigning complete subnets and other network and interface parameters from a DHCPv6-PD server to a DHCPv6-PD client. This means that instead of a single address assignment, DHCPv6-PD will assign a set of IPv6 "subnets". An example could be the assignment of "2001:db8::/60" from a DHCPv6-PD server to a DHCPv6-PD client. This will allow the DHCPv6-PD client (often a CPE device) to segment the received address IPv6 address space, and assign it dynamically to its IPv6 enabled interfaces.
5. Stateless DHCPv6
Stateless DHCPv6 is a combination of "stateless Address Autoconfiguration" and "Dynamic Host Configuration Protocol for IPv6" and is specified by RFC3736. When using stateless- DHCPv6, a device will use Stateless Address Auto-Configuration (SLAAC) to assign one or more IPv6 addresses to an interface, while it utilizes DHCPv6 to receive "additional parameters" which may not be available through SLAAC. For example, additional parameters could include information such as DNS or NTP server addresses, and are provided in a stateless manner by DHCPv6. Using stateless DHCPv6 means that the DHCPv6 server does not need to keep track of any state of assigned IPv6 addresses, and there is no need for state refreshment as result. On network media supporting a large number of hosts associated to a single DHCPv6 server, this could mean a significant reduction in DHCPv6 messages due to the reduced need for address state

refreshments. From Cisco IOS 12.4(15)T onwards the client can also receive timing information, in addition to the "additional parameters" through DHCPv6. This timing information provides an indication to a host when it should refresh its DHCPv6 configuration data. This behavior (RFC4242) is particularly useful in unstable environments where changes are likely to occur.

QUESTION 519

Which feature allows a device to use a switch port that is configured for half-duplex to access the network?

A. CSMA/CD
B. IGMP
C. port security
D. split horizon

Answer: A

Explanation:

Ethernet began as a local area network technology that provided a half-duplex shared channel for stations connected to coaxial cable segments linked with signal repeaters. In this appendix, we take a detailed look at the half-duplex shared-channel mode of operation, and at the CSMA/CD mechanism that makes it work.

In the original half-duplex mode, the CSMA/CD protocol allows a set of stations to compete for access to a shared Ethernet channel in a fair and equitable manner. The protocol's rules determine the behavior of Ethernet stations, including when they are allowed to transmit a frame onto a shared Ethernet channel, and what to do when a collision occurs. Today, virtually all devices are connected to Ethernet switch ports over full-duplex media, such as twisted-pair cables. On this type of connection, assuming that both devices can support the full-duplex mode of operation and that Auto-Negotiation (AN) is enabled, the AN protocol will automatically select the highest-performance mode of operation supported by the devices at each end of the link. That will result in full-duplex mode for the vast majority of Ethernet connections with modern interfaces that support full duplex and AN.

QUESTION 520

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

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

Answer: D

QUESTION 521

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

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

Answer: C

QUESTION 522
What is one requirement for interfaces to run IPv6?

A. An IPv6 address must be configured on the interface.
B. An IPv4 address must be configured.
C. Stateless autoconfiguration must be enabled after enabling IPv6 on the interface.
D. IPv6 must be enabled with the ipv6 enable command in global configuration mode.

Answer: A
Explanation:
To use IPv6 on your router, you must, at a minimum, enable the protocol and assign IPv6 addresses to your interfaces.

QUESTION 523
Which destination IP address can a host use to send one message to multiple devices across different subnets?

A. 172.20.1.0
B. 127.0.0.1
C. 192.168.0.119
D. 239.255.0.1

Answer: D
Explanation:
Multicast is a networking protocol where one host can send a message to a special multicast IP address and one or more network devices can listen for and receive those messages.
Multicast works by taking advantage of the existing IPv4 networking infrastructure, and it does so in something of a weird fashion. As you read, keep in mind that things are a little confusing because multicast was "shoe-horned" in to an existing technology. For the rest of this article, let's use the multicast IP address of 239.255.0.1. We'll not worry about port numbers yet, but make a mental note that they are used in multicast. We'll discuss that later.

QUESTION 524
Which MTU size can cause a baby giant error?

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

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

QUESTION 525
Which entity assigns IPv6 addresses to end users?

A. ICANN

B. APNIC
C. RIR
D. ISPs

Answer: C

QUESTION 526
Which option is the default switch port port-security violation mode?

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

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

QUESTION 527
Which statement about the inside interface configuration in a NAT deployment is true?

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

Answer: B
Explanation:
This module describes how to configure Network Address Translation (NAT) for IP address conservation and how to configure inside and outside source addresses. This module also provides information about the benefits of configuring NAT for IP address conservation.
NAT enables private IP internetworks that use nonregistered IP addresses to connect to the Internet. NAT operates on a device, usually connecting two networks, and translates the private (not globally unique) addresses in the internal network into legal addresses before packets are forwarded onto another network. NAT can be configured to advertise to the outside world only one address for the entire network. This ability provides additional security by effectively hiding the entire internal network behind that one address. NAT is also used at the enterprise edge to allow internal users access to the Internet and to allow Internet access to internal devices such as mail servers.

QUESTION 528
Which value is indicated by the next hop in a routing table?

A. preference of the route source

B. IP address of the remote router for forwarding the packets
C. how the route was learned
D. exit interface IP address for forwarding the packets

Answer: D
Explanation:
The routing table contains network/next hop associations. These associations tell a router that a particular destination can be optimally reached by sending the packet to a specific router that represents the "next hop" on the way to the final destination. The next hop association can also be the outgoing or exit interface to the final destination.

QUESTION 529
Which option is a valid hostname for a switch?

A. Switch-Cisco
B. Switch-Cisco!
C. SwitchCisco
D. SwitchCisc0

Answer: C

QUESTION 530
Which component of the routing table ranks routing protocols according to their preferences?

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

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

QUESTION 531
Which statement about unicast frame forwarding on a switch is true?

A. The TCAM table stores destination MAC addresses
B. If the destination MAC address is unknown, the frame is flooded to every port that is configured in the same VLAN except on the port that it was received on.
C. The CAM table is used to determine whether traffic is permitted or denied on a switch
D. The source address is used to determine the switch port to which a frame is forwarded

Answer: B

QUESTION 532
Which statement about native VLAN traffic is true?

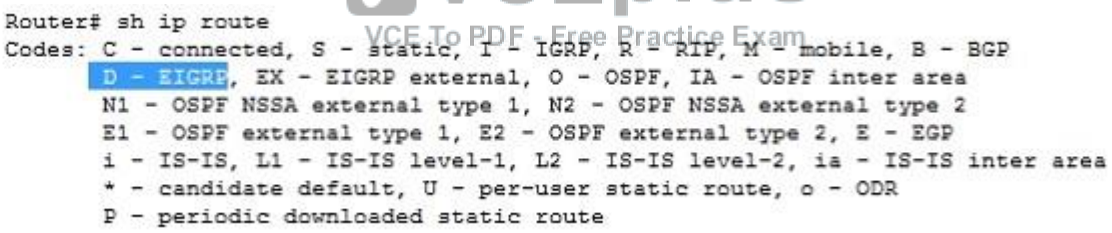
A. Cisco Discovery Protocol traffic travels on the native VLAN by default
B. Traffic on the native VLAN is tagged with 1 by default
C. Control plane traffic is blocked on the native VLAN.
D. The native VLAN is typically disabled for security reasons

Answer: B

QUESTION 533
Which route source code represents the routing protocol with a default administrative distance of 90 in the routing table?

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

Answer: C
Explanation:
SStatic
EEGP
DEIGRP
RRIP
OOSPF
Default Administrative distance of EIGRP protocol is 90 then answer is C.

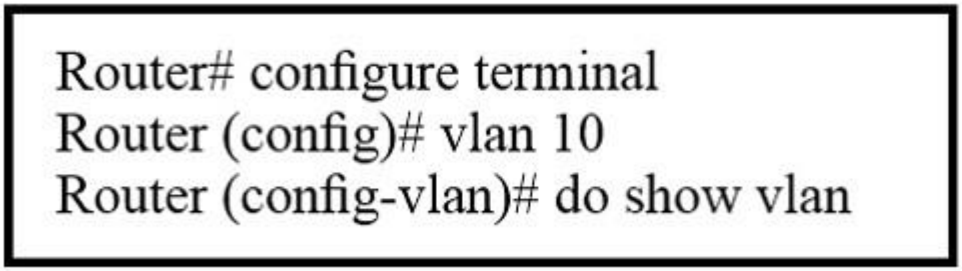


```
Router# sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E -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

Default Distance Value TableThis table lists the administrative distance default values of the protocols that Cisco supports:
Route Source
Default Distance Values
Connected interface
Static route
Enhanced Interior Gateway Routing Protocol (EIGRP) summary route External Border Gateway Protocol (BGP)
Internal EIGRP
IGRP
OSPF
Intermediate System-to-Intermediate System (IS-IS) Routing Information Protocol (RIP)
Exterior Gateway Protocol (EGP)
On Demand Routing (ODR)
External EIGRP
Internal BGP
Unknown*

QUESTION 534

Refer to the exhibit. Which statement describes the effect of this configuration?



```
Router# configure terminal
Router (config)# vlan 10
Router (config-vlan)# do show vlan
```

A. The VLAN 10 VTP configuration is displayed.
B. VLAN 10 spanning-tree output is displayed.
C. The VLAN 10 configuration is saved when the router exits VLAN configuration mode.
D. VLAN 10 is added to the VLAN database.

Answer: D

QUESTION 535

When enabled, which feature prevents routing protocols from sending hello messages on an interface'?

A. virtual links
B. passive-interface
C. directed neighbors
D. OSPF areas

Answer: B
Explanation:

You can use the passive-interface command in order to control the advertisement of routing information. The command enables the suppression of routing updates over some interfaces while it allows updates to be exchanged normally over other interfaces. With most routing protocols, the passive-interface command restricts outgoing advertisements only.
But, when used with Enhanced Interior Gateway Routing Protocol (EIGRP), the effect is slightly different. This document demonstrates that use of the passive-interface command in EIGRP suppresses the exchange of hello packets between two routers, which results in the loss of their neighbor relationship. This stops not only routing updates from being advertised, but it also suppresses incoming routing updates. This document also discusses the configuration required in order to allow the suppression of outgoing routing updates, while it also allows incoming routing updates to be learned normally from the neighbor.

QUESTION 536

Which device allows users to connect to the network using a single or double radio?

A. access point
B. switch
C. wireless controller
D. firewall

Answer: A

QUESTION 537
Two hosts are attached to a switch with the default configuration. Which statement about the configuration is true?

A. IP routing must be enabled to allow the two hosts to communicate.
B. The two hosts are in the same broadcast domain.
C. The switch must be configured with a VLAN to allow the two hosts to communicate.
D. Port security prevents the hosts from connecting to the switch.

Answer: A
Explanation:
IP routing must be enables to allow the two hosts to communicate with each other with default configuration.
http://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlan-routing/41860-howto-L3-intervlanrouting.html

QUESTION 538
By default, how many MAC addresses are permitted to be learned on a switch port with port security enabled?

A. 8
B. 2
C. 1
D. 0

Answer: C

QUESTION 539
Which statement about a router on a stick is true?

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

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

QUESTION 540
Which network topology allows all traffic to flow through a central hub?

A. bus
B. star
C. mesh

D. ring

Answer: B

QUESTION 541

Which NAT type is used to translate a single inside address to a single outside address?

A. dynamic NAT
B. NAT overload
C. PAT
D. static NAT

Answer: D

Explanation:

Network address translation (NAT) is the process of modifying IP address information in IP packet headers while in transit across a traffic routing device.
There are two different types of NAT:
NAT
PAT

QUESTION 542

What is the default lease time for a DHCP binding?

A. 24 hours
B. 12 hours
C. 48 hours
D. 36 hours

Answer: A

Explanation:

By default, each IP address assigned by a DHCP Server comes with a one- day lease, which is the amount of time that the address is valid. To change the lease value for an IP address, use the following command in DHCP pool configuration mode:

QUESTION 543

Which RFC was created to alleviate the depletion of IPv4 public addresses?

A. RFC 4193
B. RFC 1519
C. RFC 1518
D. RFC 1918

Answer: C

QUESTION 544

Which method does a connected trunk port use to tag VLAN traffic?

A. IEEE 802 1w
B. IEEE 802 1D

C. IEEE 802 1Q
D. IEEE 802 1p

Answer: C
Explanation:
http://www.cisco.com/c/en/us/support/docs/lan-switching/8021q/17056-741-4.html

QUESTION 545
Configuration of which option is required on a Cisco switch for the Cisco IP phone to work?

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

Answer: B
Explanation:
Configure the Switch Port to Carry Both Voice and Data TrafficWhen you connect an IP phone to a switch using a trunk link, it can cause high CPU utilization in the switches. As all the VLANs for a particular interface are trunked to the phone, it increases the number of STP instances the switch has to manage. This increases the CPU utilization. Trunking also causes unnecessary broadcast / multicast / unknown unicast traffic to hit the phone link. In order to avoid this, remove the trunk configuration and keep the voice and access VLAN configured along with Quality of Service (QoS). Technically, it is still a trunk, but it is called a Multi-VLAN Access Port (MVAP). Because voice and data traffic can travel through the same port, you should specify a different VLAN for each type of traffic. You can configure a switch port to forward voice and data traffic on different VLANs. Configure IP phone ports with a voice VLAN configuration. This configuration creates a pseudo trunk, but does not require you to manually prune the unnecessary VLANs.
The voice VLAN feature enables access ports to carry IP voice traffic from an IP phone.
The voice VLAN feature is disabled by default. The Port Fast feature is automatically enabled when voice VLAN is configured. When you disable voice VLAN, the Port Fast feature is not automatically disabled.