CCNA 1 – Introduction to Networks (Version 7.00) – ITNv7 Final Exam Answers Full

Number of questions: 60; Passed score: 80-100%

1. Which two traffic types use the Real-Time Transport Protocol (RTP)? (Choose two.)

- **video**
- web
- file transfer
- **voice**
- peer to peer

2. Which wireless technology has low-power and data rate requirements making it popular in home automation applications?

- **ZigBee**
- LoRaWAN
- 5G
- Wi-Fi

Explanation: ZigBee is an IEEE 802.15.4 wireless standard designed for creating personal-area networks. Low energy, power, and data rate requirements make Zigbee a popular protocol for connecting home automation devices.

3. Which layer of the TCP/IP model provides a route to forward messages through an internetwork?

- application
- network access
- **internet**
- transport

Explain:
The OSI model network layer corresponds directly to the internet layer of the TCP/IP model and is used to describe protocols that address and route messages through an internetwork.

4. Which type of server relies on record types such as A, NS, AAAA, and MX in order to provide services?

- **DNS**
- email
- file
- web

Explain:
A DNS server stores records that are used to resolve IP addresses to host names. Some DNS record types include the following:

A – an end device IPv4 address
NS – an authoritative name server
AAAA – an end device IPv6 address
MX – a mail exchange record

5. What are proprietary protocols?

- protocols developed by private organizations to operate on any vendor hardware
- protocols that can be freely used by any organization or vendor
- **protocols developed by organizations who have control over their definition and operation**
- a collection of protocols known as the TCP/IP protocol suite

Explain:
Proprietary protocols have their definition and operation controlled by one company or vendor. Some of them can be used by different organizations with permission from the owner. The TCP/IP protocol suite is an open standard, not a proprietary protocol.

6. What service is provided by DNS?

- **Resolves domain names, such as cisco.com, into IP addresses.**
- A basic set of rules for exchanging text, graphic images, sound, video, and other multimedia files on the web.
- Allows for data transfers between a client and a file server.
- Uses encryption to secure the exchange of text, graphic images, sound, and video on the web.

7. A client packet is received by a server. The packet has a destination port number of 110. What service is the client requesting?

- DNS
- DHCP
- SMTP
- **POP3**

8. What command can be used on a Windows PC to see the IP configuration of that computer?

- show ip interface brief
- ping
- show interfaces
- **ipconfig**

9. A wired laser printer is attached to a home computer. That printer has been shared so that other computers on the home network can also use the printer. What networking model is in use?

- client-based
- master-slave
- point-to-point
- **peer-to-peer (P2P)**

Explanation: Peer-to-peer (P2P) networks have two or more network devices that can share resources such as printers or files without having a dedicated server.

10. What characteristic describes a virus?

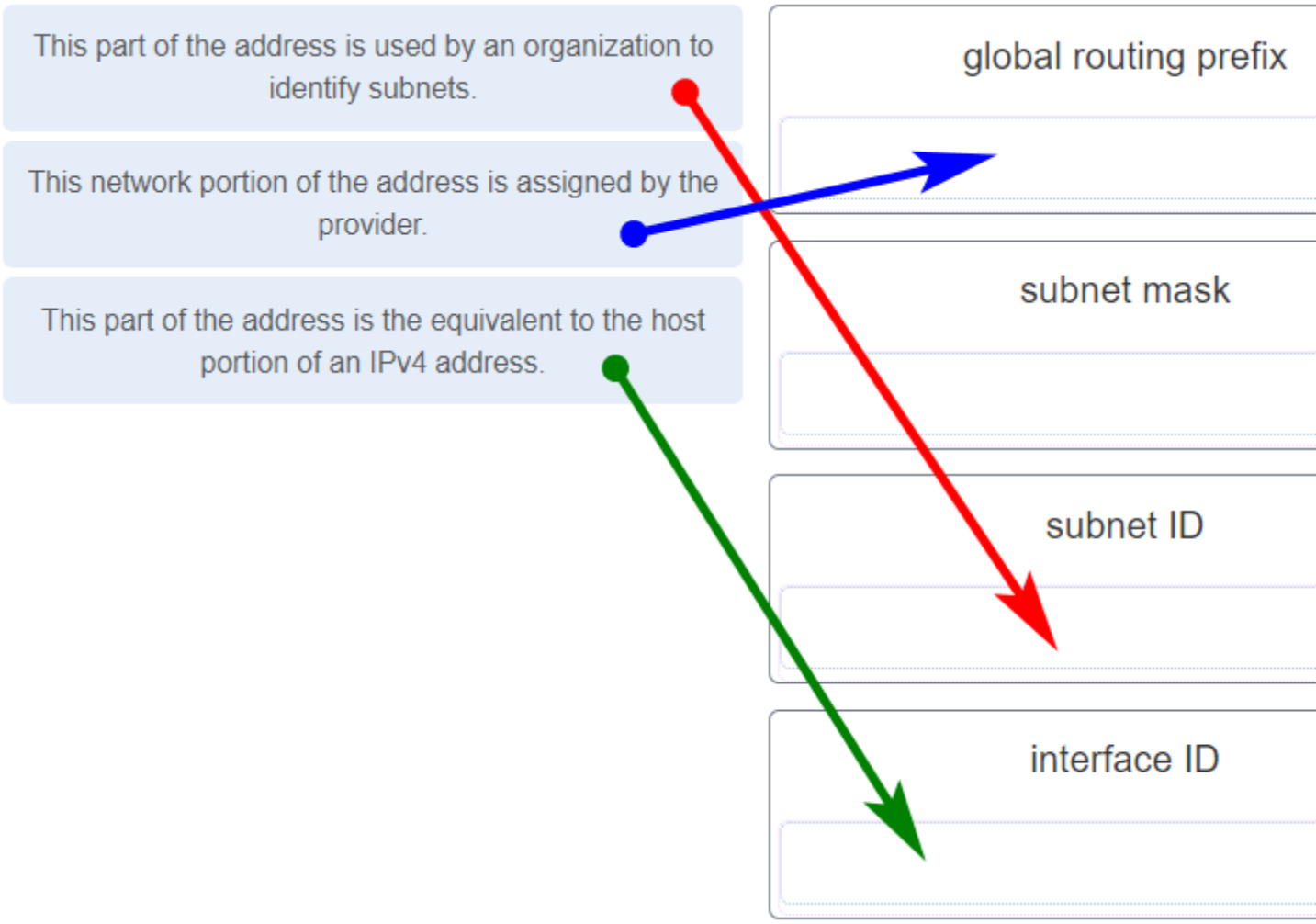
- a network device that filters access and traffic coming into a network
- the use of stolen credentials to access private data
- an attack that slows or crashes a device or network service
- **malicious software or code running on an end device**

11. Three bank employees are using the corporate network. The first employee uses a web browser to view a company web page in order to read some announcements. The second employee accesses the corporate database to perform some financial transactions. The third employee participates in an important live audio conference with other corporate managers in branch offices. If QoS is implemented on this network, what will be the priorities from highest to lowest of the different data types?

- financial transactions, web page, audio conference
- **audio conference, financial transactions, web page**
- financial transactions, audio conference, web page
- audio conference, web page, financial transactions

Explanation: QoS mechanisms enable the establishment of queue management strategies that enforce priorities for different categories of application data. Thus, this queuing enables voice data to have priority over transaction data, which has priority over web data.

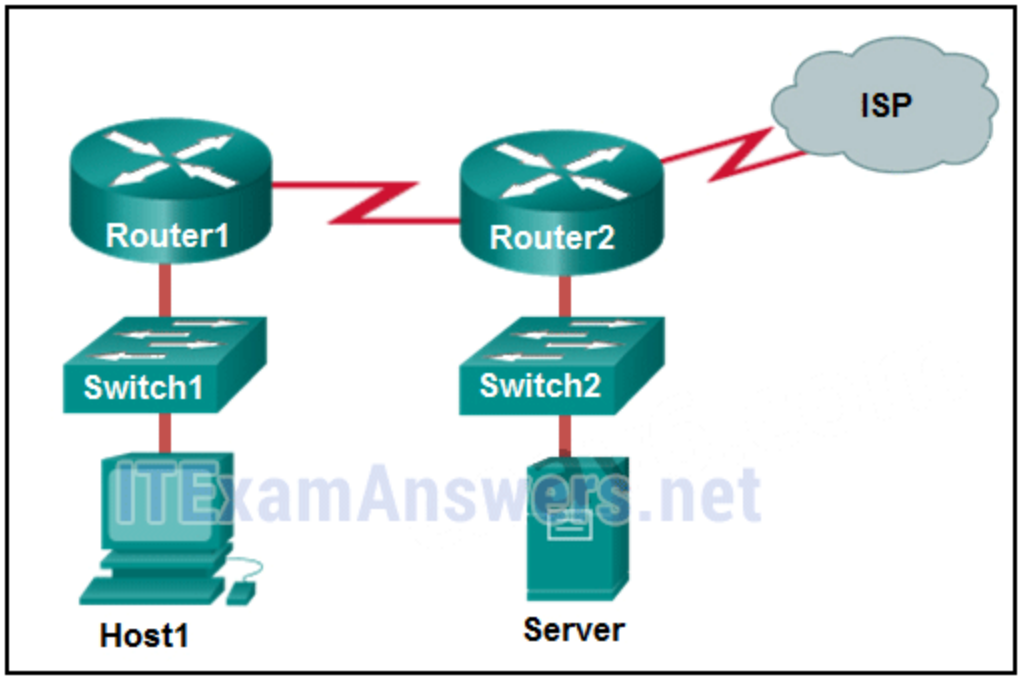
12. Match the description to the IPv6 addressing component. (Not all options are used.)



Place the options in the following order:

This network portion of the address is assigned by the provider.	global routing
This part of the address is used by an organization to identify subnets.	subnet ID
This part of the address is the equivalent to the host portion of an IPv4 address.	interface ID

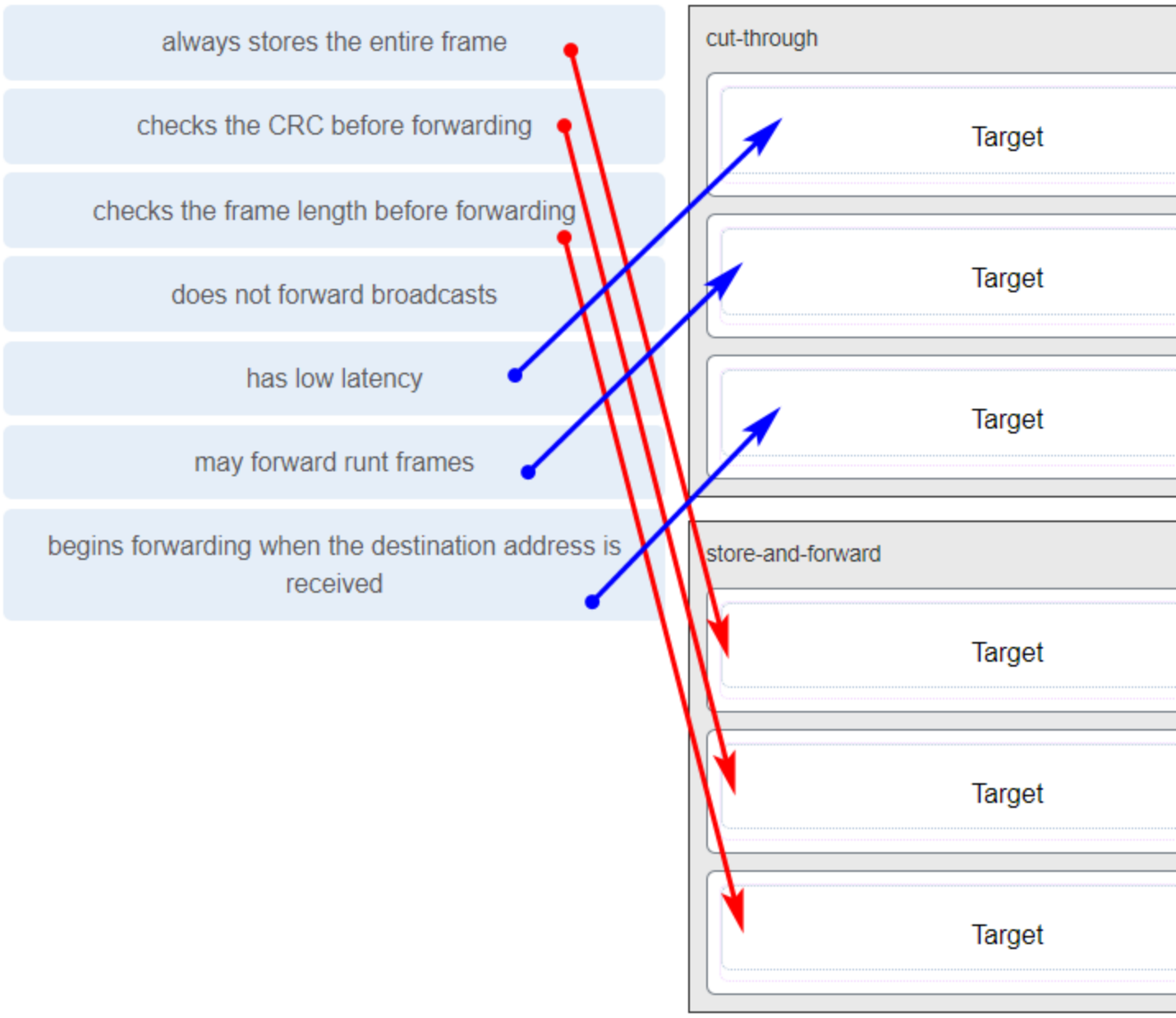
13. Refer to the exhibit. If Host1 were to transfer a file to the server, what layers of the TCP/IP model would be used?



- only application and Internet layers
- only Internet and network access layers
- only application, Internet, and network access layers
- **application, transport, Internet, and network access layers**
- only application, transport, network, data link, and physical layers
- application, session, transport, network, data link, and physical layers

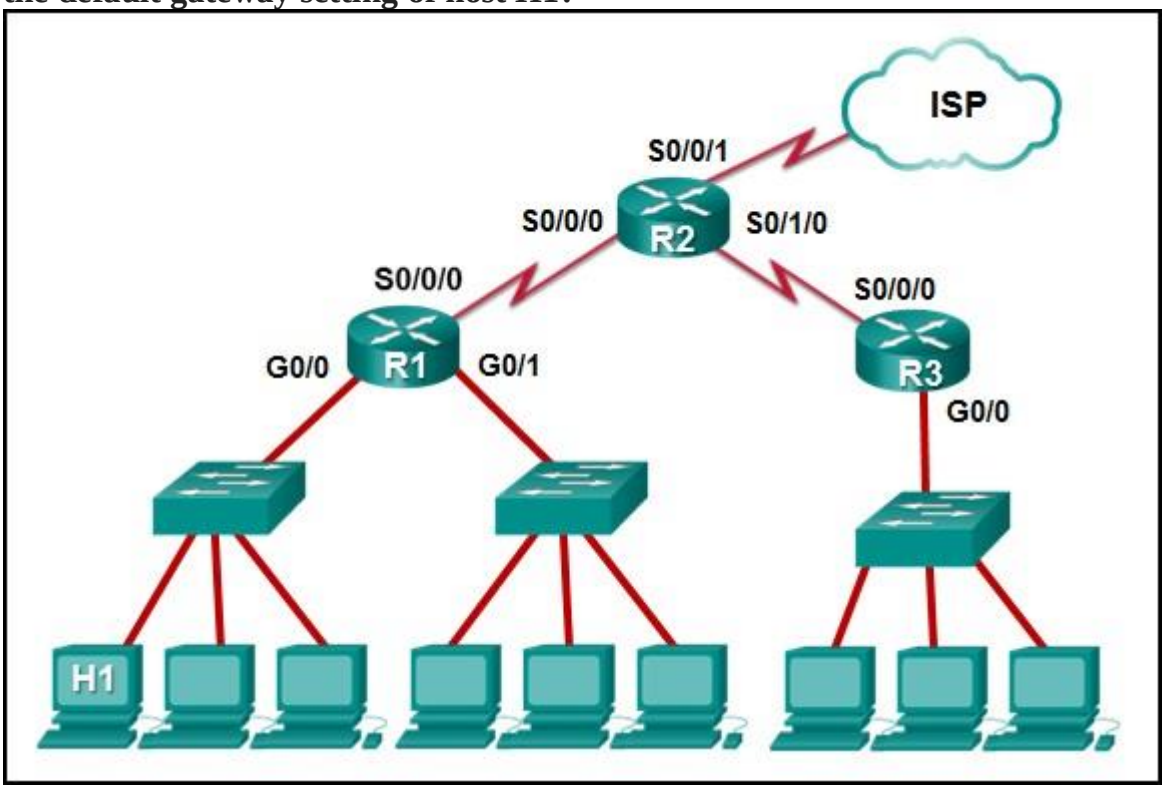
Explanation: The TCP/IP model contains the application, transport, internet, and network access layers. A file transfer uses the FTP application layer protocol. The data would move from the application layer through all of the layers of the model and across the network to the file server.

14. Match the characteristic to the forwarding method. (Not all options are used.)



Explanation: A store-and-forward switch always stores the entire frame before forwarding, and checks its CRC and frame length. A cut-through switch can forward frames before receiving the destination address field, thus presenting less latency than a store-and-forward switch. Because the frame can begin to be forwarded before it is completely received, the switch may transmit a corrupt or runt frame. All forwarding methods require a Layer 2 switch to forward broadcast frames.

15. Refer to the exhibit. The IP address of which device interface should be used as the default gateway setting of host H1?



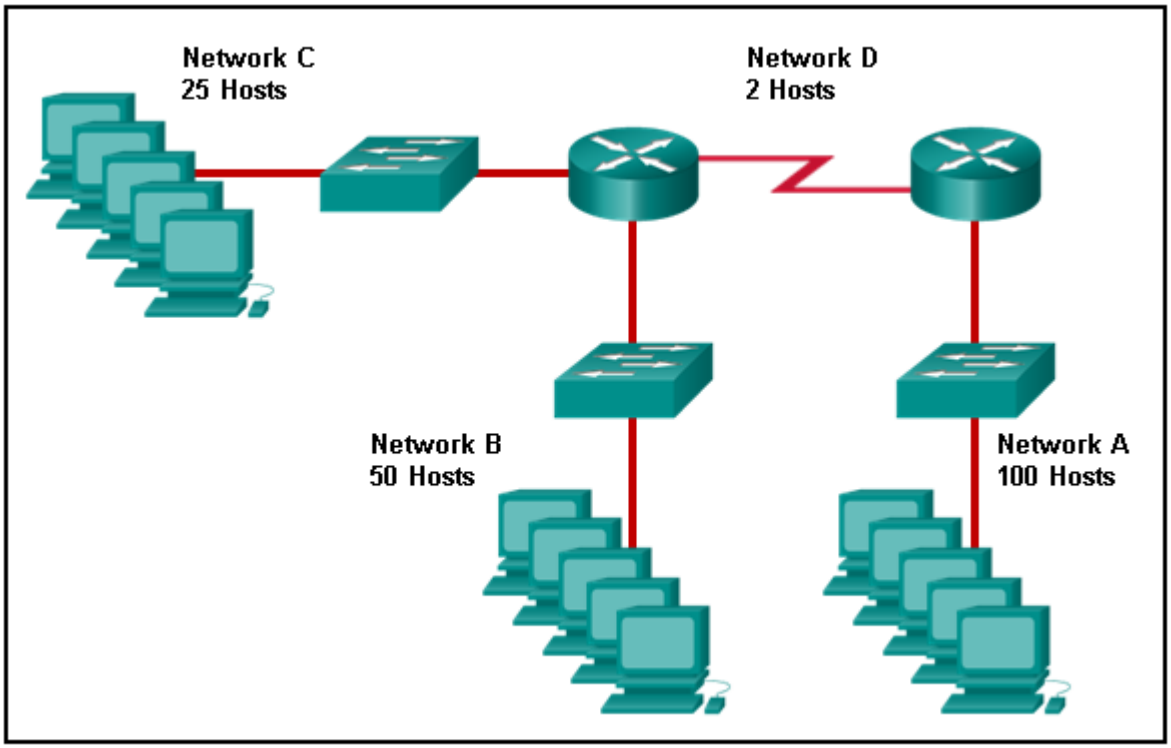
- R1: S0/0/0
- R2: S0/0/1
- **R1: G0/0**
- R2: S0/0/0

Explanation: The default gateway for host H1 is the router interface that is attached to the LAN that H1 is a member of. In this case, that is the G0/0 interface of R1. H1 should be configured with the IP address of that interface in its addressing settings. R1 will provide routing services to packets from H1 that need to be forwarded to remote networks.

16. What service is provided by Internet Messenger?

- **An application that allows real-time chatting among remote users.**
- Allows remote access to network devices and servers.
- Resolves domain names, such as cisco.com, into IP addresses.
- Uses encryption to provide secure remote access to network devices and servers.

17. Refer to the exhibit. Match the network with the correct IP address and prefix that will satisfy the usable host addressing requirements for each network.


Network C
25 Hosts
Network D
2 Hosts
Network B
50 Hosts
Network A
100 Hosts

Network A

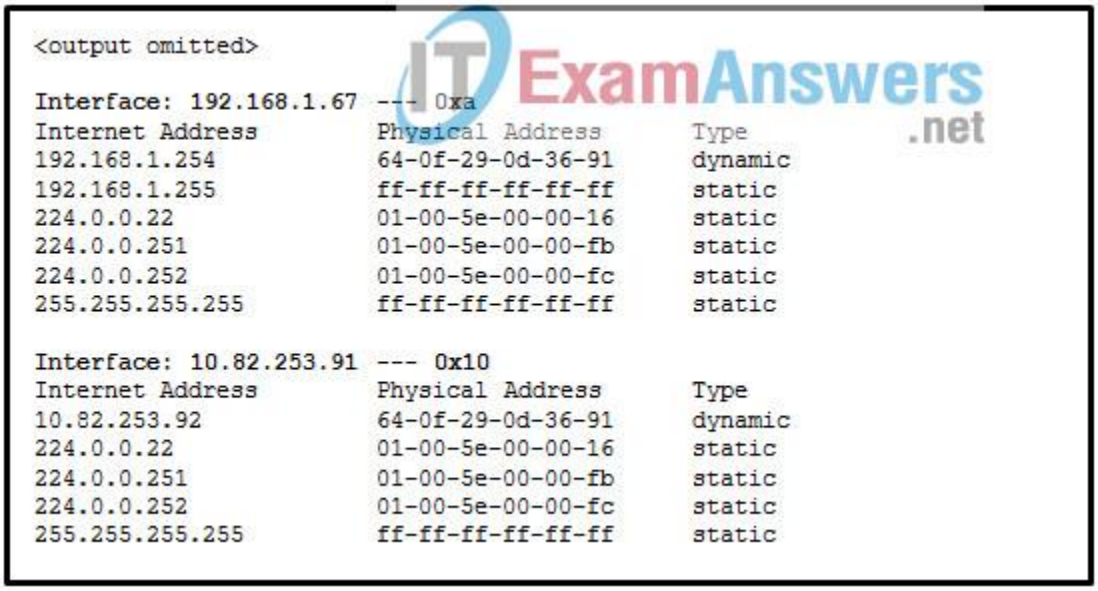
Network B

Network C

Network D

Explanation: Network A needs to use 192.168.0.128 /25, which yields 128 host addresses.
Network B needs to use 192.168.0.0 /26, which yields 64 host addresses.
Network C needs to use 192.168.0.96 /27, which yields 32 host addresses.
Network D needs to use 192.168.0.80/30, which yields 4 host addresses.

18. Refer to the exhibit. Which protocol was responsible for building the table that is shown?



```
<output omitted>

Interface: 192.168.1.67 --- 0xa
Internet Address      Physical Address      Type
192.168.1.254         64-0f-29-0d-36-91     dynamic
192.168.1.255         ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251           01-00-5e-00-00-fb     static
224.0.0.252           01-00-5e-00-00-fc     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 10.82.253.91 --- 0x10
Internet Address      Physical Address      Type
10.82.253.92          64-0f-29-0d-36-91     dynamic
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251           01-00-5e-00-00-fb     static
224.0.0.252           01-00-5e-00-00-fc     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static
```


- DHCP
- **ARP**
- DNS
- ICMP

Explanation: The table that is shown corresponds to the output of the arp -a command, a command that is used on a Windows PC to display the ARP table.

19. A network administrator notices that some newly installed Ethernet cabling is carrying corrupt and distorted data signals. The new cabling was installed in the ceiling close to fluorescent lights and electrical equipment. Which two factors may interfere with the copper cabling and result in signal distortion and data corruption? (Choose two.)

- crosstalk
- extended length of cabling
- **RFI**
- **EMI**
- signal attenuation

20. A host is trying to send a packet to a device on a remote LAN segment, but there are currently no mappings in its ARP cache. How will the device obtain a destination MAC address?

(A host is trying to send a packet to a device on a remote LAN segment, but

there are currently no mappings in the ARP cache. How will the device obtain a destination MAC address?)

- It will send the frame and use its own MAC address as the destination.
- It will send an ARP request for the MAC address of the destination device.
- It will send the frame with a broadcast MAC address.
- It will send a request to the DNS server for the destination MAC address.
- **It will send an ARP request for the MAC address of the default gateway.**

22. A client packet is received by a server. The packet has a destination port number of 53. What service is the client requesting?

- **DNS**
- NetBIOS (NetBT)
- POP3
- IMAP

23. A network administrator is adding a new LAN to a branch office. The new LAN must support 25 connected devices. What is the smallest network mask that the network administrator can use for the new network?

- 255.255.255.128
- 255.255.255.192
- **255.255.255.224**
- 255.255.255.240

24. What characteristic describes a Trojan horse?

- **malicious software or code running on an end device**
- an attack that slows or crashes a device or network service
- the use of stolen credentials to access private data
- a network device that filters access and traffic coming into a network

25. What service is provided by HTTPS?

- Uses encryption to provide secure remote access to network devices and servers.
- Resolves domain names, such as cisco.com, into IP addresses.
- **Uses encryption to secure the exchange of text, graphic images, sound, and video on the web.**
- Allows remote access to network devices and servers.

26. A technician with a PC is using multiple applications while connected to the Internet. How is the PC able to keep track of the data flow between multiple application sessions and have each application receive the correct packet flows?

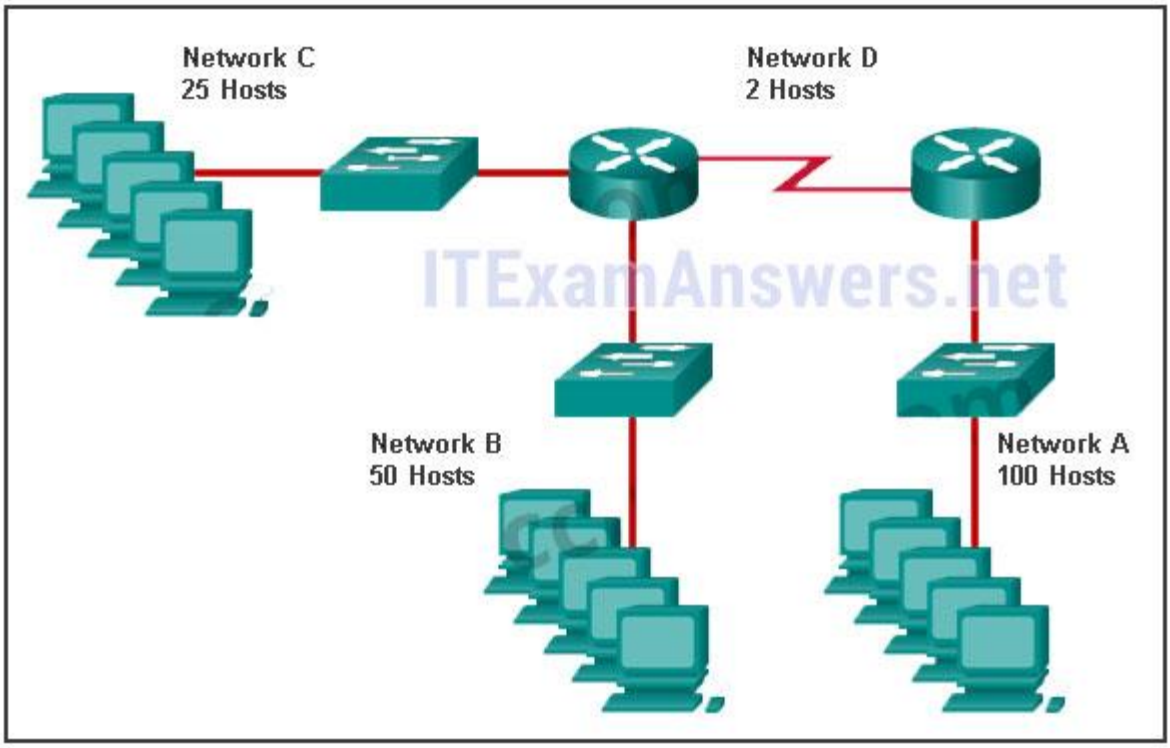
- The data flow is being tracked based on the destination MAC address of the technician PC.
- **The data flow is being tracked based on the source port number that is used by each application.**
- The data flow is being tracked based on the source IP address that is used by the PC of the technician.
- The data flow is being tracked based on the destination IP address that is used by the PC of the technician.

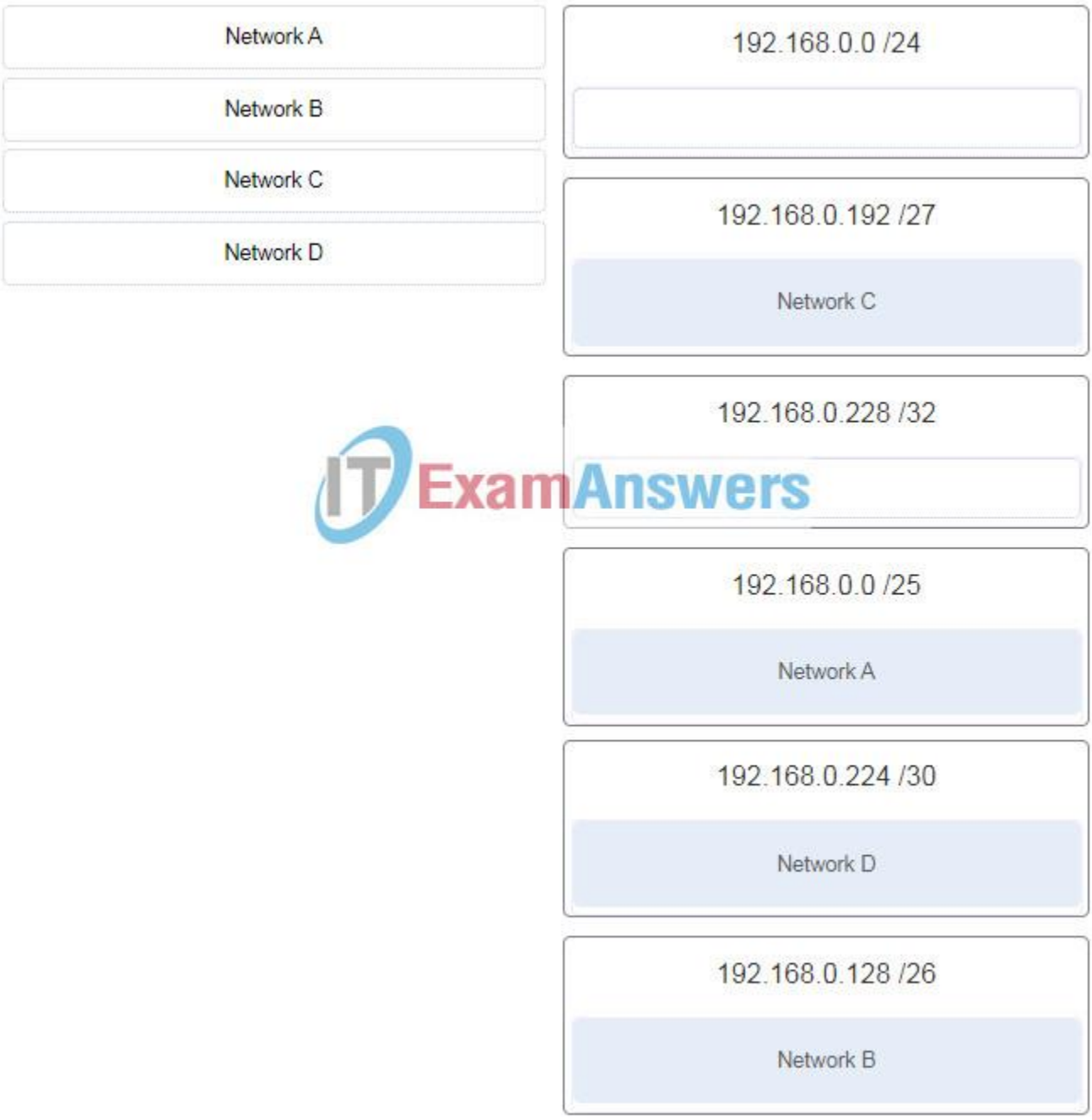
Explanation:
The source port number of an application is randomly generated and used to individually keep track of each session connecting out to the Internet. Each application will use a unique source port number to provide simultaneous communication from multiple applications through the Internet.

27. A network administrator is adding a new LAN to a branch office. The new LAN must support 61 connected devices. What is the smallest network mask that the network administrator can use for the new network?

- 255.255.255.240
- 255.255.255.224
- **255.255.255.192**
- 255.255.255.128

28. Refer to the exhibit. Match the network with the correct IP address and prefix that will satisfy the usable host addressing requirements for each network. (Not all options are used.)





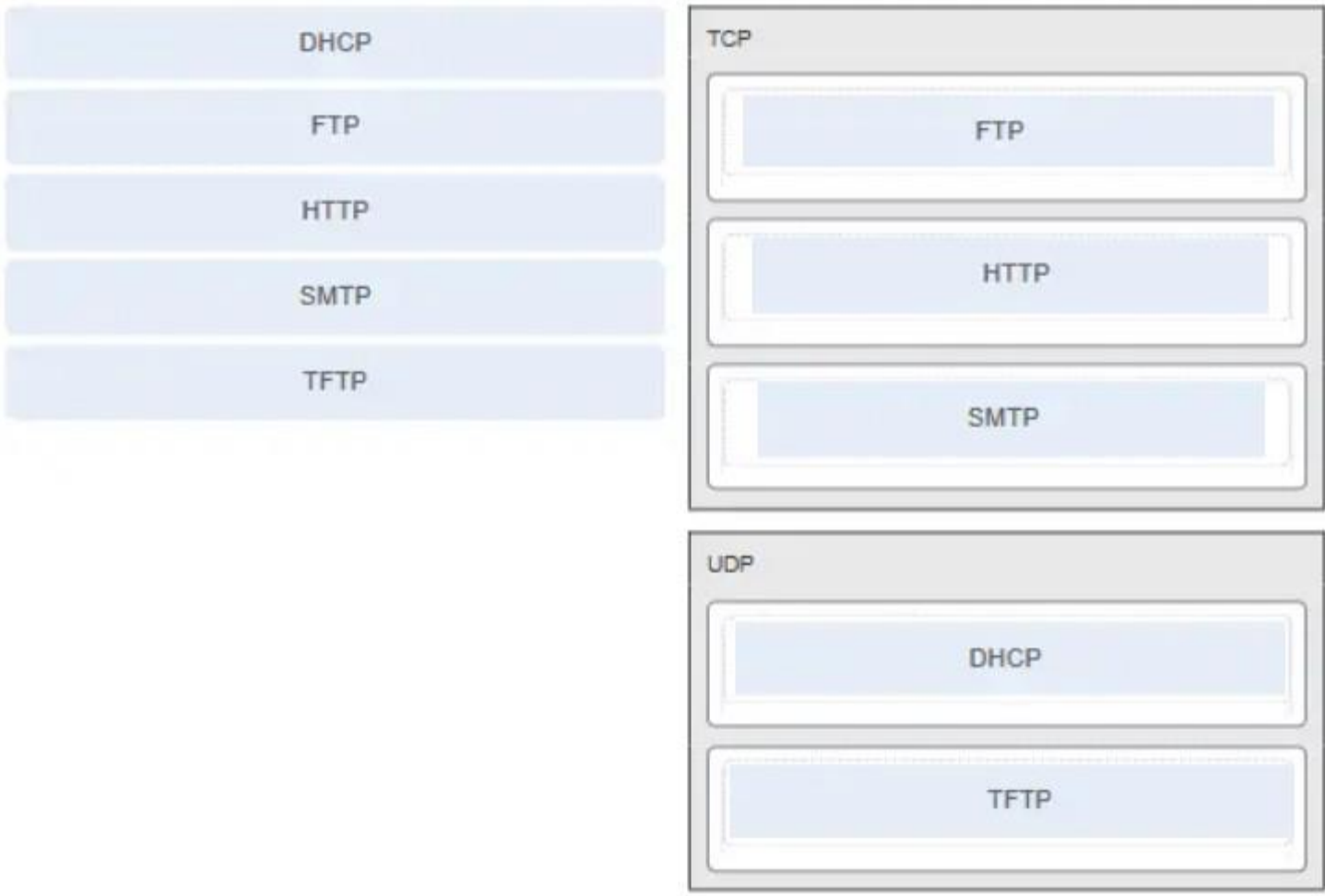
Explanation:
Network A needs to use 192.168.0.0 /25 which yields 128 host addresses.
Network B needs to use 192.168.0.128 /26 which yields 64 host addresses.
Network C needs to use 192.168.0.192 /27 which yields 32 host addresses.
Network D needs to use 192.168.0.224 /30 which yields 4 host addresses.

29. What characteristic describes a DoS attack?

- the use of stolen credentials to access private data

- a network device that filters access and traffic coming into a network
- software that is installed on a user device and collects information about the user
- **an attack that slows or crashes a device or network service**

30. Match the application protocols to the correct transport protocols



31. What service is provided by SMTP?

- **Allows clients to send email to a mail server and the servers to send email to other servers.**
- Allows remote access to network devices and servers.
- Uses encryption to provide secure remote access to network devices and servers.
- An application that allows real-time chatting among remote users.

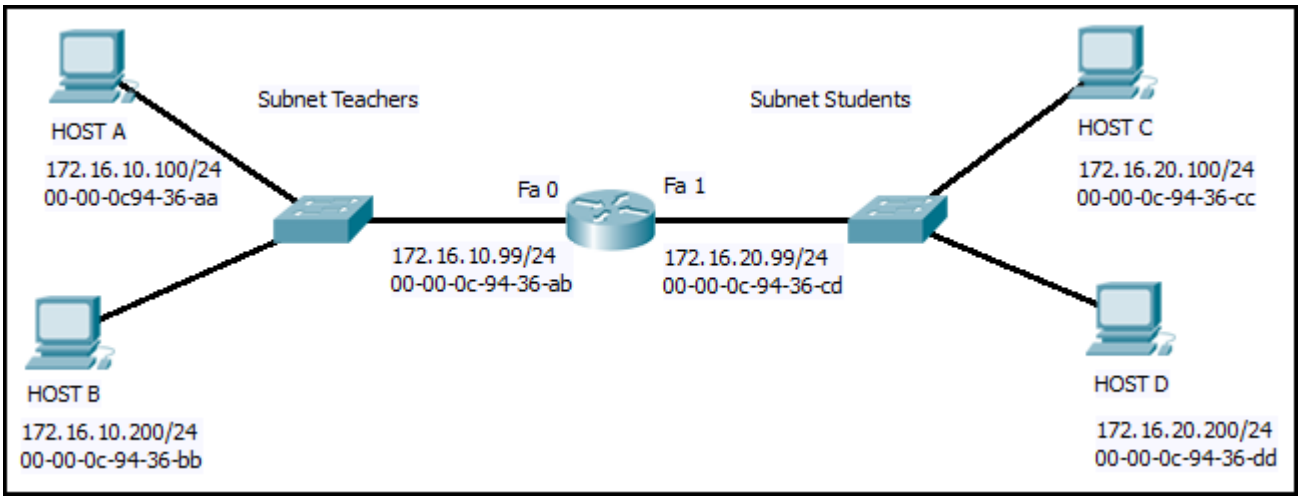
32. Which scenario describes a function provided by the transport layer?

- A student is using a classroom VoIP phone to call home. The unique identifier burned into the phone is a transport layer address used to contact another network device on the same network.
- A student is playing a short web-based movie with sound. The movie and sound are encoded within the transport layer header.

- **A student has two web browser windows open in order to access two web sites. The transport layer ensures the correct web page is delivered to the correct browser window.**
- A corporate worker is accessing a web server located on a corporate network. The transport layer formats the screen so the web page appears properly no matter what device is being used to view the web site.

Explain:
The source and destination port numbers are used to identify the correct application and window within that application.

33.Refer to the exhibit. Host B on subnet Teachers transmits a packet to host D on subnet Students. Which Layer 2 and Layer 3 addresses are contained in the PDUs that are transmitted from host B to the router?



Layer 2 destination address = 00-00-0c-94-36-ab
Layer 2 source address = 00-00-0c-94-36-bb
Layer 3 destination address = 172.16.20.200
Layer 3 source address = 172.16.10.200
Layer 2 destination address = 00-00-0c-94-36-dd
Layer 2 source address = 00-00-0c-94-36-bb
Layer 3 destination address = 172.16.20.200
Layer 3 source address = 172.16.10.200

Layer 2 destination address = 00-00-0c-94-36-cd
Layer 2 source address = 00-00-0c-94-36-bb
Layer 3 destination address = 172.16.20.99
Layer 3 source address = 172.16.10.200

Layer 2 destination address = 00-00-0c-94-36-ab
Layer 2 source address = 00-00-0c-94-36-bb
Layer 3 destination address = 172.16.20.200
Layer 3 source address = 172.16.100.200

34. What does the term "attenuation" mean in data communication?

- strengthening of a signal by a networking device
- leakage of signals from one cable pair to another
- time for a signal to reach its destination
- **loss of signal strength as distance increases**

Explanation: Data is transmitted on copper cables as electrical pulses. A detector in the network interface of a destination device must receive a signal that can be successfully decoded to match the signal sent. However, the farther the signal travels, the more it deteriorates. This is referred to as signal attenuation.

35. Refer to the exhibit. An administrator is trying to configure the switch but receives the error message that is displayed in the exhibit. What is the problem?

```
Switch1> config t
               ^
% Invalid input detected at '^' marker.
```

- The entire command, configure terminal, must be used.
- The administrator is already in global configuration mode.
- **The administrator must first enter privileged EXEC mode before issuing the command.**
- The administrator must connect via the console port to access global configuration mode.

36. Which two protocols operate at the top layer of the TCP/IP protocol suite? (Choose two.)

- TCP
- IP
- UDP
- **POP**
- **DNS**
- Ethernet

37. A company has a file server that shares a folder named Public. The network security policy specifies that the Public folder is assigned Read-Only rights to anyone who can log into the server while the Edit rights are assigned only to the network admin group. Which component is addressed in the AAA network service framework?

- automation
- accounting
- authentication
- **authorization**

After a user is successfully authenticated (logged into the server), the authorization is the process of determining what network resources the user can access and what operations (such as read or edit) the user can perform.

38. What three requirements are defined by the protocols used in network communcations to allow message transmission across a network? (Choose three.)

- **message size**
- **message encoding**
- connector specifications
- media selection
- **delivery options**
- end-device installation

39. What are two characteristics of IP? (Choose two.)

- **does not require a dedicated end-to-end connection**
- **operates independently of the network media**
- retransmits packets if errors occur
- re-assembles out of order packets into the correct order at the receiver end
- guarantees delivery of packets

Explain:
The Internet Protocol (IP) is a connectionless, best effort protocol. This means that IP requires no end-to-end connection nor does it guarantee delivery of packets. IP is also media independent, which means it operates independently of the network media carrying the packets.

40. An employee of a large corporation remotely logs into the company using the appropriate username and password. The employee is attending an important video conference with a customer concerning a large sale. It is important for the video quality to be excellent during the meeting. The employee is unaware that after a successful login, the connection to the company ISP failed. The secondary connection, however, activated within seconds. The disruption was not noticed by the employee or other employees.
What three network characteristics are described in this scenario? (Choose three.)

- **security**
- **quality of service**
- scalability
- powerline networking
- integrity
- **fault tolerance**

41. What are two common causes of signal degradation when using UTP cabling? (Choose two.)

- **improper termination**
- low-quality shielding in cable
- installing cables in conduit
- **low-quality cable or connectors**
- loss of light over long distances

Explanation: When terminated improperly, each cable is a potential source of physical layer performance degradation.

42. Which subnet would include the address 192.168.1.96 as a usable host address?

- **192.168.1.64/26**

- 192.168.1.32/27
- 192.168.1.32/28
- 192.168.1.64/29

Explanation: For the subnet of 192.168.1.64/26, there are 6 bits for host addresses, yielding 64 possible addresses. However, the first and last subnets are the network and broadcast addresses for this subnet. Therefore, the range of host addresses for this subnet is 192.168.1.65 to 192.168.1.126. The other subnets do not contain the address 192.168.1.96 as a valid host address.

43. Refer to the exhibit. On the basis of the output, which two statements about network connectivity are correct? (Choose two.)

```
C:\Windows\system32> tracert 192.168.100.1
Tracing route to 192.168.100.1 over a maximum of 30 hops
1    1 ms    <1 ms    <1 ms     10.10.10.10
2    2 ms     2 ms     1 ms     192.168.1.22
3    2 ms     2 ms     1 ms     192.168.1.62
4     2 ms     2 ms     1 ms     172.16.1.1
5     2 ms     2 ms     1 ms     192.168.100.1
Trace complete.
```

- This host does not have a default gateway configured.
- **There are 4 hops between this device and the device at 192.168.100.1.**
- **There is connectivity between this device and the device at 192.168.100.1.**
- The connectivity between these two hosts allows for videoconferencing calls.
- The average transmission time between the two hosts is 2 milliseconds.

Explain:
The output displays a successful Layer 3 connection between a host computer and a host at 19.168.100.1. It can be determined that 4 hops exist between them and the average transmission time is 1 milliseconds. Layer 3 connectivity does not necessarily mean that an application can run between the hosts.

44. Which two statements describe how to assess traffic flow patterns and network traffic types using a protocol analyzer? (Choose two.)

- Capture traffic on the weekends when most employees are off work.
- **Capture traffic during peak utilization times to get a good representation of the different traffic types.**
- Only capture traffic in the areas of the network that receive most of the traffic such as the data center.
- **Perform the capture on different network segments.**
- Only capture WAN traffic because traffic to the web is responsible for the largest amount of traffic on a network.

Explanation: Traffic flow patterns should be gathered during peak utilization times to get a good representation of the different traffic types. The capture should also be performed on different network segments because some traffic will be local to a particular segment.

45. What is the consequence of configuring a router with the *ipv6 unicast-routing* global configuration command?

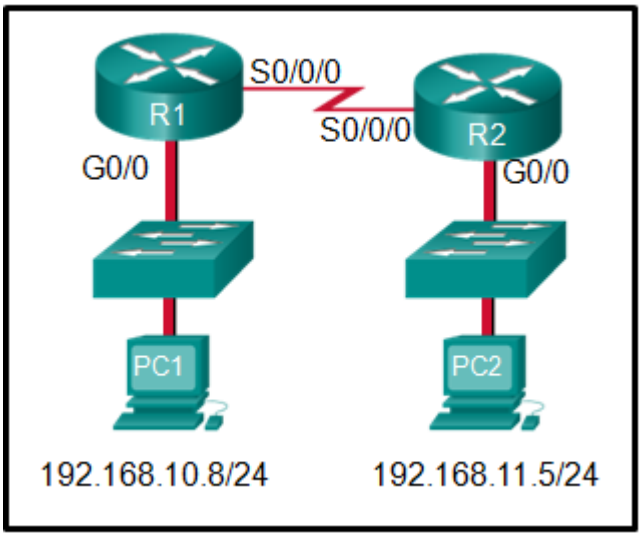
- All router interfaces will be automatically activated.
- **The IPv6 enabled router interfaces begin sending ICMPv6 Router Advertisement messages.**
- Each router interface will generate an IPv6 link-local address.
- It statically creates a global unicast address on this router.

46. Which three layers of the OSI model map to the application layer of the TCP/IP model? (Choose three.)

- **application**
- network
- data link
- **session**
- **presentation**
- transport

Explanation: The TCP/IP model consists of four layers: application, transport, internet, and network access. The OSI model consists of seven layers: application, presentation, session, transport, network, data link, and physical. The top three layers of the OSI model: application, presentation, and session map to the application layer of the TCP/IP model.

47. Refer to the exhibit. If PC1 is sending a packet to PC2 and routing has been configured between the two routers, what will R1 do with the Ethernet frame header attached by PC1?



- nothing, because the router has a route to the destination network
- open the header and use it to determine whether the data is to be sent out S0/0/0
- open the header and replace the destination MAC address with a new one

- **remove the Ethernet header and configure a new Layer 2 header before sending it out S0/0/0**

Explanation: When PC1 forms the various headers attached to the data one of those headers is the Layer 2 header. Because PC1 connects to an Ethernet network, an Ethernet header is used. The source MAC address will be the MAC address of PC1 and the destination MAC address will be that of G0/0 on R1. When R1 gets that information, the router removes the Layer 2 header and creates a new one for the type of network the data will be placed onto (the serial link).

48. What will happen if the default gateway address is incorrectly configured on a host?

- The host cannot communicate with other hosts in the local network.
- **The host cannot communicate with hosts in other networks.**
- A ping from the host to 127.0.0.1 would not be successful.
- The host will have to use ARP to determine the correct address of the default gateway.
- The switch will not forward packets initiated by the host.

49. What are two features of ARP? (Choose two.)

- When a host is encapsulating a packet into a frame, it refers to the MAC address table to determine the mapping of IP addresses to MAC addresses.
- An ARP request is sent to all devices on the Ethernet LAN and contains the IP address of the destination host and its multicast MAC address.
- **If a host is ready to send a packet to a local destination device and it has the IP address but not the MAC address of the destination, it generates an ARP broadcast.**
- If no device responds to the ARP request, then the originating node will broadcast the data packet to all devices on the network segment.
- **If a device receiving an ARP request has the destination IPv4 address, it responds with an ARP reply.**

50. A network administrator is adding a new LAN to a branch office. The new LAN must support 90 connected devices. What is the smallest network mask that the network administrator can use for the new network?

- **255.255.255.128**
- 255.255.255.240
- 255.255.255.248
- 255.255.255.224

51. What are two ICMPv6 messages that are not present in ICMP for IPv4? (Choose two.)

- **Neighbor Solicitation**
- Destination Unreachable
- Host Confirmation
- Time Exceeded

- **Router Advertisement**
- Route Redirection

52. A client packet is received by a server. The packet has a destination port number of 80. What service is the client requesting?

- DHCP
- SMTP
- DNS
- **HTTP**

53. What is an advantage for small organizations of adopting IMAP instead of POP?

- POP only allows the client to store messages in a centralized way, while IMAP allows distributed storage.
- **Messages are kept in the mail servers until they are manually deleted from the email client.**
- When the user connects to a POP server, copies of the messages are kept in the mail server for a short time, but IMAP keeps them for a long time.
- IMAP sends and retrieves email, but POP only retrieves email.

Explanation: IMAP and POP are protocols that are used to retrieve email messages. The advantage of using IMAP instead of POP is that when the user connects to an IMAP-capable server, copies of the messages are downloaded to the client application. IMAP then stores the email messages on the server until the user manually deletes those messages.

54. A technician can ping the IP address of the web server of a remote company but cannot successfully ping the URL address of the same web server. Which software utility can the technician use to diagnose the problem?

- tracert
- ipconfig
- netstat
- **nslookup**

Explain:
Traceroute (tracert) is a utility that generates a list of hops that were successfully reached along the path from source to destination.This list can provide important verification and troubleshooting information. The ipconfig utility is used to display the IP configuration settings on a Windows PC. The Netstat utility is used to identify which active TCP connections are open and running on a networked host. Nslookup is a utility that allows the user to manually query the name servers to resolve a given host name. This utility can also be used to troubleshoot name resolution issues and to verify the current status of the name servers.

55. Which two functions are performed at the LLC sublayer of the OSI Data Link Layer to facilitate Ethernet communication? (Choose two.)

- implements CSMA/CD over legacy shared half-duplex media

- **enables IPv4 and IPv6 to utilize the same physical medium**
- integrates Layer 2 flows between 10 Gigabit Ethernet over fiber and 1 Gigabit Ethernet over copper
- implements a process to delimit fields within an Ethernet 2 frame
- **places information in the Ethernet frame that identifies which network layer protocol is being encapsulated by the frame**

Other case:

- responsible for internal structure of Ethernet frame
- applies source and destination MAC addresses to Ethernet frame
- **handles communication between upper layer networking software and Ethernet NIC hardware**
- **adds Ethernet control information to network protocol data**
- implements trailer with frame check sequence for error detection

Other case:

- integrates Layer 2 flows between 10 Gigabit Ethernet over fiber and 1 Gigabit Ethernet over copper
- **places information in the Ethernet frame that identifies which network layer protocol is being encapsulated by the frame**
- implements CSMA/CD over legacy shared half-duplex media
- **adds Ethernet control information to network protocol data**
- applies source and destination MAC addresses to Ethernet frame

Other case:

- **enables IPv4 and IPv6 to utilize the same physical medium**
- **adds Ethernet control information to network protocol data**
- applies source and destination MAC addresses to Ethernet frame
- responsible for the internal structure of Ethernet frame
- implements trailer with frame check sequence for error detection

Other case:

- **enables IPv4 and IPv6 to utilize the same physical medium**
- applies source and destination MAC addresses to Ethernet frame
- integrates Layer 2 flows between 10 Gigabit Ethernet over fiber and 1 Gigabit Ethernet over copper
- **handles communication between upper layer networking software and Ethernet NIC hardware**
- responsible for internal structure of Ethernet frame

Explanation: The data link layer is actually divided into two sublayers:
+ Logical Link Control (LLC): This upper sublayer defines the software processes that provide services to the network layer protocols. It places information in the frame that identifies which network layer protocol is being used for the frame. This information allows multiple Layer 3 protocols, such as IPv4 and IPv6, to utilize the same network interface and media.
+ Media Access Control (MAC): This lower sublayer defines the media access processes performed by the hardware. It provides data link layer addressing and

delimiting of data according to the physical signaling requirements of the medium and the type of data link layer protocol in use.

56. The global configuration command *ip default-gateway 172.16.100.1* is applied to a switch. What is the effect of this command?

- The switch can communicate with other hosts on the 172.16.100.0 network.
- **The switch can be remotely managed from a host on another network.**
- The switch is limited to sending and receiving frames to and from the gateway 172.16.100.1.
- The switch will have a management interface with the address 172.16.100.1.

Explanation: A default gateway address is typically configured on all devices to allow them to communicate beyond just their local network.In a switch this is achieved using the command ip default-gateway <ip address>.

57. What happens when the *transport input ssh* command is entered on the switch vty lines?

- The SSH client on the switch is enabled.
- The switch requires a username/password combination for remote access.
- **Communication between the switch and remote users is encrypted.**
- The switch requires remote connections via a proprietary client software.

Explanation: The **transport input ssh** command when entered on the switch vty (virtual terminal lines) will encrypt all inbound controlled telnet connections.

58. Match the type of threat with the cause. (Not all options are used.)

hardware threats	poor handling of key electrical components (electrostatic discharge), lack of critical spare parts, poor cabling, and poor labeling
environmental threats	maintenance threats
electrical threats	unauthorized access resulting in loss of data
maintenance threats	temperature extremes (too hot or too cold) or humidity extremes (too wet or too dry)
	environmental threats
	physical damage to servers, routers, switches, cabling plant, and workstations
	hardware threats
	voltage spikes, insufficient supply voltage (brownouts), unconditioned power (noise), and total power loss
	electrical threats

59. A disgruntled employee is using some free wireless networking tools to determine information about the enterprise wireless networks. This person is planning on using this information to hack the wireless network. What type of attack is this?

- DoS
- access
- **reconnaissance**
- Trojan horse

Explanation: A reconnaissance attack is the unauthorized discovery and documentation of various computing networks, network systems, resources, applications, services, or vulnerabilities.

60. What service is provided by HTTP?

- Uses encryption to secure the exchange of text, graphic images, sound, and video on the web.
- Allows for data transfers between a client and a file server.
- An application that allows real-time chatting among remote users.
- **A basic set of rules for exchanging text, graphic images, sound, video, and other multimedia files on the web.**

61. A client packet is received by a server. The packet has a destination port number of 67. What service is the client requesting?

- FTP
- **DHCP**
- Telnet
- SSH

62. What are two problems that can be caused by a large number of ARP request and reply messages? (Choose two.)

- Switches become overloaded because they concentrate all the traffic from the attached subnets.
- **The ARP request is sent as a broadcast, and will flood the entire subnet.**
- The network may become overloaded because ARP reply messages have a very large payload due to the 48-bit MAC address and 32-bit IP address that they contain.
- A large number of ARP request and reply messages may slow down the switching process, leading the switch to make many changes in its MAC table.
- **All ARP request messages must be processed by all nodes on the local network.**

Explanation: ARP requests are sent as broadcasts:
(1) All nodes will receive them, and they will be processed by software, interrupting the CPU.
(2) The switch forwards (floods) Layer 2 broadcasts to all ports.

A switch does not change its MAC table based on ARP request or reply messages. The switch populates the MAC table using the source MAC address of all frames. The ARP payload is very small and does not overload the switch.

63. A group of Windows PCs in a new subnet has been added to an Ethernet network. When testing the connectivity, a technician finds that these PCs can access local network resources but not the Internet resources. To troubleshoot the problem, the technician wants to initially confirm the IP address and DNS configurations on the PCs, and also verify connectivity to the local router. Which three Windows CLI commands and utilities will provide the necessary information? (Choose three.)

- netsh interface ipv6 show neighbor
- arp -a
- tracert
- **ping**
- **ipconfig**
- **nslookup**
- telnet

64. During the process of forwarding traffic, what will the router do immediately after matching the destination IP address to a network on a directly connected routing table entry?

- analyze the destination IP address
- **switch the packet to the directly connected interface**
- look up the next-hop address for the packet
- discard the traffic after consulting the route table

Explanation: A router receives a packet on an interface and looks at the destination IP address. It consults its routing table and matches the destination IP address to a routing table entry. The router then discovers that it has to send the packet to the next-hop address or out to a directly connected interface. When the destination address is on a directly connected interface, the packet is switched over to that interface.

65. What characteristic describes antispyware?

- **applications that protect end devices from becoming infected with malicious software**
- a network device that filters access and traffic coming into a network
- software on a router that filters traffic based on IP addresses or applications
- a tunneling protocol that provides remote users with secure access into the network of an organization

66. A network administrator needs to keep the user ID, password, and session contents private when establishing remote CLI connectivity with a switch to manage it. Which access method should be chosen?

- Telnet
- AUX

- **SSH**
- Console

67. What are the two most effective ways to defend against malware? (Choose two.)

- Implement a VPN.
- Implement network firewalls.
- Implement RAID.
- Implement strong passwords.
- **Update the operating system and other application software.**
- **Install and update antivirus software.**

Explanation: A cybersecurity specialist must be aware of the technologies and measures that are used as countermeasures to protect the organization from threats and vulnerabilities.

68. Which type of security threat would be responsible if a spreadsheet add-on disables the local software firewall?

- brute-force attack
- **Trojan horse**
- DoS
- buffer overflow

Explanation: A Trojan horse is software that does something harmful, but is hidden in legitimate software code. A denial of service (DoS) attack results in interruption of network services to users, network devices, or applications. A brute-force attack commonly involves trying to access a network device. A buffer overflow occurs when a program attempts to store more data in a memory location than it can hold.

69. Which frame field is created by a source node and used by a destination node to ensure that a transmitted data signal has not been altered by interference, distortion, or signal loss?

- User Datagram Protocol field
- transport layer error check field
- flow control field
- **frame check sequence field**
- error correction process field

70. A network administrator is adding a new LAN to a branch office. The new LAN must support 4 connected devices. What is the smallest network mask that the network administrator can use for the new network?

- **255.255.255.248**
- 255.255.255.0
- 255.255.255.128
- 255.255.255.192

71. What service is provided by POP3?

- **Retrieves email from the server by downloading the email to the local mail application of the client.**

- An application that allows real-time chatting among remote users.
- Allows remote access to network devices and servers.
- Uses encryption to provide secure remote access to network devices and servers.

72. What two security solutions are most likely to be used only in a corporate environment? (Choose two.)

- antispyware
- **virtual private networks**
- **intrusion prevention systems**
- strong passwords
- antivirus software

73. What characteristic describes antivirus software?

- **applications that protect end devices from becoming infected with malicious software**
- a network device that filters access and traffic coming into a network
- a tunneling protocol that provides remote users with secure access into the network of an organization
- software on a router that filters traffic based on IP addresses or applications

74. What mechanism is used by a router to prevent a received IPv4 packet from traveling endlessly on a network?

- It checks the value of the TTL field and if it is 0, it discards the packet and sends a Destination Unreachable message to the source host.
- It checks the value of the TTL field and if it is 100, it discards the packet and sends a Destination Unreachable message to the source host.
- **It decrements the value of the TTL field by 1 and if the result is 0, it discards the packet and sends a Time Exceeded message to the source host.**
- It increments the value of the TTL field by 1 and if the result is 100, it discards the packet and sends a Parameter Problem message to the source host.

75. A client packet is received by a server. The packet has a destination port number of 69. What service is the client requesting?

- DNS
- DHCP
- SMTP
- **TFTP**

76. An administrator defined a local user account with a secret password on router R1 for use with SSH. Which three additional steps are required to configure R1 to accept only encrypted SSH connections? (Choose three.)

- Configure DNS on the router.
- Generate two-way pre-shared keys.
- **Configure the IP domain name on the router.**
- **Generate the SSH keys.**
- **Enable inbound vty SSH sessions.**

- Enable inbound vty Telnet sessions.

77. Which two functions are performed at the MAC sublayer of the OSI Data Link Layer to facilitate Ethernet communication? (Choose two.)

- handles communication between upper layer networking software and Ethernet NIC hardware
- **implements trailer with frame check sequence for error detection**
- places information in the Ethernet frame that identifies which network layer protocol is being encapsulated by the frame
- **implements a process to delimit fields within an Ethernet 2 frame**
- adds Ethernet control information to network protocol data

Case 2:

- places information in the Ethernet frame that identifies which network layer protocol is being encapsulated by the frame
- adds Ethernet control information to network protocol data
- **responsible for internal structure of Ethernet frame**
- enables IPv4 and IPv6 to utilize the same physical medium
- **implements trailer with frame check sequence for error detection**

Case 3:

- **integrates Layer 2 flows between 10 Gigabit Ethernet over fiber and 1 Gigabit Ethernet over copper**
- enables IPv4 and IPv6 to utilize the same physical medium
- handles communication between upper layer networking software and Ethernet NIC hardware
- adds Ethernet control information to network protocol data
- **implements CSMA/CD over legacy shared half-duplex media**

Case 4:

- **applies delimiting of Ethernet frame fields to synchronize communication between nodes**
- places information in the Ethernet frame that identifies which network layer protocol is being encapsulated by the frame
- adds Ethernet control information to network protocol data
- **implements trailer with frame check sequence for error detection**
- handles communication between upper layer networking software and Ethernet NIC hardware

78. An IPv6 enabled device sends a data packet with the destination address of FF02::2. What is the target of this packet?

- all IPv6 enabled devices on the local link
- all IPv6 DHCP servers
- all IPv6 enabled devices across the network
- **all IPv6 configured routers on the local link**

79. What are the three parts of an IPv6 global unicast address? (Choose three.)

- **subnet ID**
- subnet mask

- broadcast address
- **global routing prefix**
- **interface ID**

Explanation: The general format for IPv6 global unicast addresses includes a global routing prefix, a subnet ID, and an interface ID. The global routing prefix is the network portion of the address. A typical global routing prefix is /48 assigned by the Internet provider. The subnet ID portion can be used by an organization to create multiple subnetwork numbers. The interface ID is similar to the host portion of an IPv4 address.

80. A network administrator is designing the layout of a new wireless network. Which three areas of concern should be accounted for when building a wireless network? (Choose three.)

- extensive cabling
- mobility options
- packet collision
- **interference**
- **security**
- **coverage area**

Explanation: The three areas of concern for wireless networks focus on the size of the coverage area, any nearby interference, and providing network security. Extensive cabling is not a concern for wireless networks, as a wireless network will require minimal cabling for providing wireless access to hosts. Mobility options are not a component of the areas of concern for wireless networks.

81. A new network administrator has been asked to enter a banner message on a Cisco device. What is the fastest way a network administrator could test whether the banner is properly configured?

- Enter CTRL-Z at the privileged mode prompt.
- Exit global configuration mode.
- Power cycle the device.
- Reboot the device.
- **Exit privileged EXEC mode and press Enter .**

82. What method is used to manage contention-based access on a wireless network?

- token passing
- **CSMA/CA**
- priority ordering
- CSMA/CD

83. What is a function of the data link layer?

- provides the formatting of data
- provides end-to-end delivery of data between hosts
- provides delivery of data between two applications
- **provides for the exchange of frames over a common local media**

84. What is the purpose of the TCP sliding window?

- to ensure that segments arrive in order at the destination
- to end communication when data transmission is complete
- to inform a source to retransmit data from a specific point forward
- **to request that a source decrease the rate at which it transmits data**

Explanation: The TCP sliding window allows a destination device to inform a source to slow down the rate of transmission. To do this, the destination device reduces the value contained in the window field of the segment. It is acknowledgment numbers that are used to specify retransmission from a specific point forward. It is sequence numbers that are used to ensure segments arrive in order. Finally, it is a FIN control bit that is used to end a communication session.

85. What characteristic describes spyware?

- a network device that filters access and traffic coming into a network
- **software that is installed on a user device and collects information about the user**
- an attack that slows or crashes a device or network service
- the use of stolen credentials to access private data

86. Which switching method drops frames that fail the FCS check?

- **store-and-forward switching**
- borderless switching
- ingress port buffering
- cut-through switching

87. Which range of link-local addresses can be assigned to an IPv6-enabled interface?

- FEC0::/10
- FDEE::/7
- **FE80::/10**
- FF00::/8

Explain:
Link-local addresses are in the range of FE80::/10 to FEBF::/10. The original IPv6 specification defined site-local addresses and used the prefix range FEC0::/10, but these addresses were deprecated by the IETF in favor of unique local addresses. FDEE::/7 is a unique local address because it is in the range of FC00::/7 to FDFF::/7. IPv6 multicast addresses have the prefix FF00::/8.

88. What service is provided by FTP?

- A basic set of rules for exchanging text, graphic images, sound, video, and other multimedia files on the web.
- An application that allows real-time chatting among remote users.
- **Allows for data transfers between a client and a file server.**
- Uses encryption to secure the exchange of text, graphic images, sound, and video on the web.

89. A user is attempting to access http://www.cisco.com/ without success. Which two configuration values must be set on the host to allow this access? (Choose two.)

- **DNS server**
- source port number
- HTTP server
- source MAC address
- **default gateway**

90. Which two statements accurately describe an advantage or a disadvantage when deploying NAT for IPv4 in a network? (Choose two.)

- NAT adds authentication capability to IPv4.
- **NAT introduces problems for some applications that require end-to-end connectivity.**
- NAT will impact negatively on switch performance.
- **NAT provides a solution to slow down the IPv4 address depletion.**
- NAT improves packet handling.
- NAT causes routing tables to include more information.

Explanation: Network Address Translation (NAT) is a technology that is implemented within IPv4 networks. One application of NAT is to use private IP addresses inside a network and use NAT to share a few public IP addresses for many internal hosts. In this way it provides a solution to slow down the IPv4 address depletion. However, since NAT hides the actual IP addresses that are used by end devices, it may cause problems for some applications that require end-to-end connectivity.

91. What would be the interface ID of an IPv6 enabled interface with a MAC address of 1C-6F-65-C2-BD-F8 when the interface ID is generated by using the EUI-64 process?

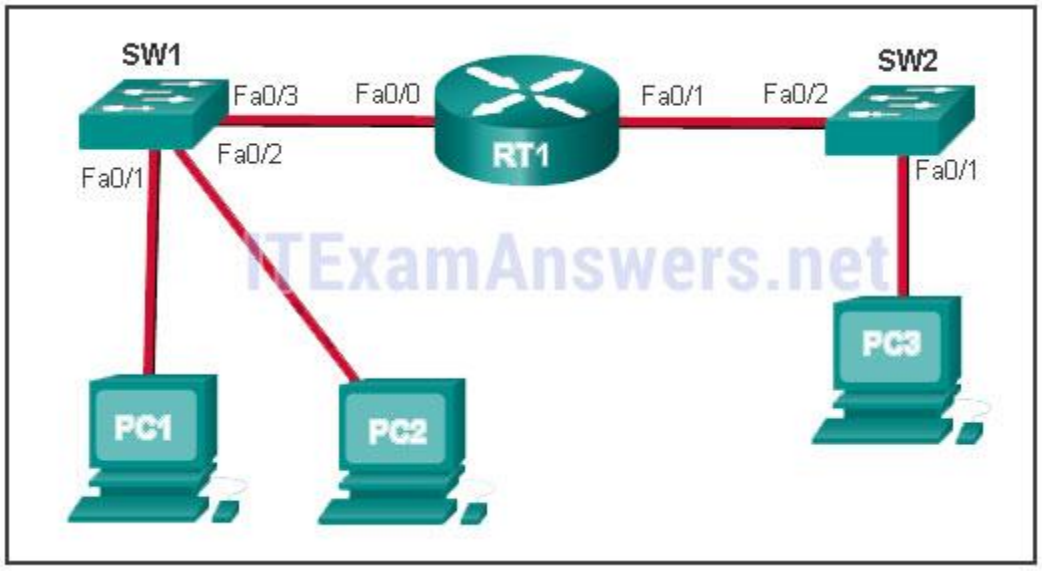
- 0C6F:65FF:FEC2:BDF8
- **1E6F:65FF:FEC2:BDF8**
- C16F:65FF:FEC2:BDF8
- 106F:65FF:FEC2:BDF8

Explanation: To derive the EUI-64 interface ID by using the MAC address 1C-6F-65-C2-BD-F8, three steps are taken.

- Change the seventh bit of the MAC address from a binary 0 to a binary 1 which changes the hex C, into a hex E.
- Insert hex digits FFFE into the middle of the address.
- Rewrite the address in IPv6 format.

The three steps, when complete, give the interface ID of **1E6F:65FF:FEC2:BDF8**.

92. Refer to the exhibit. PC1 issues an ARP request because it needs to send a packet to PC2. In this scenario, what will happen next?



- SW1 will send an ARP reply with the SW1 Fa0/1 MAC address.
- SW1 will send an ARP reply with the PC2 MAC address.
- **PC2 will send an ARP reply with the PC2 MAC address.**
- RT1 will send an ARP reply with the RT1 Fa0/0 MAC address.
- RT1 will send an ARP reply with the PC2 MAC address.

Explain: When a network device wants to communicate with another device on the same network, it sends a broadcast ARP request. In this case, the request will contain the IP address of PC2. The destination device (PC2) sends an ARP reply with its MAC address.

93. What service is provided by BOOTP?

- Uses encryption to secure the exchange of text, graphic images, sound, and video on the web.
- Allows for data transfers between a client and a file server.
- **Legacy application that enables a diskless workstation to discover its own IP address and find a BOOTP server on the network.**
- A basic set of rules for exchanging text, graphic images, sound, video, and other multimedia files on the web.

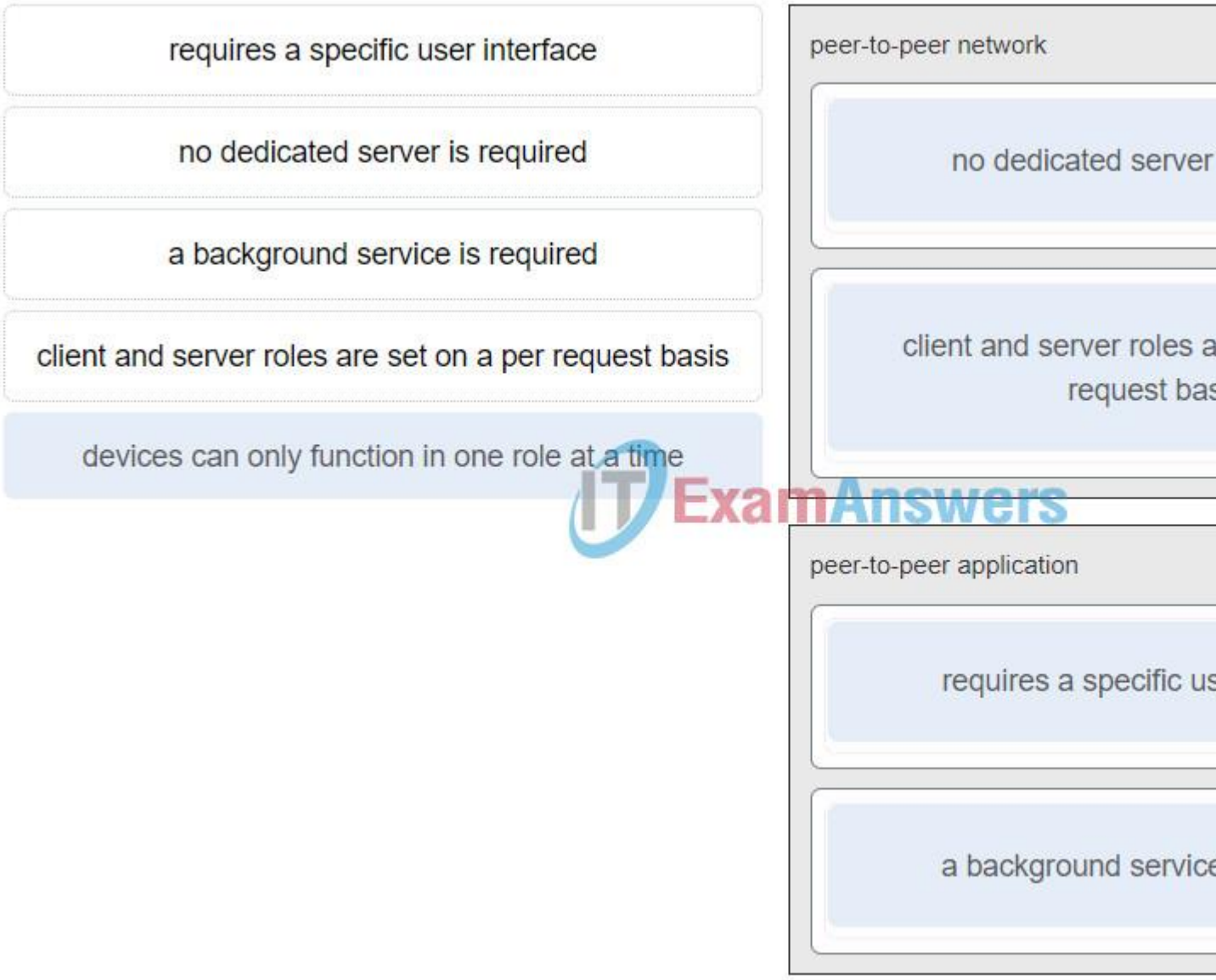
94. What characteristic describes adware?

- a network device that filters access and traffic coming into a network
- **software that is installed on a user device and collects information about the user**
- the use of stolen credentials to access private data
- an attack that slows or crashes a device or network service

95. When a switch configuration includes a user-defined error threshold on a per-port basis, to which switching method will the switch revert when the error threshold is reached?

- cut-through
- **store-and-forward**
- fast-forward
- fragment-free

96. Match a statement to the related network model. (Not all options are used.)



Place the options in the following order:peer-to-peer network
[+] no dedicated server is required
[+] client and server roles are set on a per request basis
peer-to-peer aplication

[#] requires a specific user interface
[#] a background service is required

Explain:
Peer-to-peer networks do not require the use of a dedicated server, and devices can assume both client and server roles simultaneously on a per request basis. Because they do not require formalized accounts or permissions, they are best used in limited situations. Peer-to-peer applications require a user interface and background service to be running, and can be used in more diverse situations.

97. What are two primary responsibilities of the Ethernet MAC sublayer? (Choose two.)

- error detection
- frame delimiting
- **accessing the media**
- **data encapsulation**
- logical addressing

98. Refer to the exhibit. What three facts can be determined from the viewable output of the show ip interface brief command? (Choose three.)

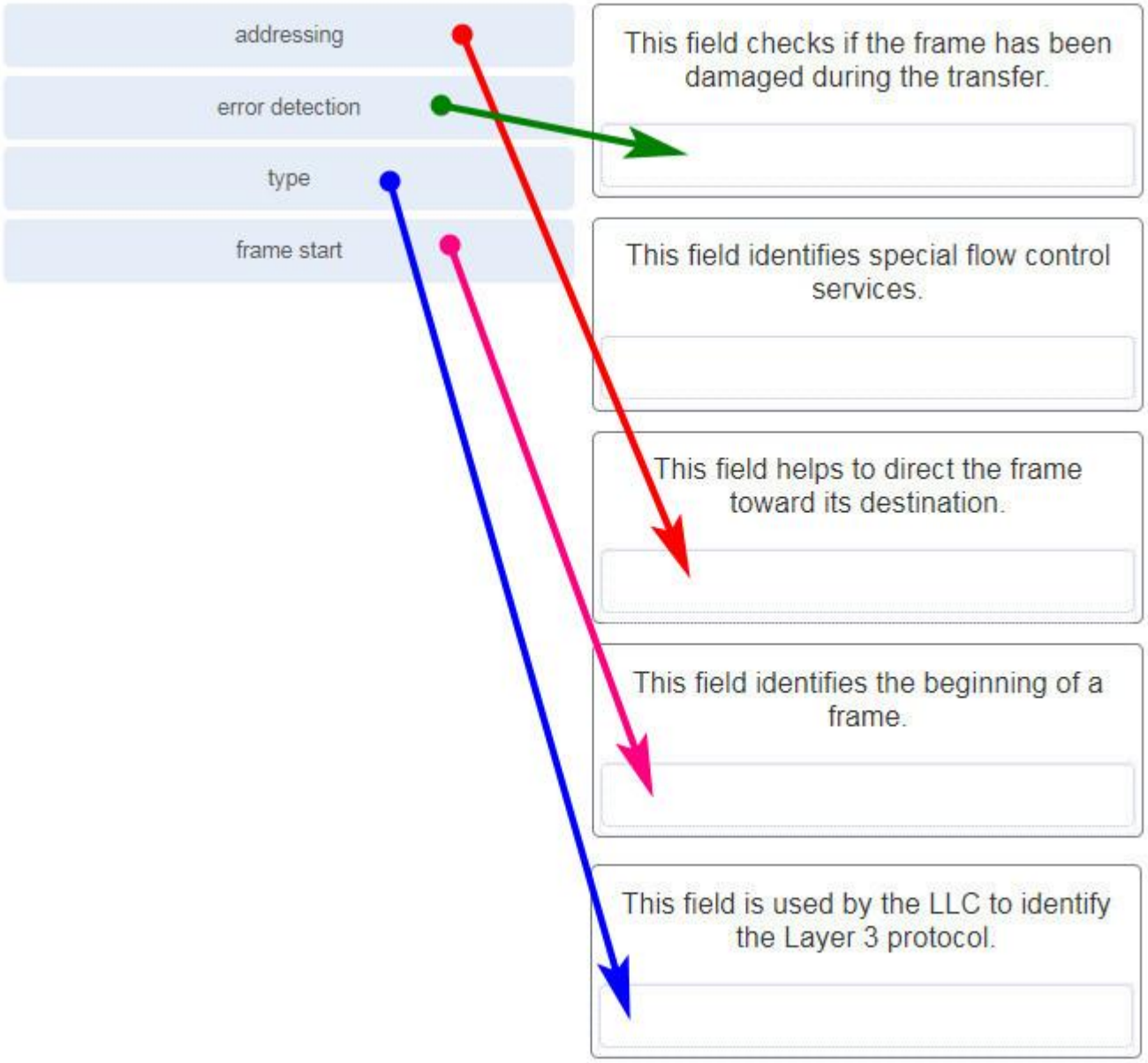
```
Switch# show ip interface brief
Interface              IP-Address      OK? Method  Status    Protocol
FastEthernet0/1        unassigned      YES manual  up        up
FastEthernet0/2        unassigned      YES manual  down      down
FastEthernet0/3        unassigned      YES manual  down      down
FastEthernet0/5        unassigned      YES manual  down      down
FastEthernet0/6        unassigned      YES manual  down      down

(output omitted)

FastEthernet0/23       unassigned      YES manual  down      down
FastEthernet0/24       unassigned      YES manual  down      down
Vlan1                  192.168.11.3    YES manual  up        up
```


- Two physical interfaces have been configured.
- **The switch can be remotely managed.**
- **One device is attached to a physical interface.**
- Passwords have been configured on the switch.
- Two devices are attached to the switch.
- **The default SVI has been configured.**

Explain:
Vlan1 is the default SVI. Because an SVI has been configured, the switch can be

configured and managed remotely. FastEthernet0/0 is showing up and up, so a device is connected.

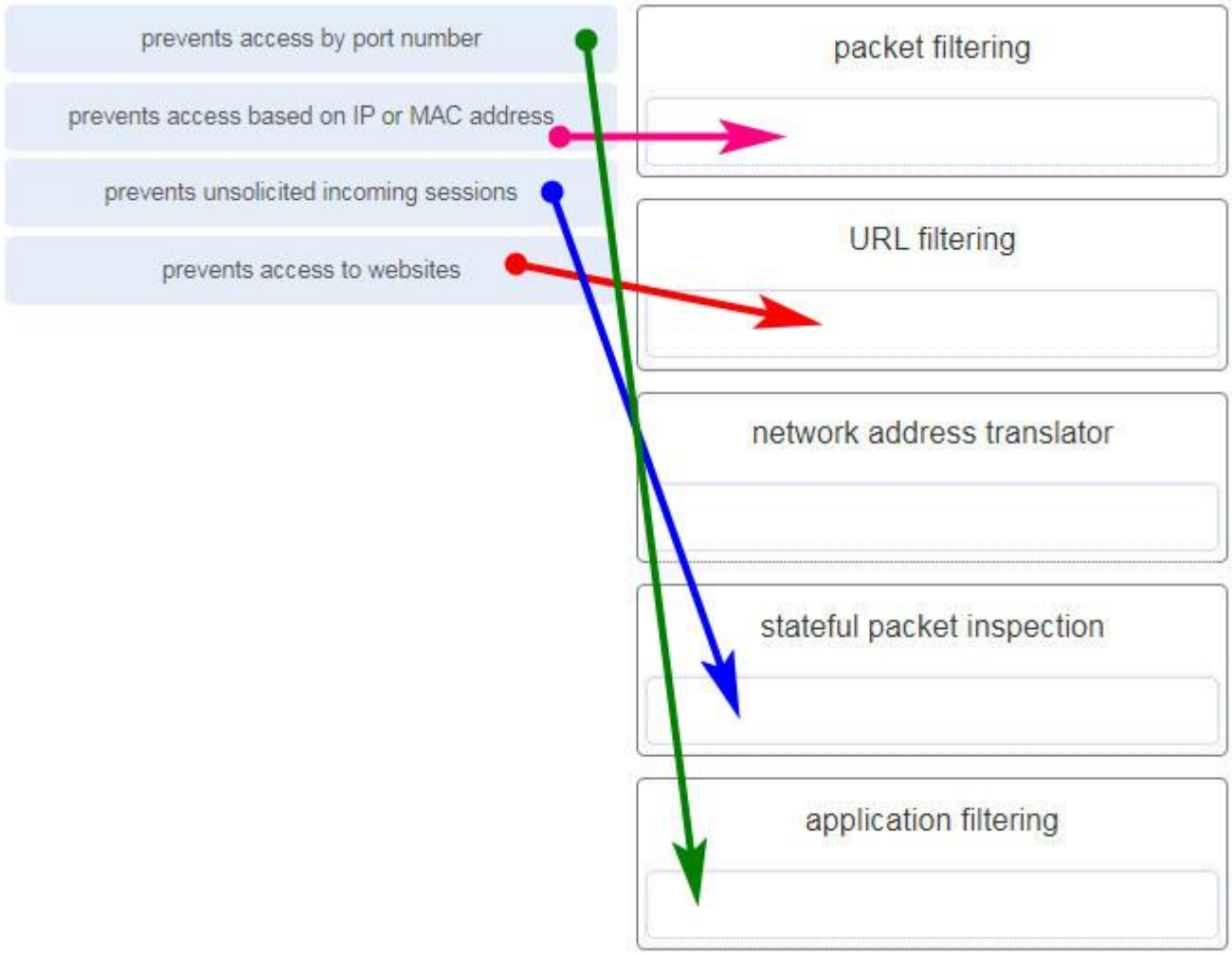
99. Match each type of frame field to its function. (Not all options are used.)



100. What is the subnet ID associated with the IPv6 address 2001:DA48:FC5:A4:3D1B::1/64?

- 2001:DA48::/64
- 2001:DA48:FC5::A4:/64
- **2001:DA48:FC5:A4::/64**
- 2001::/64

101. Match the firewall function to the type of threat protection it provides to the network. (Not all options are used.)



- packet filtering – prevents access based on IP or MAC address
- URL filtering – prevents access to websites
- network address translator – (none)
- stateful packet inspection – prevents unsolicited incoming sessions
- application filtering – prevents access by port number

Explain: Firewall products come packaged in various forms. These products use different techniques for determining what will be permitted or denied access to a network. They include the following:
+ Packet filtering – Prevents or allows access based on IP or MAC addresses
+ Application filtering – Prevents or allows access by specific application types based on port numbers
+ URL filtering – Prevents or allows access to websites based on specific URLs or keywords
+ Stateful packet inspection (SPI) – Incoming packets must be legitimate responses to requests from internal hosts. Unsolicited packets are blocked

unless permitted specifically. SPI can also include the capability to recognize and filter out specific types of attacks, such as denial of service (DoS)

102. Users are reporting longer delays in authentication and in accessing network resources during certain time periods of the week. What kind of information should network engineers check to find out if this situation is part of a normal network behavior?

- syslog records and messages
- **the network performance baseline**
- debug output and packet captures
- network configuration files

103. How does the service password-encryption command enhance password security on Cisco routers and switches?

- It requires encrypted passwords to be used when connecting remotely to a router or switch with Telnet.
- **It encrypts passwords that are stored in router or switch configuration files.**
- It requires that a user type encrypted passwords to gain console access to a router or switch.
- It encrypts passwords as they are sent across the network.

Explain: The service password-encryption command encrypts plaintext passwords in the configuration file so that they cannot be viewed by unauthorized users.

104. Which two statements are correct in a comparison of IPv4 and IPv6 packet headers? (Choose two.)

- **The Source Address field name from IPv4 is kept in IPv6.**
- The Version field from IPv4 is not kept in IPv6.
- The Destination Address field is new in IPv6.
- The Header Checksum field name from IPv4 is kept in IPv6.
- **The Time-to-Live field from IPv4 has been replaced by the Hop Limit field in IPv6.**

Explanation: The IPv6 packet header fields are as follows: Version, Traffic Class, Flow Label, Payload Length, Next Header, Hop Limit, Source Address, and Destination Address. The IPv4 packet header fields include the following: Version, Differentiated Services, Time-to-Live, Protocol, Source IP Address, and Destination IP Address. Both versions have a 4-bit Version field. Both versions have a Source (IP) Address field. IPv4 addresses are 32 bits; IPv6 addresses are 128 bits. The Time-to-Live or TTL field in IPv4 is now called Hop Limit in IPv6, but this field serves the same purpose in both versions. The value in this 8-bit field decrements each time a packet passes through any router. When this value is 0, the packet is discarded and is not forwarded to any other router.

105. A network administrator wants to have the same network mask for all networks at a particular small site. The site has the following networks and number

of devices:
IP phones – 22 addresses
PCs – 20 addresses needed
Printers – 2 addresses needed
Scanners – 2 addresses needed
The network administrator has deemed that 192.168.10.0/24 is to be the network used at this site. Which single subnet mask would make the most efficient use of the available addresses to use for the four subnetworks?

- 255.255.255.192
- 255.255.255.252
- 255.255.255.240
- 255.255.255.248
- 255.255.255.0
- **255.255.255.224**

106. What characteristic describes identity theft?

- **the use of stolen credentials to access private data**
- software on a router that filters traffic based on IP addresses or applications
- software that identifies fast-spreading threats
- a tunneling protocol that provides remote users with secure access into the network of an organization

107. A network administrator is adding a new LAN to a branch office. The new LAN must support 200 connected devices. What is the smallest network mask that the network administrator can use for the new network?

- 255.255.255.240
- **255.255.255.0**
- 255.255.255.248
- 255.255.255.224

108. What are three commonly followed standards for constructing and installing cabling? (Choose three.)

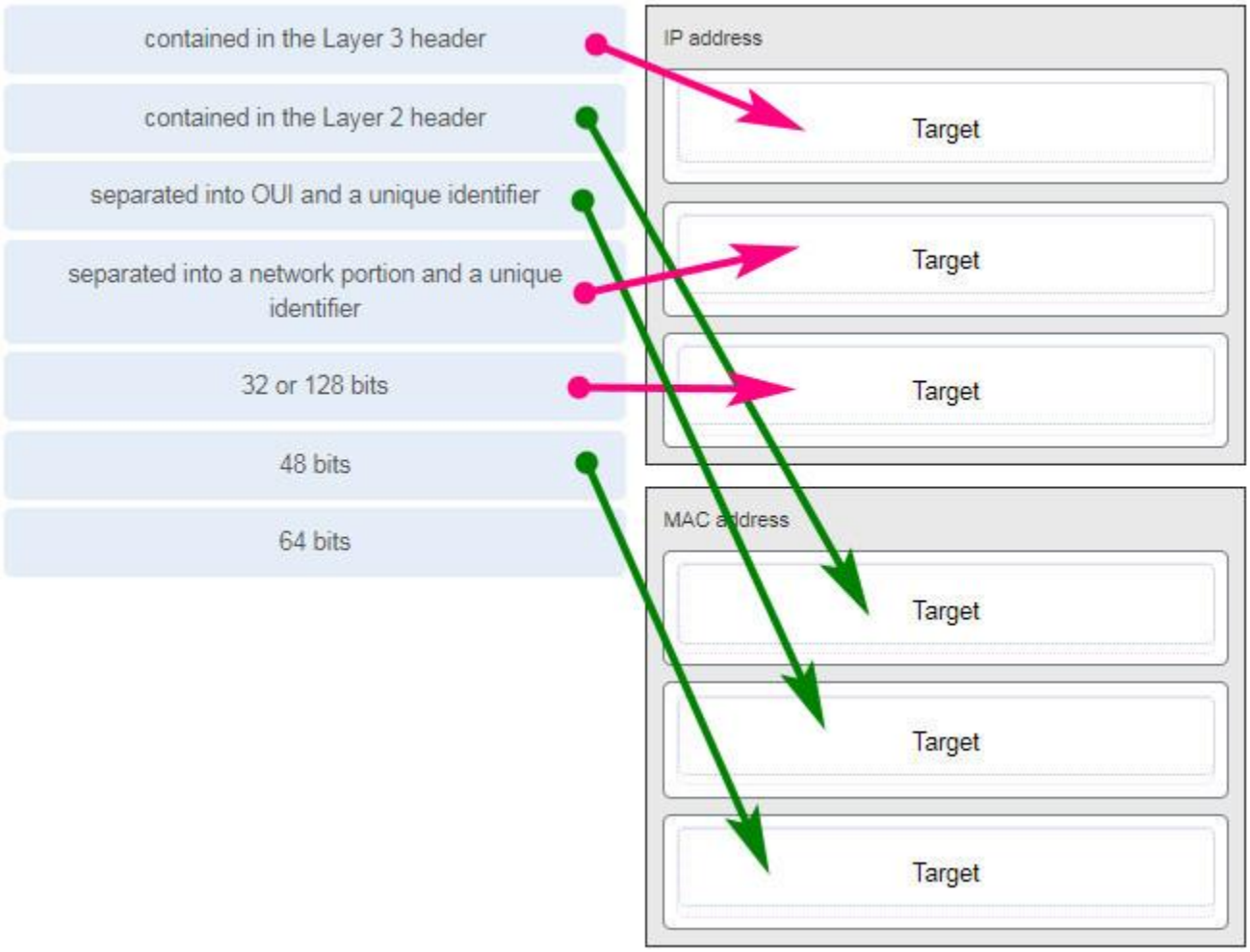
- cost per meter (foot)
- **cable lengths**
- connector color
- **pinouts**
- **connector types**
- tensile strength of plastic insulator

109. Refer to the exhibit. What is wrong with the displayed termination?

- The woven copper braid should not have been removed.
- The wrong type of connector is being used.
- **The untwisted length of each wire is too long.**
- The wires are too thick for the connector that is used.

Explanation: When a cable to an RJ-45 connector is terminated, it is important to ensure that the untwisted wires are not too long and that the flexible plastic sheath surrounding the wires is crimped down and not the bare wires. None of the colored wires should be visible from the bottom of the jack.

110. Match the characteristic to the category. (Not all options are used.)



111. A client packet is received by a server. The packet has a destination port number of 143. What service is the client requesting?

- **IMAP**
- FTP
- SSH
- Telnet

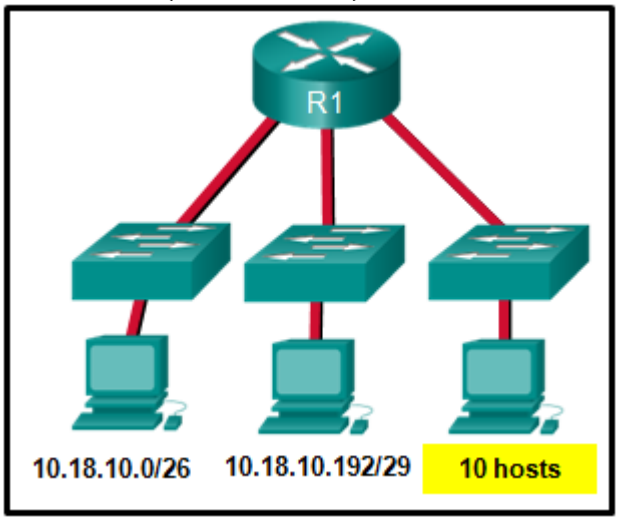
112. What are two characteristics shared by TCP and UDP? (Choose two.)

- default window size
- connectionless communication
- **port numbering**
- 3-way handshake
- ability to to carry digitized voice
- **use of checksum**

Explain:
Both TCP and UDP use source and destination port numbers to distinguish different data streams and to forward the right data segments to the right applications. Error checking the header and data is done by both protocols by

using a checksum calculation to determine the integrity of the data that is received. TCP is connection-oriented and uses a 3-way handshake to establish an initial connection. TCP also uses window to regulate the amount of traffic sent before receiving an acknowledgment. UDP is connectionless and is the best protocol for carry digitized VoIP signals.

113. Refer to the exhibit. Which two network addresses can be assigned to the network containing 10 hosts? Your answers should waste the fewest addresses, not reuse addresses that are already assigned, and stay within the 10.18.10.0/24 range of addresses. (Choose two.)



- 10.18.10.200/28
- **10.18.10.208/28**
- 10.18.10.240/27
- 10.18.10.200/27
- 10.18.10.224/27
- **10.18.10.224/28**

Explanation: Addresses 10.18.10.0 through 10.18.10.63 are taken for the leftmost network. Addresses 192 through 199 are used by the center network. Because 4 host bits are needed to accommodate 10 hosts, a /28 mask is needed. 10.18.10.200/28 is not a valid network number. Two subnets that can be used are 10.18.10.208/28 and 10.18.10.224/28.

114. A client packet is received by a server. The packet has a destination port number of 21. What service is the client requesting?

- **FTP**
- LDAP
- SLP
- SNMP

115. What attribute of a NIC would place it at the data link layer of the OSI model?

- attached Ethernet cable

- IP address
- **MAC address**
- RJ-45 port
- TCP/IP protocol stack

116. A network administrator is adding a new LAN to a branch office. The new LAN must support 10 connected devices. What is the smallest network mask that the network administrator can use for the new network?

- 255.255.255.192
- 255.255.255.248
- 255.255.255.224
- **255.255.255.240**

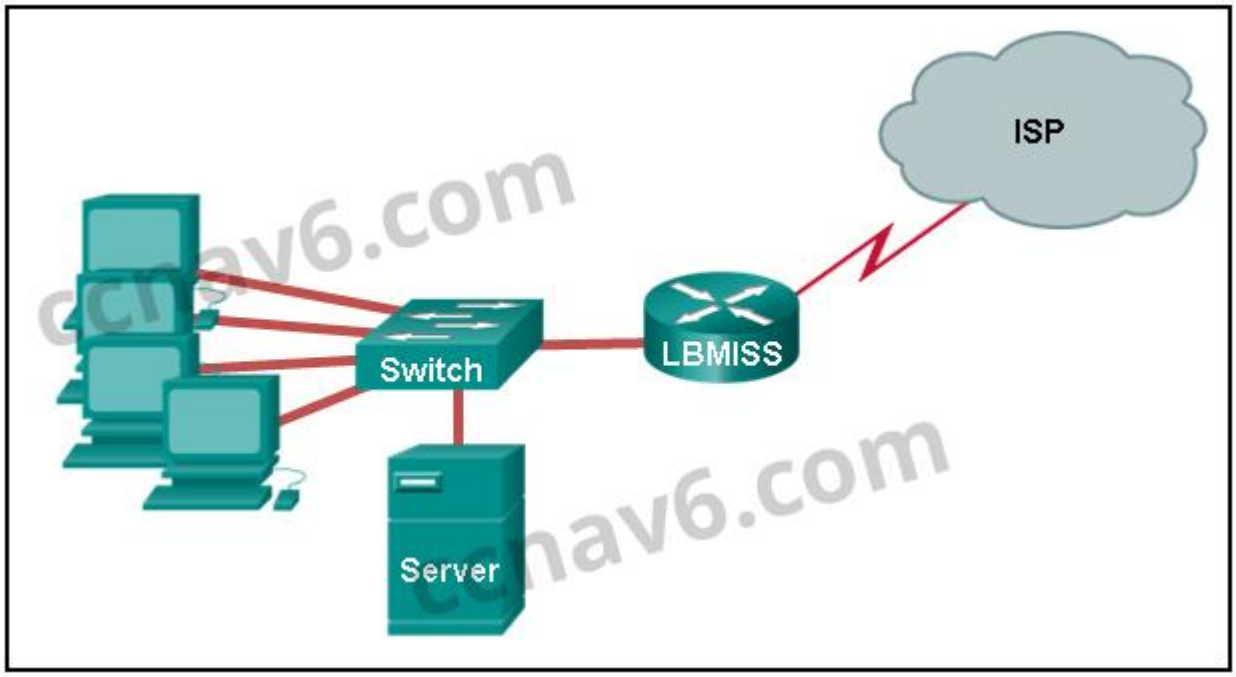
117. What technique is used with UTP cable to help protect against signal interference from crosstalk?

- wrapping a foil shield around the wire pairs
- **twisting the wires together into pairs**
- terminating the cable with special grounded connectors
- encasing the cables within a flexible plastic sheath

Explanation: To help prevent the effects of crosstalk, UTP cable wires are twisted together into pairs. Twisting the wires together causes the magnetic fields of each wire to cancel each other out.

118. Refer to the exhibit. The network administrator has assigned the LAN of LBMISS an address range of 192.168.10.0. This address range has been subnetted using a /29 prefix. In order to accommodate a new building, the technician has decided to use the fifth subnet for configuring the new network (subnet zero is the first subnet). By company policies, the router interface is always assigned the first usable host address and the workgroup server is given the last usable host address. Which configuration should be entered into the properties of the workgroup server

to allow connectivity to the Internet?

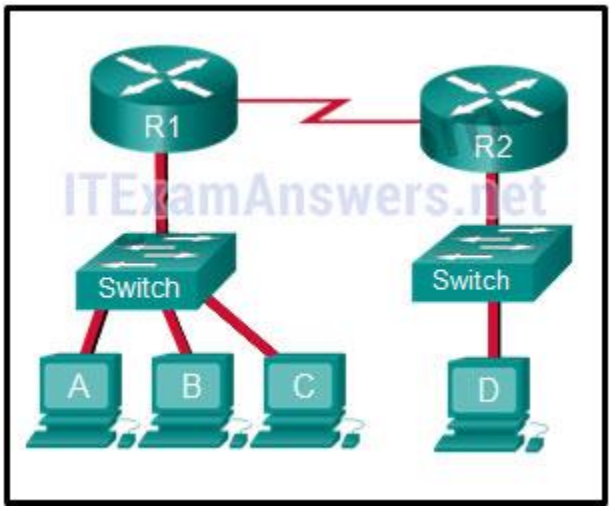


- IP address: 192.168.10.65 subnet mask: 255.255.255.240, default gateway: 192.168.10.76
- IP address: 192.168.10.38 subnet mask: 255.255.255.240, default gateway: 192.168.10.33
- **IP address: 192.168.10.38 subnet mask: 255.255.255.248, default gateway: 192.168.10.33**
- IP address: 192.168.10.41 subnet mask: 255.255.255.248, default gateway: 192.168.10.46
- IP address: 192.168.10.254 subnet mask: 255.255.255.0, default gateway: 192.168.10.1

Explain:
Using a /29 prefix to subnet 192.168.10.0 results in subnets that increment by 8:
192.168.10.0 (1)
192.168.10.8 (2)
192.168.10.16 (3)
192.168.10.24 (4)
192.168.10.32 (5)

119. Refer to the exhibit. The switches are in their default configuration. Host A needs to communicate with host D, but host A does not have the MAC address for its default gateway. Which network hosts will receive the ARP request sent by host

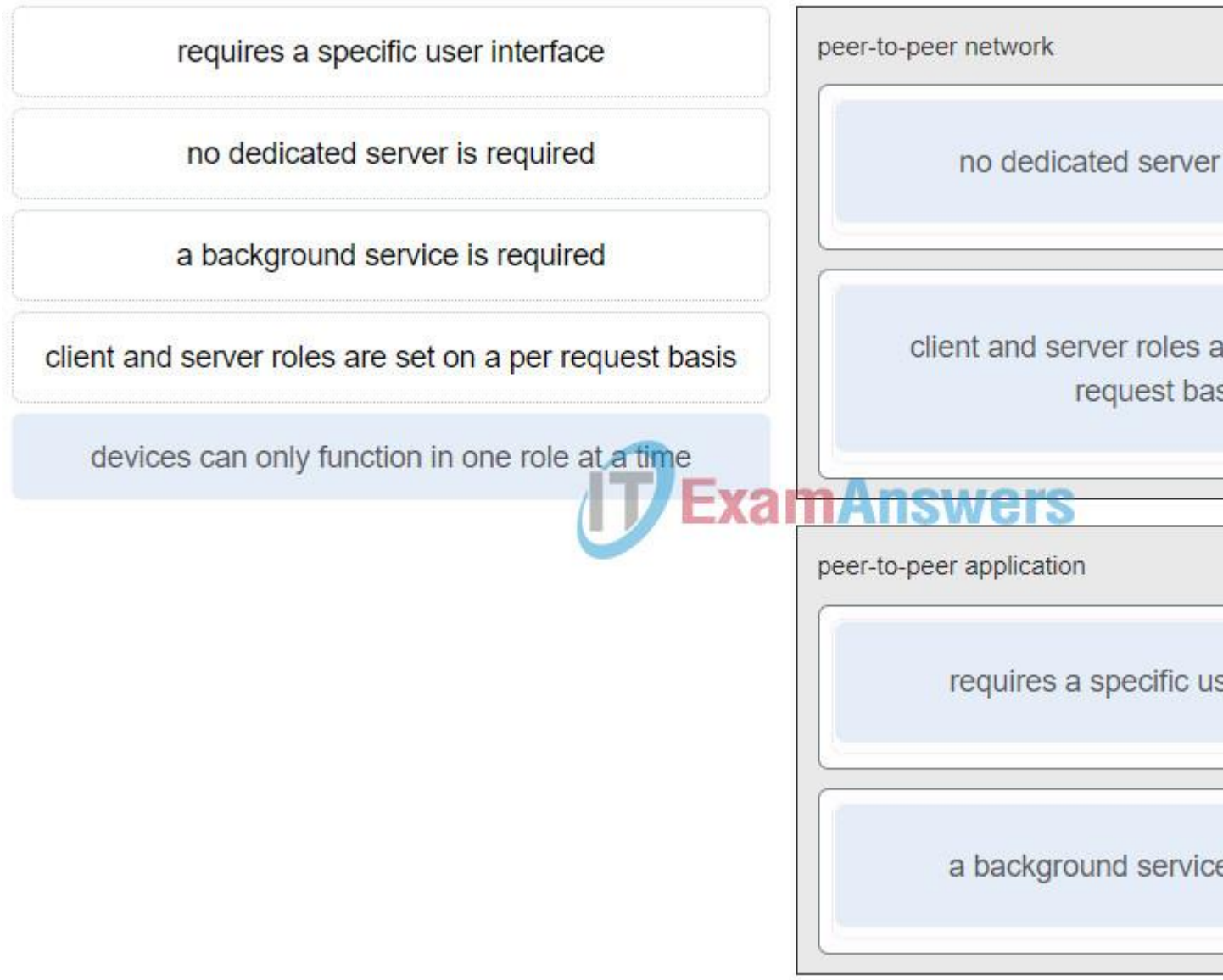
A?



- only host D
- only router R1
- only hosts A, B, and C
- only hosts A, B, C, and D
- only hosts B and C
- **only hosts B, C, and router R1**

Explain:
Since host A does not have the MAC address of the default gateway in its ARP table, host A sends an ARP broadcast. The ARP broadcast would be sent to every device on the local network. Hosts B, C, and router R1 would receive the broadcast. Router R1 would not forward the message.

120. Match a statement to the related network model. (Not all options are used.)

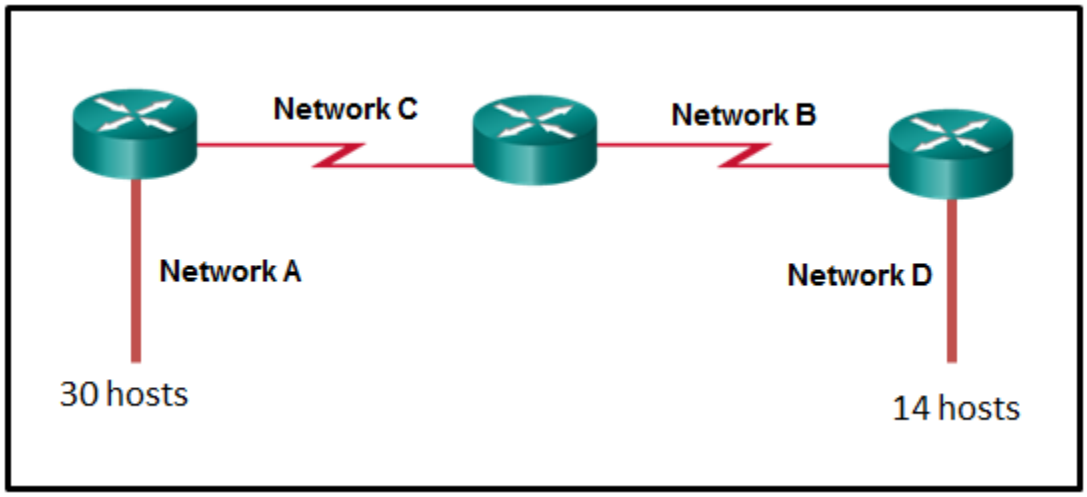


ITN (Version 7.00) – ITNv7 Final Exam

Place the options in the following order:peer-to-peer network
[+] no dedicated server is required
[+] client and server roles are set on a per request basis
peer-to-peer aplication
[#] requires a specific user interface
[#] a background service is required

Explain:
Peer-to-peer networks do not require the use of a dedicated server, and devices can assume both client and server roles simultaneously on a per request basis. Because they do not require formalized accounts or permissions, they are best used in limited situations. Peer-to-peer applications require a user interface and background service to be running, and can be used in more diverse situations.

121. Refer to the exhibit. A network engineer has been given the network address of 192.168.99.0 and a subnet mask of 255.255.255.192 to subnet across the four networks shown. How many total host addresses are unused across all four subnets?



- 88
- **200**
- 72
- 224
- 158

122. Which connector is used with twisted-pair cabling in an Ethernet LAN?

LC conector

SC conector

BNC

RJ 11

True Answer:

RJ 45 (true answer)

123. A client packet is received by a server. The packet has a destination port number of 22. What service is the client requesting?

- **SSH**
- SMB/CIFS
- HTTPS
- SLP

124. What characteristic describes an IPS?

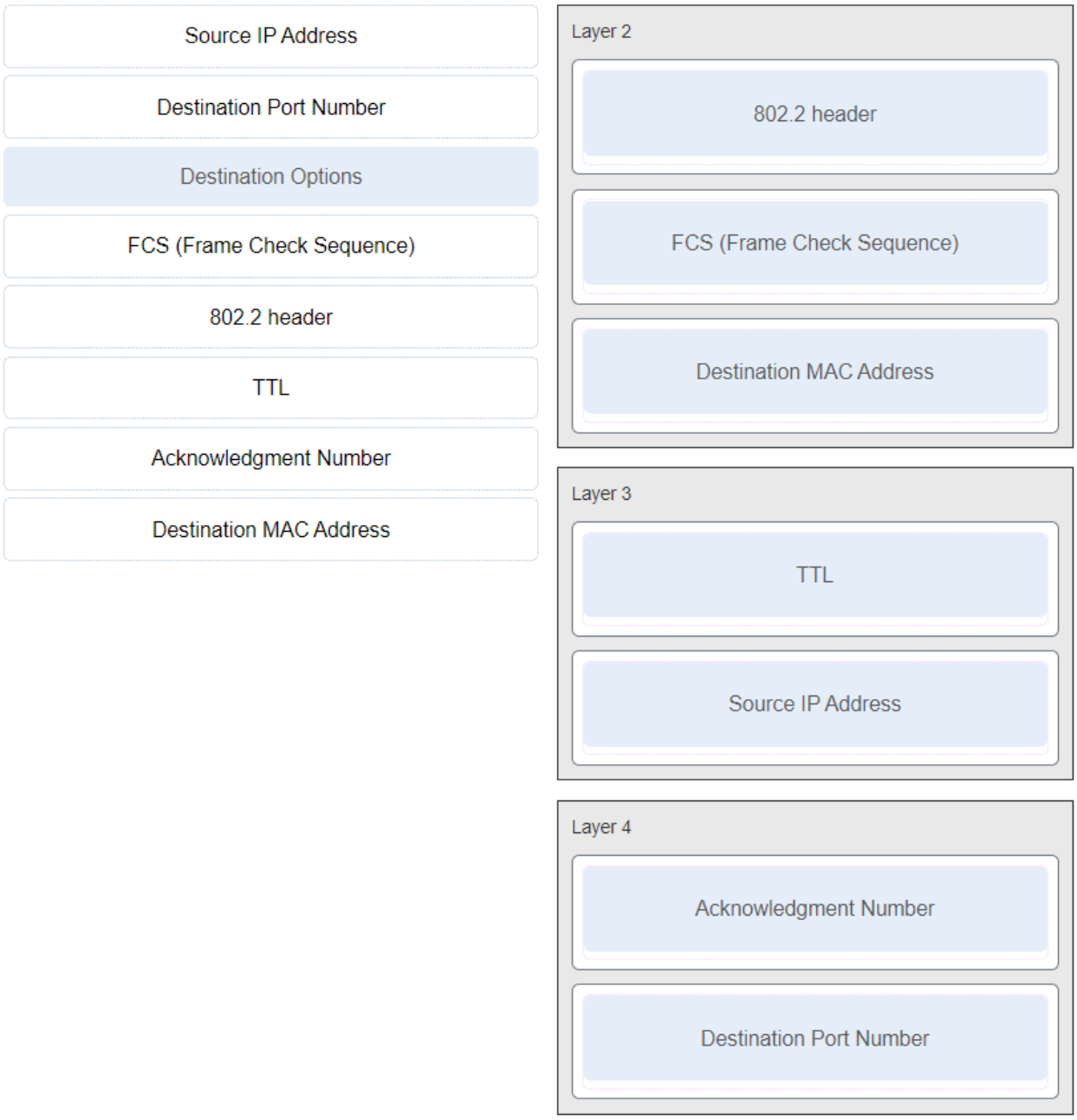
- a tunneling protocol that provides remote users with secure access into the network of an organization
- **a network device that filters access and traffic coming into a network**
- software that identifies fast-spreading threats
- software on a router that filters traffic based on IP addresses or applications

Explanation: IPS – An intrusion prevention system (IPS) monitors incoming and outgoing traffic looking for malware, network attack signatures, and more. If it recognizes a threat, it can immediately stop it.

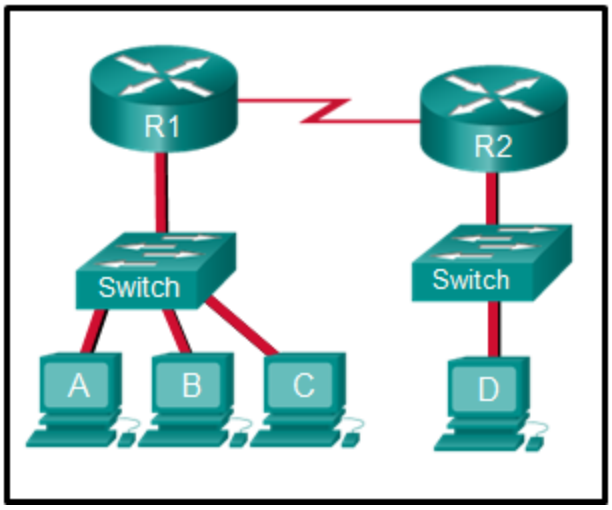
125. What service is provided by DHCP?

- An application that allows real-time chatting among remote users.
- Allows remote access to network devices and servers.
- **Dynamically assigns IP addresses to end and intermediary devices.**
- Uses encryption to provide secure remote access to network devices and servers.

126. Match the header field with the appropriate layer of the OSI model. (Not all options are used.)



127. Refer to the exhibit. The switches have a default configuration. Host A needs to communicate with host D, but host A does not have the MAC address for the default gateway. Which network devices will receive the ARP request sent by host A?



i360201v3n1_275353.png

- only host D
- only hosts A, B, C, and D
- only hosts B and C
- **only hosts B, C, and router R1**
- only hosts A, B, and C
- only router R1

Explanation: Because host A does not have the MAC address of the default gateway in the ARP table, host A sends an ARP broadcast. The ARP broadcast would be sent to every device on the local network. Hosts B, C, and router R1 would receive the broadcast. Router R1 would not forward the message.

128. Which wireless technology has low-power and low-data rate requirements making it popular in IoT environments?

- Bluetooth
- **Zigbee**
- WiMAX
- Wi-Fi

Explanation: Zigbee is a specification used for low-data rate, low-power communications. It is intended for applications that require short-range, low data-rates and long battery life. Zigbee is typically used for industrial and Internet of Things (IoT) environments such as wireless light switches and medical device data collection.

129. What two ICMPv6 message types must be permitted through IPv6 access control lists to allow resolution of Layer 3 addresses to Layer 2 MAC addresses? (Choose two.)

- **neighbor solicitations**
- echo requests
- **neighbor advertisements**
- echo replies

- router solicitations
- router advertisements

130. A client is using SLAAC to obtain an IPv6 address for its interface. After an address has been generated and applied to the interface, what must the client do before it can begin to use this IPv6 address?

- It must send a DHCPv6 INFORMATION-REQUEST message to request the address of the DNS server.
- It must send a DHCPv6 REQUEST message to the DHCPv6 server to request permission to use this address.
- It must send an ICMPv6 Router Solicitation message to determine what default gateway it should use.
- **It must send an ICMPv6 Neighbor Solicitation message to ensure that the address is not already in use on the network.**

131. Two pings were issued from a host on a local network. The first ping was issued to the IP address of the default gateway of the host and it failed. The second ping was issued to the IP address of a host outside the local network and it was successful. What is a possible cause for the failed ping?

- The default gateway is not operational.
- The default gateway device is configured with the wrong IP address.
- **Security rules are applied to the default gateway device, preventing it from processing ping requests.**
- The TCP/IP stack on the default gateway is not working properly.

132. An organization is assigned an IPv6 address block of 2001:db8:0:ca00::/56. How many subnets can be created without using bits in the interface ID space?

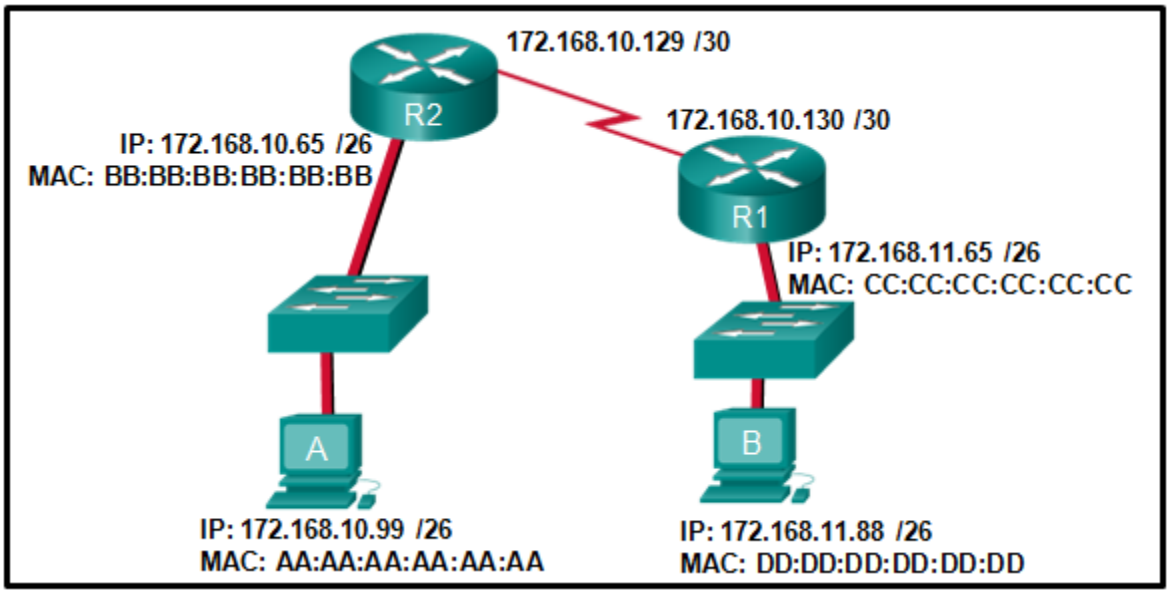
- **256**
- 512
- 1024
- 4096

133. What subnet mask is needed if an IPv4 network has 40 devices that need IP addresses and address space is not to be wasted?

- 255.255.255.0
- 255.255.255.240
- 255.255.255.128
- **255.255.255.192**
- 255.255.255.224

Explanation: In order to accommodate 40 devices, 6 host bits are needed. With 6 bits, 64 addresses are possible, but one address is for the subnet number and one address is for a broadcast. This leaves 62 addresses that can be assigned to network devices. The mask associated with leaving 6 host bits for addressing is 255.255.255.192.

134. Refer to the exhibit. If host A sends an IP packet to host B, what will the destination address be in the frame when it leaves host A?



- DD:DD:DD:DD:DD:DD
- 172.168.10.99
- CC:CC:CC:CC:CC:CC
- 172.168.10.65
- **BB:BB:BB:BB:BB:BB**
- AA:AA:AA:AA:AA:AA

Explain:
When a host sends information to a distant network, the Layer 2 frame header will contain a source and destination MAC address. The source address will be the originating host device. The destination address will be the router interface that connects to the same network. In the case of host A sending information to host B, the source address is AA:AA:AA:AA:AA:AA and the destination address is the MAC address assigned to the R2 Ethernet interface, BB:BB:BB:BB:BB:BB.

135. What is a benefit of using cloud computing in networking?

- Technology is integrated into every-day appliances allowing them to interconnect with other devices, making them more 'smart' or automated.
- **Network capabilities are extended without requiring investment in new infrastructure, personnel, or software.**
- End users have the freedom to use personal tools to access information and communicate across a business network.
- Home networking uses existing electrical wiring to connect devices to the network wherever there is an electrical outlet, saving the cost of installing data cables.

Explanation: Cloud computing extends IT's capabilities without requiring investment in new infrastructure, training new personnel, or licensing new software. These services are available on-demand and delivered economically to any device anywhere in the world without compromising security or function.

BYOD is about end users having the freedom to use personal tools to access information and communicate across a business or campus network. Smart home technology is integrated into every-day appliances allowing them to interconnect with other devices, making them more 'smart' or automated. Powerline networking is a trend for home networking that uses existing electrical wiring to connect devices to the network wherever there is an electrical outlet, saving the cost of installing data cables.

136. Which two statements are correct about MAC and IP addresses during data transmission if NAT is not involved? (Choose two.)

- **Destination IP addresses in a packet header remain constant along the entire path to a target host.**
- Destination MAC addresses will never change in a frame that goes across seven routers.
- Every time a frame is encapsulated with a new destination MAC address, a new destination IP address is needed.
- **Destination and source MAC addresses have local significance and change every time a frame goes from one LAN to another.**
- A packet that has crossed four routers has changed the destination IP address four times.

137. What is one main characteristic of the data link layer?

- It generates the electrical or optical signals that represent the 1 and 0 on the media.
- It converts a stream of data bits into a predefined code.
- **It shields the upper layer protocol from being aware of the physical medium to be used in the communication.**
- It accepts Layer 3 packets and decides the path by which to forward the packet to a remote network.

138. What are three characteristics of the CSMA/CD process? (Choose three.)

- The device with the electronic token is the only one that can transmit after a collision.
- **A device listens and waits until the media is not busy before transmitting.**
- **After detecting a collision, hosts can attempt to resume transmission after a random time delay has expired.**
- **All of the devices on a segment see data that passes on the network medium.**
- A jam signal indicates that the collision has cleared and the media is not busy.
- Devices can be configured with a higher transmission priority.

Explanation: The Carrier Sense Multiple Access/Collision Detection (CSMA/CD) process is a contention-based media access control mechanism used on shared media access networks, such as Ethernet. When a device needs to transmit data, it listens and waits until the media is available (quiet), then it will send data. If two devices transmit at the same time, a collision will occur. Both devices will

detect the collision on the network. When a device detects a collision, it will stop the data transmission process, wait for a random amount of time, then try again.

139. Which information does the show startup-config command display?

- the IOS image copied into RAM
- the bootstrap program in the ROM
- the contents of the current running configuration file in the RAM
- **the contents of the saved configuration file in the NVRAM**

Explain:
The show startup-config command displays the saved configuration located in NVRAM. The show running-config command displays the contents of the currently running configuration file located in RAM.

140. Which two commands can be used on a Windows host to display the routing table? (Choose two.)

- netstat -s
- **route print**
- show ip route
- **netstat -r**
- tracert

Explain:
On a Windows host, the route print or netstat -r commands can be used to display the host routing table. Both commands generate the same output. On a router, the show ip route command is used to display the routing table. The netstat –s command is used to display per-protocol statistics. The tracert command is used to display the path that a packet travels to its destination.

141. What are two functions that are provided by the network layer? (Choose two.)

- **directing data packets to destination hosts on other networks**
- placing data on the network medium
- carrying data between processes that are running on source and destination hosts
- providing dedicated end-to-end connections
- **providing end devices with a unique network identifier**

Explanation: The network layer is primarily concerned with passing data from a source to a destination on another network. IP addresses supply unique identifiers for the source and destination. The network layer provides connectionless, best-effort delivery. Devices rely on higher layers to supply services to processes.

142. Which two statements describe features of an IPv4 routing table on a router? (Choose two.)

- Directly connected interfaces will have two route source codes in the routing table: C and S .

- If there are two or more possible routes to the same destination, the route associated with the higher metric value is included in the routing table.
- The netstat -r command can be used to display the routing table of a router.
- The routing table lists the MAC addresses of each active interface.
- **It stores information about routes derived from the active router interfaces.**
- **If a default static route is configured in the router, an entry will be included in the routing table with source code S .**

Explanation: The **show ip route** command is used to display the routing table of the router. In IPv4, directly connected interfaces will have one source code:**C**. The routing table stores information about directly connected routes and remote routes. An entry in the routing table with a source code of **S** is included if a default static route is configured on the router.

143. What characteristic describes a VPN?

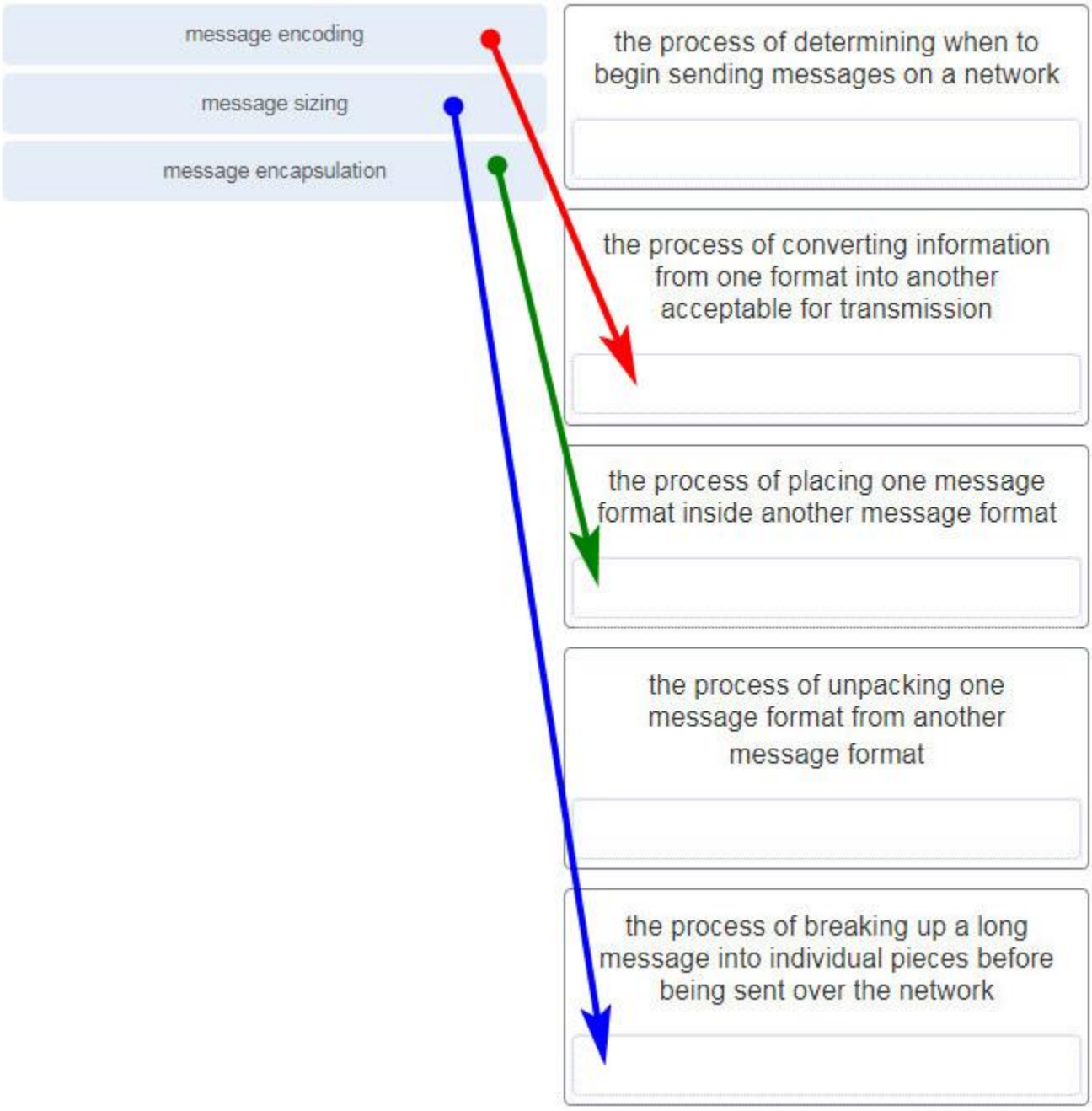
- software on a router that filters traffic based on IP addresses or applications
- software that identifies fast-spreading threats
- **a tunneling protocol that provides remote users with secure access into the network of an organization**
- a network device that filters access and traffic coming into a network

144. Why would a Layer 2 switch need an IP address?

- to enable the switch to send broadcast frames to attached PCs
- to enable the switch to function as a default gateway
- **to enable the switch to be managed remotely**
- to enable the switch to receive frames from attached PCs

Explanation: A switch, as a Layer 2 device, does not need an IP address to transmit frames to attached devices. However, when a switch is accessed remotely through the network, it must have a Layer 3 address. The IP address must be applied to a virtual interface rather than to a physical interface. Routers, not switches, function as default gateways.

145. Match each description to its corresponding term. (Not all options are used.)



146. A user sends an HTTP request to a web server on a remote network. During encapsulation for this request, what information is added to the address field of a frame to indicate the destination?

- the network domain of the destination host
- the IP address of the default gateway
- the MAC address of the destination host
- **the MAC address of the default gateway**

Explanation: A frame is encapsulated with source and destination MAC addresses. The source device will not know the MAC address of the remote host. An ARP request will be sent by the source and will be responded to by the router. The router will respond with the MAC address of its interface, the one which is connected to the same network as the source.

147. What is an advantage to using a protocol that is defined by an open standard?

- A company can monopolize the market.
- The protocol can only be run on equipment from a specific vendor.
- An open standard protocol is not controlled or regulated by standards organizations.
- **It encourages competition and promotes choices.**

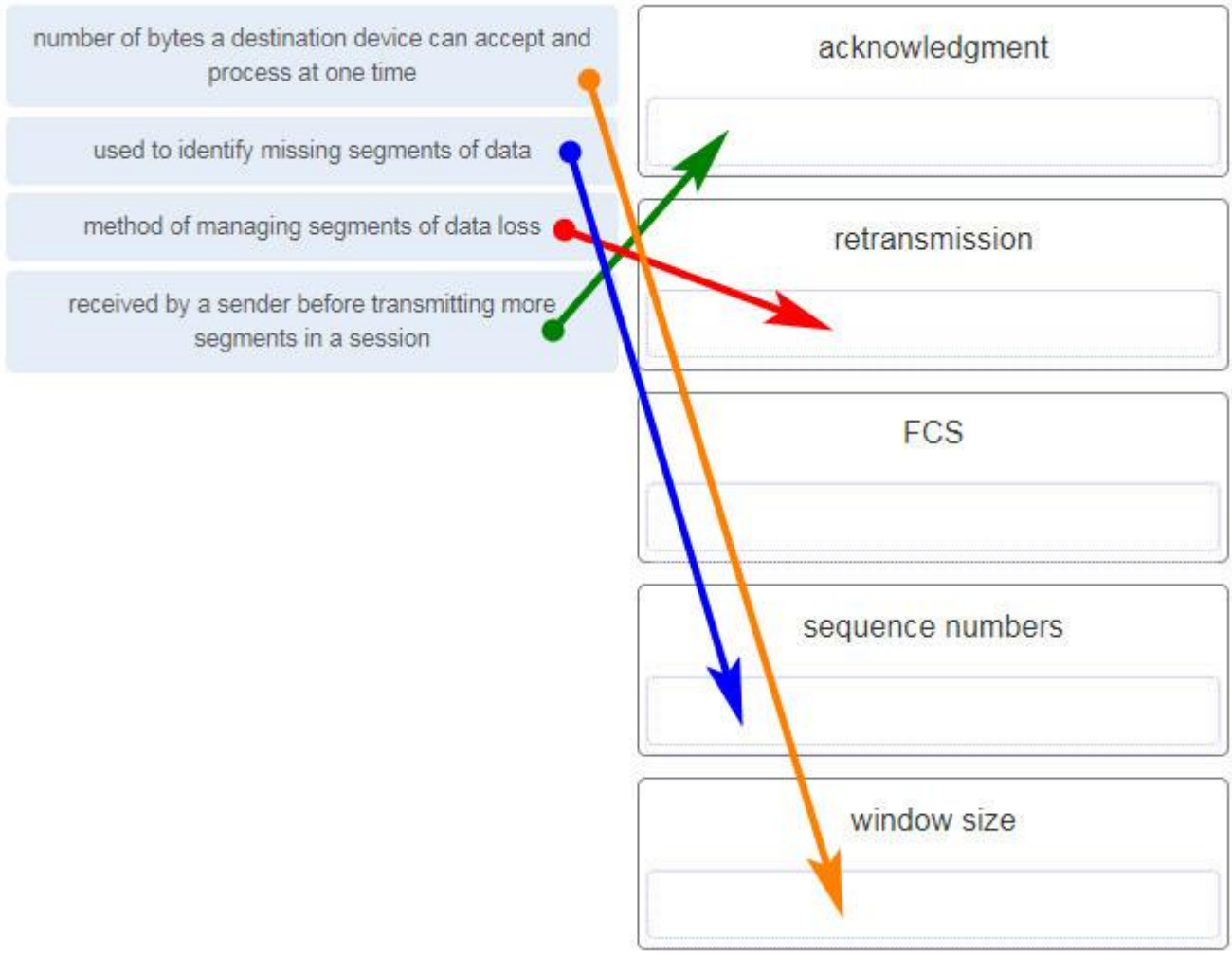
Explain:
A monopoly by one company is not a good idea from a user point of view. If a protocol can only be run on one brand, it makes it difficult to have mixed equipment in a network. A proprietary protocol is not free to use. An open standard protocol will in general be implemented by a wide range of vendors.

148. Data is being sent from a source PC to a destination server. Which three statements correctly describe the function of TCP or UDP in this situation? (Choose three.)

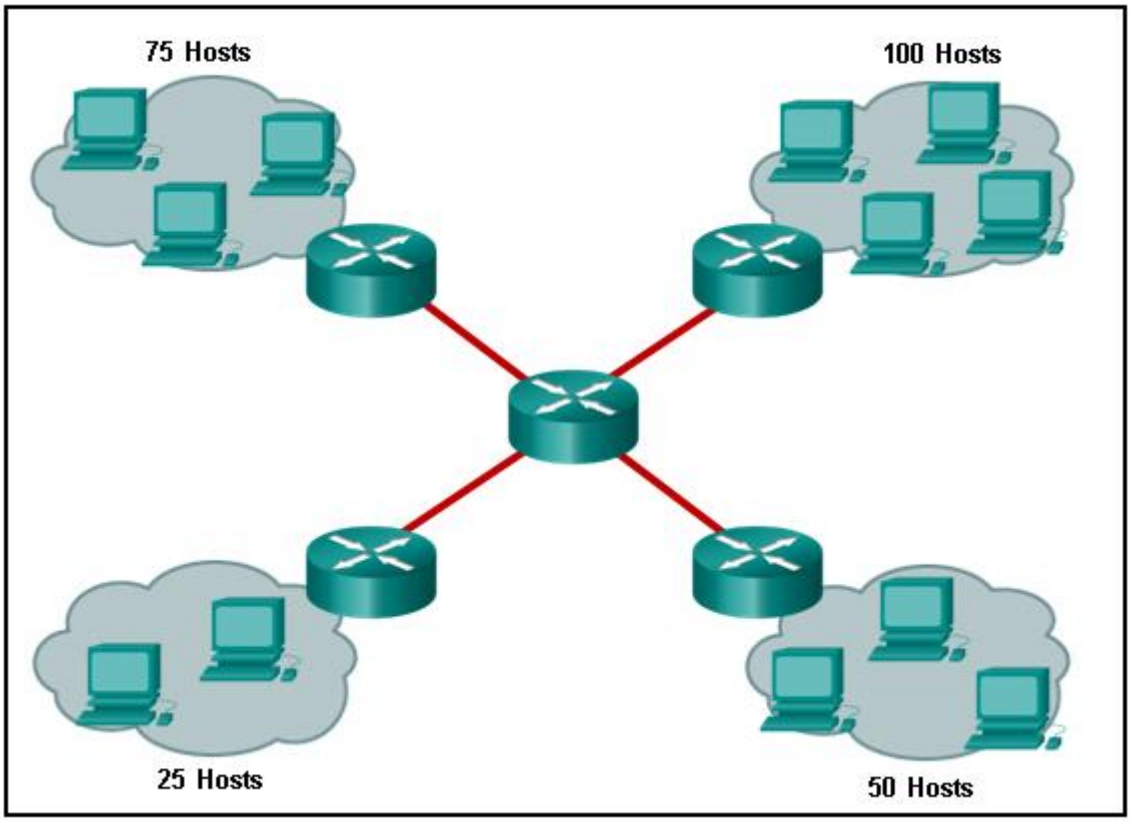
- **The source port field identifies the running application or service that will handle data returning to the PC.**
- The TCP process running on the PC randomly selects the destination port when establishing a session with the server.
- **UDP segments are encapsulated within IP packets for transport across the network.**
- **The UDP destination port number identifies the application or service on the server which will handle the data.**
- TCP is the preferred protocol when a function requires lower network overhead.
- The TCP source port number identifies the sending host on the network.

Explanation: Layer 4 port numbers identify the application or service which will handle the data. The source port number is added by the sending device and will be the destination port number when the requested information is returned. Layer 4 segments are encapsulated within IP packets. UDP, not TCP, is used when low overhead is needed. A source IP address, not a TCP source port number, identifies the sending host on the network. Destination port numbers are specific ports that a server application or service monitors for requests.

149. Match each description with the corresponding TCP mechanism. (Not all options are used.)



150. Refer to the exhibit. A company uses the address block of 128.107.0.0/16 for its network. What subnet mask would provide the maximum number of equal size subnets while providing enough host addresses for each subnet in the exhibit?



- 255.255.255.192
- 255.255.255.0
- **255.255.255.128**
- 255.255.255.240
- 255.255.255.224

Explanation: The largest subnet in the topology has 100 hosts in it so the subnet mask must have at least 7 host bits in it (27-2=126). 255.255.255.0 has 8 hosts bits, but this does not meet the requirement of providing the maximum number of subnets.

151. A network administrator wants to have the same subnet mask for three subnetworks at a small site. The site has the following networks and numbers of devices:

```
Subnetwork A: IP phones - 10 addresses

Subnetwork B: PCs - 8 addresses

Subnetwork C: Printers - 2 addresses
```

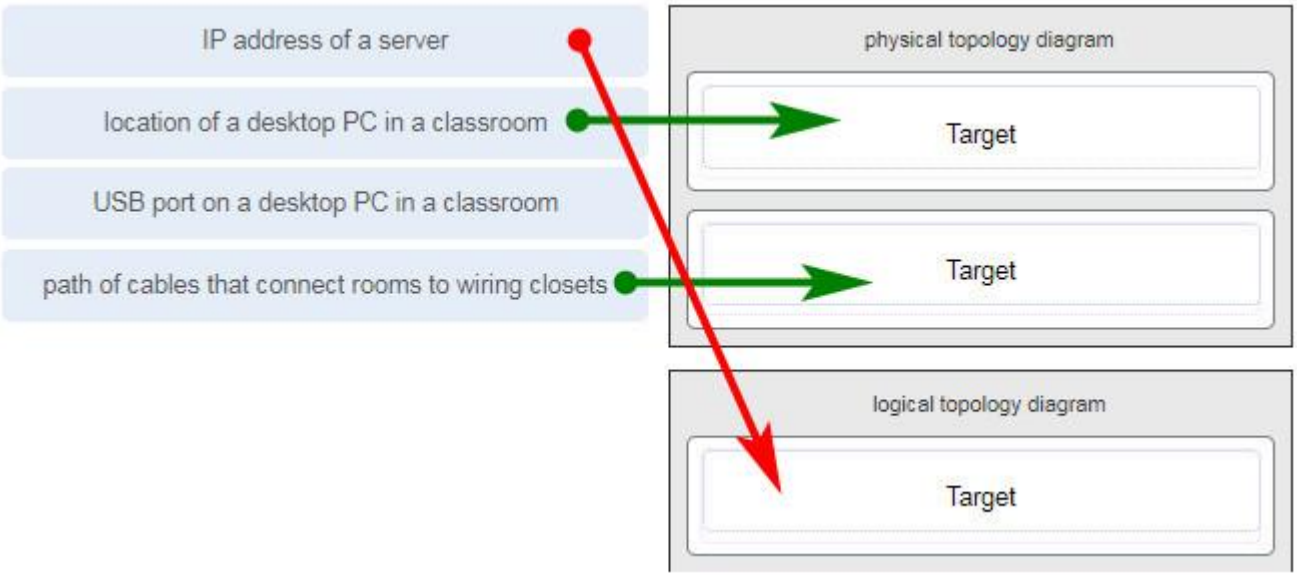
What single subnet mask would be appropriate to use for the three subnetworks?

- 255.255.255.0

- **255.255.255.240**
- 255.255.255.248
- 255.255.255.252

Explain:
If the same mask is to be used, then the network with the most hosts must be examined for number of hosts. Because this is 10 hosts, 4 host bits are needed. The /28 or 255.255.255.240 subnet mask would be appropriate to use for these networks.

152. Match each item to the type of topology diagram on which it is typically identified. (Not all options are used.)



153. What two pieces of information are displayed in the output of the show ip interface brief command? (Choose two.)

- **IP addresses**
- interface descriptions
- MAC addresses
- next-hop addresses
- **Layer 1 statuses**
- speed and duplex settings

Explanation: The command show ip interface brief shows the IP address of each interface, as well as the operational status of the interfaces at both Layer 1 and Layer 2. In order to see interface descriptions and speed and duplex settings, use the command show running-config interface. Next-hop addresses are displayed in the routing table with the command show ip route, and the MAC address of an interface can be seen with the command show interfaces.

154. A user is complaining that an external web page is taking longer than normal to load.The web page does eventually load on the user machine. Which tool should

the technician use with administrator privileges in order to locate where the issue is in the network?

- ping
- nslookup
- **tracert**
- ipconfig /displaydns

Explanation: The Command Prompt command tracert will map the path from the PC to the web server and measure transit delays of packets across the network.

155. Which value, that is contained in an IPv4 header field, is decremented by each router that receives a packet?

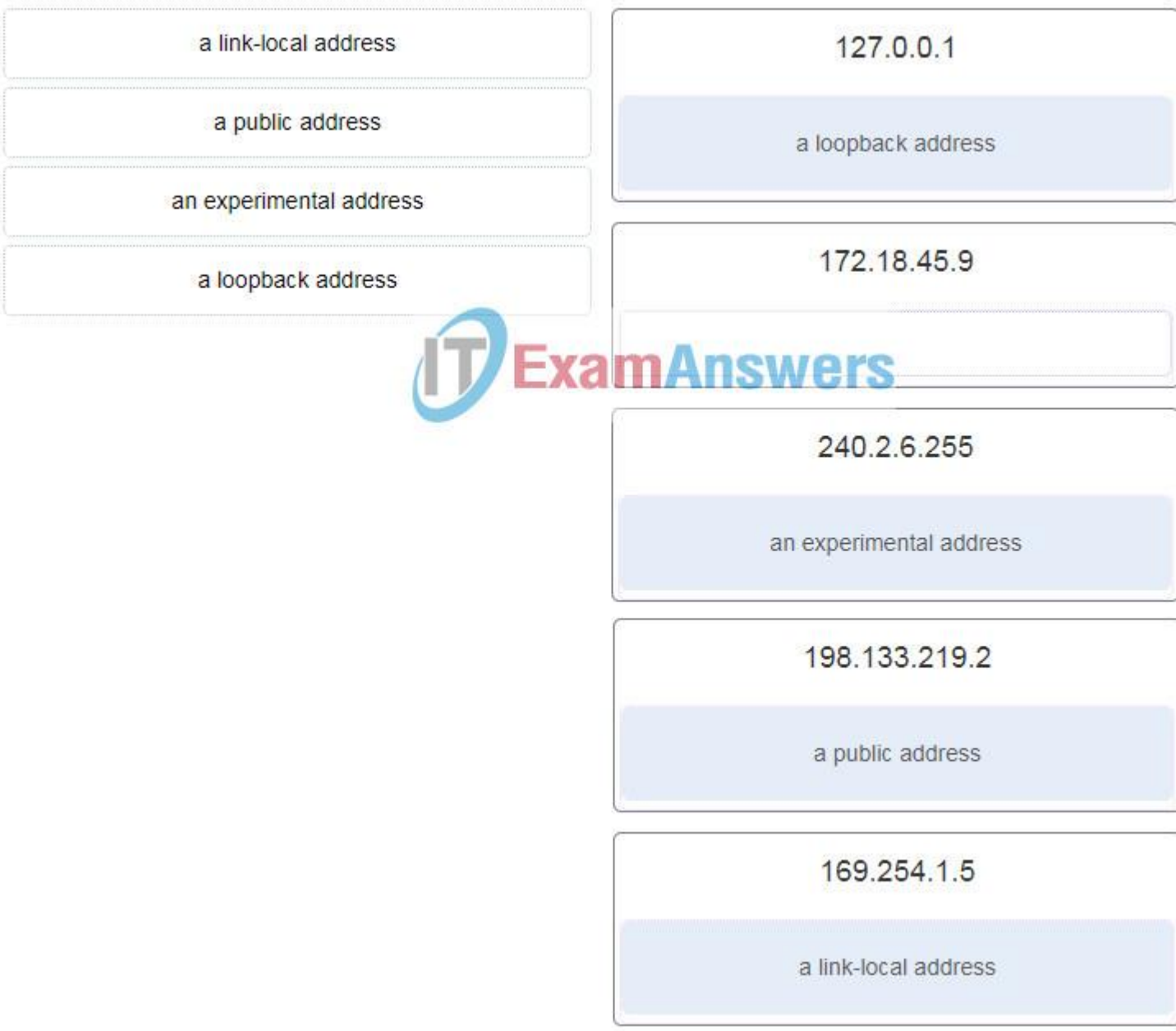
- Header Length
- Differentiated Services
- **Time-to-Live**
- Fragment Offset

Explanation: When a router receives a packet, the router will decrement the Time-to-Live (TTL) field by one. When the field reaches zero, the receiving router will discard the packet and will send an ICMP Time Exceeded message to the sender.

156. A network technician is researching the use of fiber optic cabling in a new technology center. Which two issues should be considered before implementing fiber optic media? (Choose two.)

- **Fiber optic cabling requires different termination and splicing expertise from what copper cabling requires.**
- Fiber optic cabling requires specific grounding to be immune to EMI.
- Fiber optic cabling is susceptible to loss of signal due to RFI.
- Fiber optic cable is able to withstand rough handling.
- **Fiber optic provides higher data capacity but is more expensive than copper cabling.**

157. Match each description with an appropriate IP address. (Not all options are used.)



158. A user is executing a tracert to a remote device. At what point would a router, which is in the path to the destination device, stop forwarding the packet?

- when the router receives an ICMP Time Exceeded message
- when the RTT value reaches zero
- when the host responds with an ICMP Echo Reply message
- **when the value in the TTL field reaches zero**
- when the values of both the Echo Request and Echo Reply messages reach zero

Explain:

When a router receives a traceroute packet, the value in the TTL field is

decremented by 1. When the value in the field reaches zero, the receiving router will not forward the packet, and will send an ICMP Time Exceeded message back to the source.

159. Users report that the network access is slow. After questioning the employees, the network administrator learned that one employee downloaded a third-party scanning program for the printer. What type of malware might be introduced that causes slow performance of the network?

- virus
- **worm**
- phishing
- spam

CCNA 2: Switching, Routing, and Wireless Essentials (Version 7.00) – SRWE Final Exam Answers

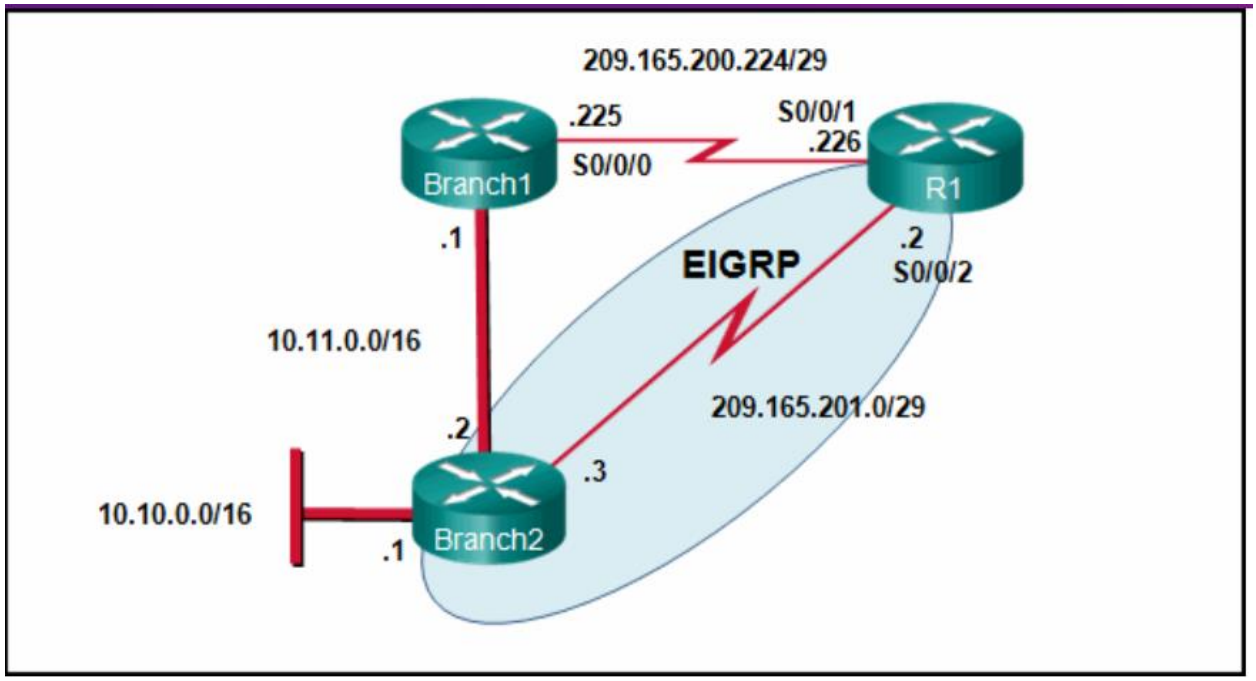
1. Refer to the exhibit. What will router R1 do with a packet that has a destination IPv6 address of 2001:db8:cafe:5::1?

```
R1# show ipv6 route

<output omitted>

S ::/0 [1/0]
via Serial0/0/0, directly connected
C 2001:DB8:CAFE:1::/64 [0/0]
via GigabitEthernet0/1, directly connected
L 2001:DB8:CAFE:1::1/128 [0/0]
via GigabitEthernet0/1, receive
C 2001:DB8:CAFE:2::/64 [0/0]
via GigabitEthernet0/0, directly connected
L 2001:DB8:CAFE:2::1/128 [0/0]
via GigabitEthernet0/0, receive
C 2001:DB8:CAFE:3::/64 [0/0]
via Serial0/0/0, directly connected
L 2001:DB8:CAFE:3::1/128 [0/0]
via Serial0/0/0, receive
S 2001:DB8:CAFE:4::1/128 [1/0]
via Serial0/0/0, directly connected
L FF00::/8 [0/0]
via Null0, receive
```

- forward the packet out GigabitEthernet0/0
- drop the packet
- forward the packet out GigabitEthernet0/1
- **forward the packet out Serial0/0/0**

Explanation: The route ::/0 is the compressed form of the 0000:0000:0000:0000:0000:0000:0000:0000/0 default route. The default route is used if a more specific route is not found in the routing table.

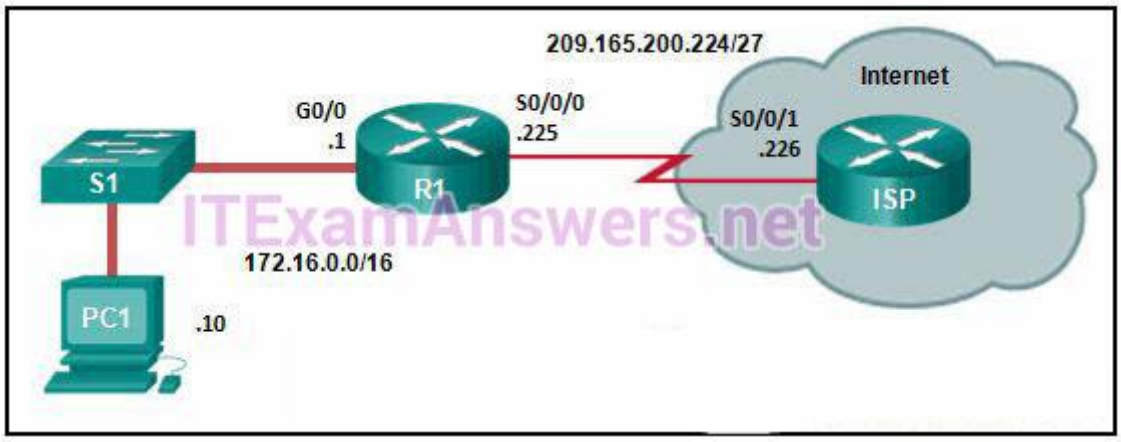
2. Refer to the exhibit. Currently router R1 uses an EIGRP route learned from Branch2 to reach the 10.10.0.0/16 network. Which floating static route would create a backup route to the 10.10.0.0/16 network in the event that the link between R1 and Branch2 goes down?



- ip route 10.10.0.0 255.255.0.0 Serial 0/0/0 100
- ip route 10.10.0.0 255.255.0.0 209.165.200.226 100
- **ip route 10.10.0.0 255.255.0.0 209.165.200.225 100**
- ip route 10.10.0.0 255.255.0.0 209.165.200.225 50

Explanation: A floating static route needs to have an administrative distance that is greater than the administrative distance of the active route in the routing table. Router R1 is using an EIGRP route which has an administrative distance of 90 to reach the 10.10.0.0/16 network. To be a backup route the floating static route must have an administrative distance greater than 90 and have a next hop address corresponding to the serial interface IP address of Branch1.

3. Refer to the exhibit. R1 was configured with the static route command ip route 209.165.200.224 255.255.255.224 S0/0/0 and consequently users on network 172.16.0.0/16 are unable to reach resources on the Internet. How should this static route be changed to allow user traffic from the LAN to reach the Internet?



- Add an administrative distance of 254.
- **Change the destination network and mask to 0.0.0.0 0.0.0.0**
- Change the exit interface to S0/0/1.
- Add the next-hop neighbor address of 209.165.200.226.

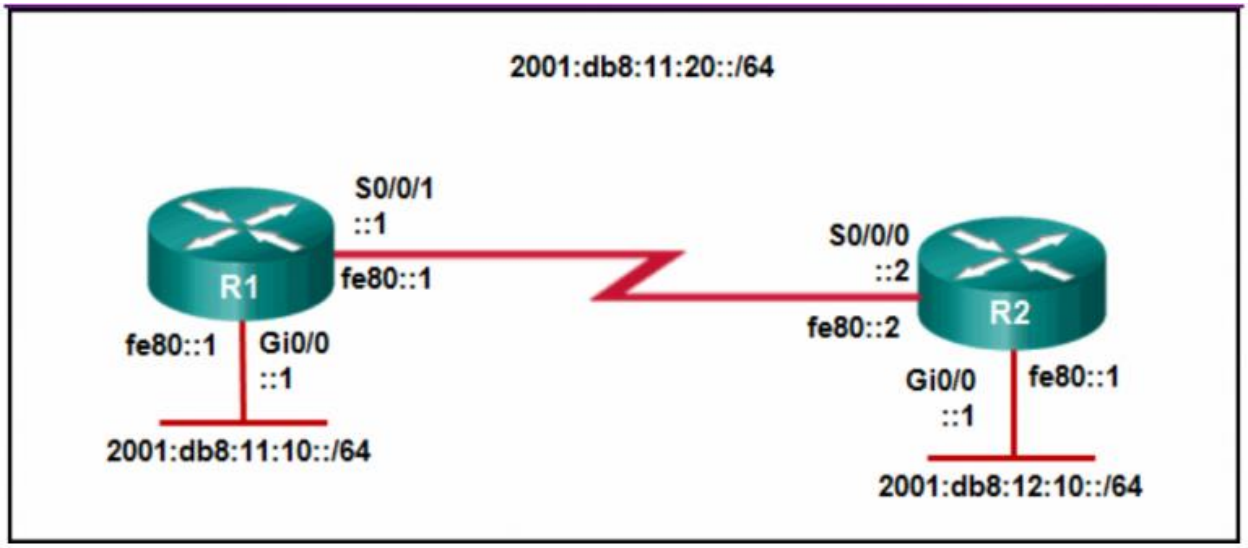
Explain: The static route on R1 has been incorrectly configured with the wrong destination network and mask. The correct destination network and mask is 0.0.0.0 0.0.0.0.

4. Which option shows a correctly configured IPv4 default static route?

- ip route 0.0.0.0 255.255.255.0 S0/0/0
- **ip route 0.0.0.0 0.0.0.0 S0/0/0**
- ip route 0.0.0.0 255.255.255.255 S0/0/0
- ip route 0.0.0.0 255.0.0.0 S0/0/0

Explanation: The static route ip route 0.0.0.0 0.0.0.0 S0/0/0 is considered a default static route and will match all destination networks.

5. Refer to the exhibit. Which static route command can be entered on R1 to forward traffic to the LAN connected to R2?



- ipv6 route 2001:db8:12:10::/64 S0/0/0
- **ipv6 route 2001:db8:12:10::/64 S0/0/1 fe80::2**
- ipv6 route 2001:db8:12:10::/64 S0/0/0 fe80::2
- ipv6 route 2001:db8:12:10::/64 S0/0/1 2001:db8:12:10::1

6. What is a method to launch a VLAN hopping attack?

- **introducing a rogue switch and enabling trunking**
- sending spoofed native VLAN information
- sending spoofed IP addresses from the attacking host
- flooding the switch with MAC addresses

7. A cybersecurity analyst is using the macof tool to evaluate configurations of switches deployed in the backbone network of an organization. Which type of LAN attack is the analyst targeting during this evaluation?

- VLAN hopping
- DHCP spoofing
- **MAC address table overflow**
- VLAN double-tagging

Explanation: Macof is a network attack tool and is mainly used to flood LAN switches with MAC addresses.

8. Refer to the exhibit. A network administrator is configuring a router as a DHCPv6 server. The administrator issues a show ipv6 dhcp pool command to verify the configuration. Which statement explains the reason that the number of active clients is 0?

```
R1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 dhcp pool ACAD_CLASS
R1(config-dhcp)# dns-server 2001:db8:acad:a1::10
R1(config-dhcp)# domain-name netacad.net
R1(config-dhcp)# exit
R1(config)# interface gigabitEthernet 0/0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# ipv6 dhcp server ACAD_CLASS
R1(config-if)# ipv6 nd other-config-flag
R1(config-if)# end
R1#
```



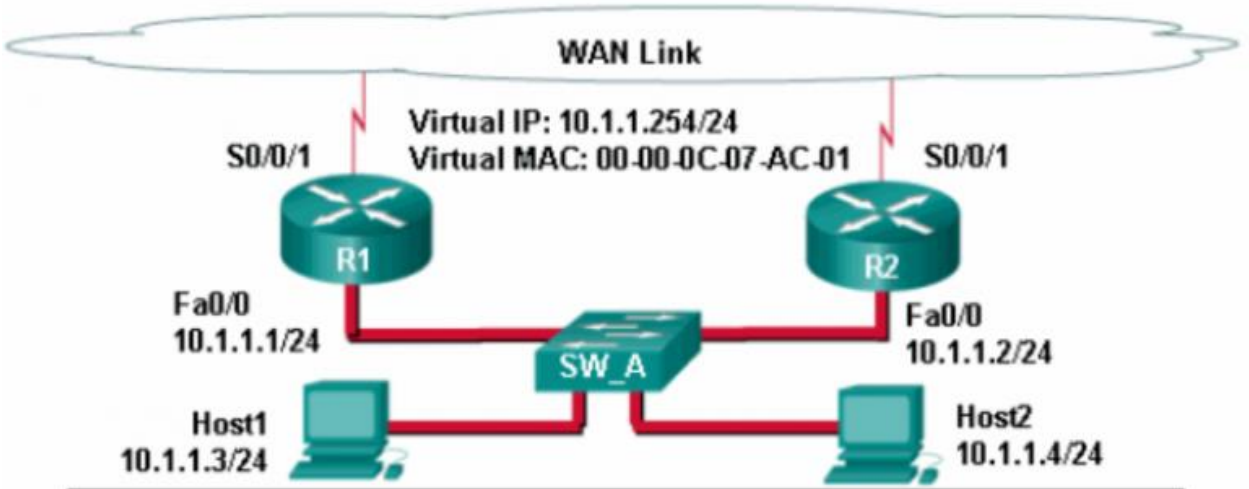
```
R1# show ipv6 dhcp pool
DHCPv6 pool: ACAD_CLASS
  DNS server: 2001:DB8:ACAD:A1::10
  Domain name: netacad.net
  Active clients: 0
R1#
```

- The default gateway address is not provided in the pool.
- No clients have communicated with the DHCPv6 server yet.
- The IPv6 DHCP pool configuration has no IPv6 address range specified.
- **The state is not maintained by the DHCPv6 server under stateless DHCPv6 operation.**

Explain:
Under the stateless DHCPv6 configuration, indicated by the command ipv6 nd other-config-flag, the DHCPv6 server does not maintain the state information, because client IPv6 addresses are not managed by the DHCP server. Because the clients will configure their IPv6 addresses by combining the prefix/prefix-length and a self-generated interface ID, the ipv6 dhcp pool configuration does not need to specify the valid IPv6 address range. And because clients will use

the link-local address of the router interface as the default gateway address, the default gateway address is not necessary.

9. Refer to the exhibit. A network administrator configured routers R1 and R2 as part of HSRP group 1. After the routers have been reloaded, a user on Host1 complained of lack of connectivity to the Internet The network administrator issued the show standby brief command on both routers to verify the HSRP operations. In addition, the administrator observed the ARP table on Host1. Which entry should be seen in the ARP table on Host1 in order to gain connectivity to the Internet?




```
R1 # show standby brief
Interface   Grp   Prio   P   State    Active      Standby     Virtual IP
Fa0/0       1     110    P   Active   local       10.1.1.2    10.1.1.254
```

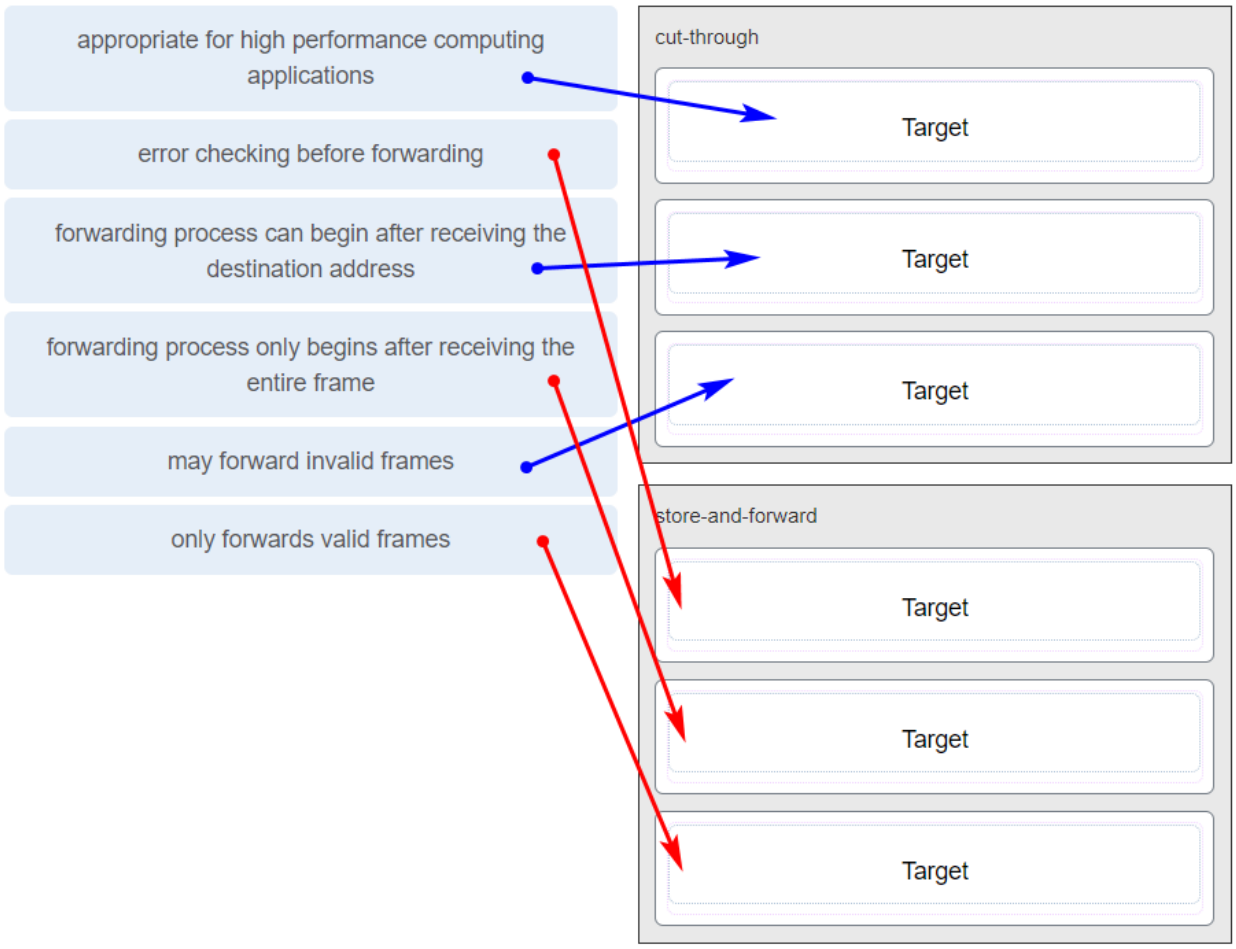
```
R2 # show standby brief
Interface   Grp   Prio   P   State    Active      Standby     Virtual IP
Fa0/0       1     100    P   Active   10.1.1.1    local       10.1.1.254
```

```
C:/ arp -a
Interface: 10.1.1.3 -----0x4
  Internet Address          Physical Address      Type
  10.1.1.2                  00-00-0c-ab-c0-d4     dynamic
```

- **the virtual IP address and the virtual MAC address for the HSRP group 1**
- the virtual IP address of the HSRP group 1 and the MAC address of R1
- the virtual IP address of the HSRP group 1 and the MAC address of R2
- the IP address and the MAC address of R1

Explanation: Hosts will send an ARP request to the default gateway which is the virtual IP address. ARP replies from the HSRP routers contain the virtual MAC address. The host ARP tables will contain a mapping of the virtual IP to the virtual MAC.

10. Match the forwarding characteristic to its type. (Not all options are used.)



Match the forwarding characteristic to its type. (Not all options are used.)

11. Which statement is correct about how a Layer 2 switch determines how to forward frames?

- **Frame forwarding decisions are based on MAC address and port mappings in the CAM table.**
- Only frames with a broadcast destination address are forwarded out all active switch ports.
- Unicast frames are always forwarded regardless of the destination MAC address.
- Cut-through frame forwarding ensures that invalid frames are always dropped.

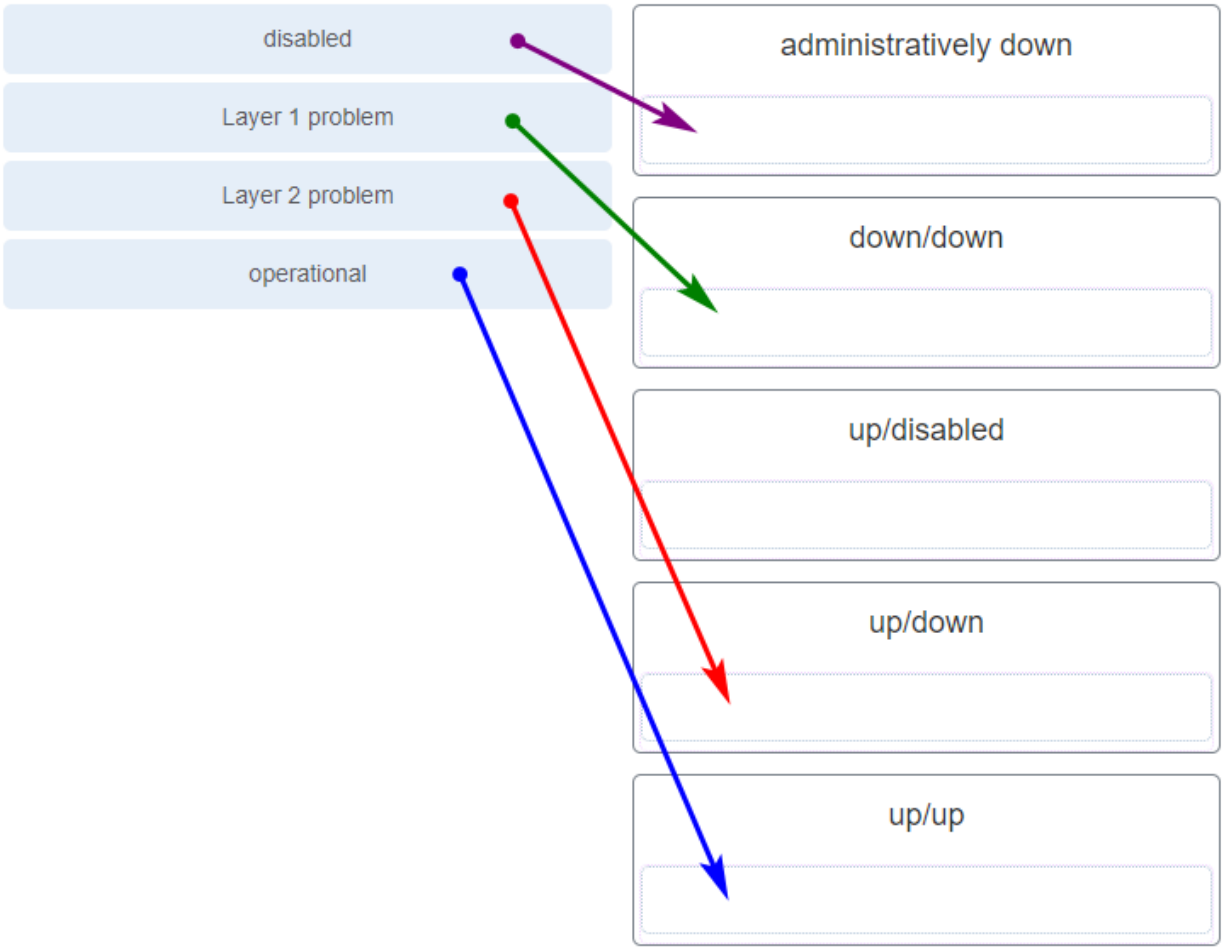
Explanation: Cut-through frame forwarding reads up to only the first 22 bytes of a frame, which excludes the frame check sequence and thus invalid frames may be forwarded. In addition to broadcast frames, frames with a destination MAC address that is not in the CAM are also flooded out all active ports. Unicast frames are not always forwarded. Received frames with a destination MAC address that is associated with the switch port on which it is received are not forwarded because the destination exists on the network segment connected to that port.

12. Which statement describes a result after multiple Cisco LAN switches are interconnected?

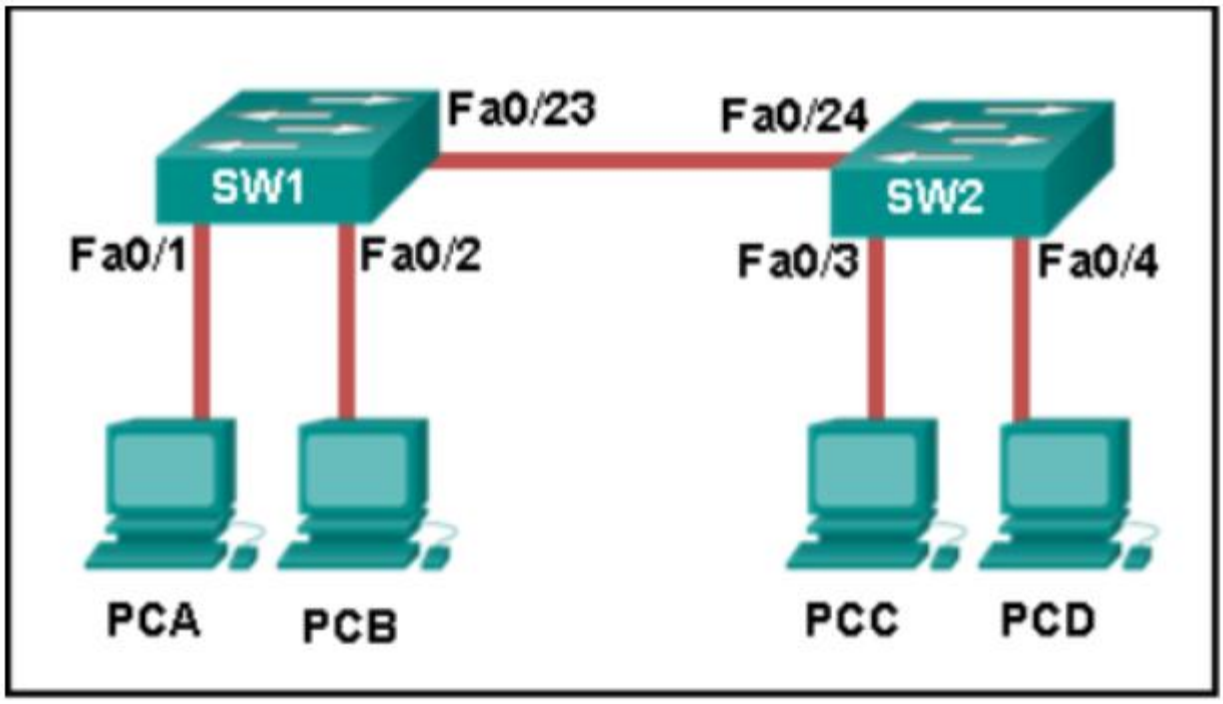
- **The broadcast domain expands to all switches.**
- One collision domain exists per switch.
- There is one broadcast domain and one collision domain per switch.
- Frame collisions increase on the segments connecting the switches.
- Unicast frames are always forwarded regardless of the destination MAC address.

Explanation: In Cisco LAN switches, the microsegmentation makes it possible for each port to represent a separate segment and thus each switch port represents a separate collision domain. This fact will not change when multiple switches are interconnected. However, LAN switches do not filter broadcast frames. A broadcast frame is flooded to all ports. Interconnected switches form one big broadcast domain.

13. Match the link state to the interface and protocol status. (Not all options are used.)



14.Refer to the exhibit. How is a frame sent from PCA forwarded to PCC if the MAC address table on switch SW1 is empty?



- SW1 forwards the frame directly to SW2. SW2 floods the frame to all ports connected to SW2, excluding the port through which the frame entered the switch.
- SW1 floods the frame on all ports on the switch, excluding the interconnected port to switch SW2 and the port through which the frame entered the switch.
- **SW1 floods the frame on all ports on SW1, excluding the port through which the frame entered the switch.**
- SW1 drops the frame because it does not know the destination MAC address.

Explanation: When a switch powers on, the MAC address table is empty. The switch builds the MAC address table by examining the source MAC address of incoming frames. The switch forwards based on the destination MAC address found in the frame header. If a switch has no entries in the MAC address table or if the destination MAC address is not in the switch table, the switch will forward the frame out all ports except the port that brought the frame into the switch.

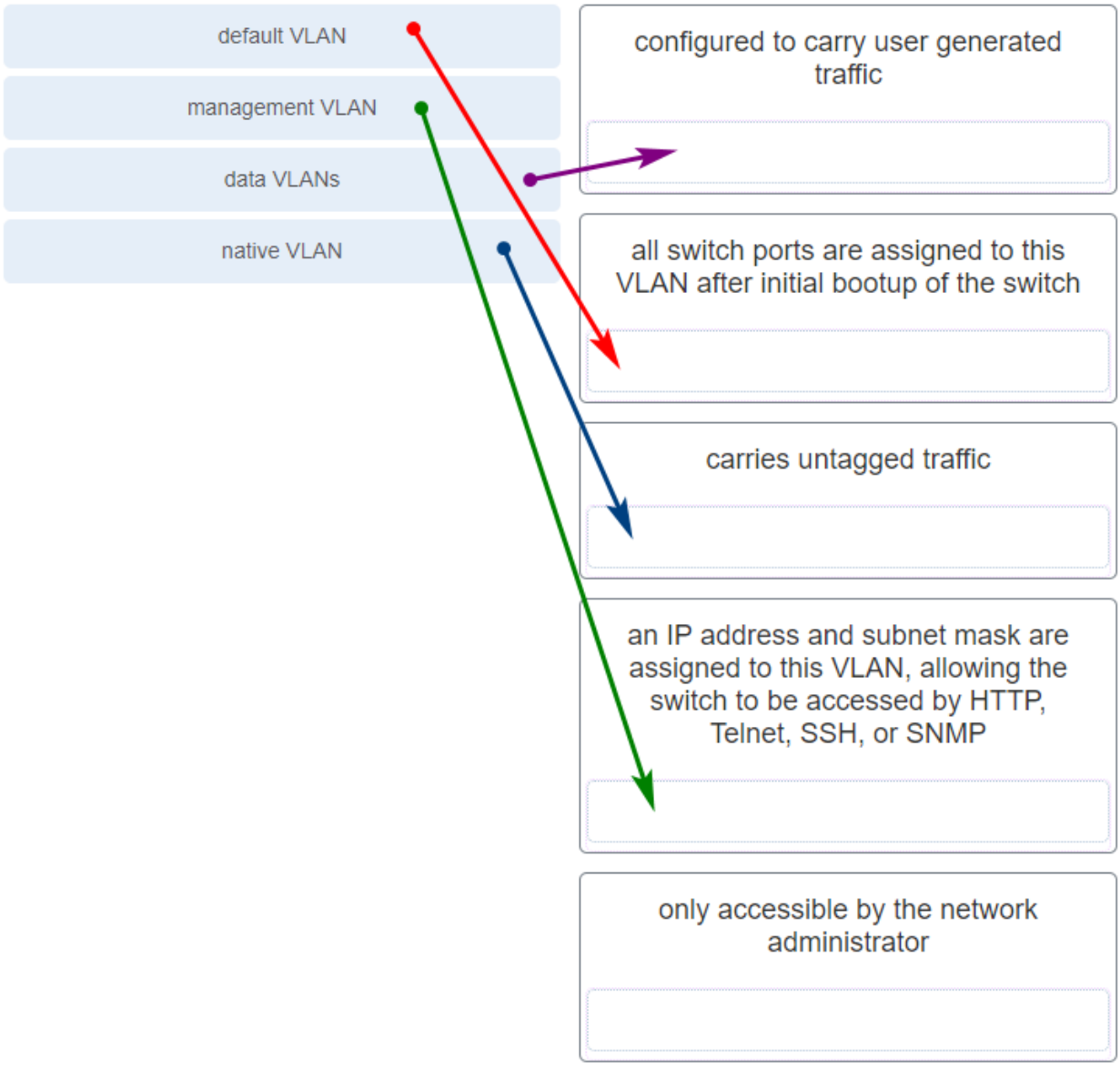
15. An administrator is trying to remove configurations from a switch. After using the command erase startup-config and reloading the switch, the administrator finds that VLANs 10 and 100 still exist on the switch. Why were these VLANs not removed?

- **Because these VLANs are stored in a file that is called vlan.dat that is located in flash memory, this file must be manually deleted.**
- These VLANs cannot be deleted unless the switch is in VTP client mode.
- These VLANs are default VLANs that cannot be removed.

- These VLANs can only be removed from the switch by using the no vlan 10 and no vlan 100 commands.

Explanation: Standard range VLANs (1-1005) are stored in a file that is called vlan.dat that is located in flash memory. Erasing the startup configuration and reloading a switch does not automatically remove these VLANs. The vlan.dat file must be manually deleted from flash memory and then the switch must be reloaded.

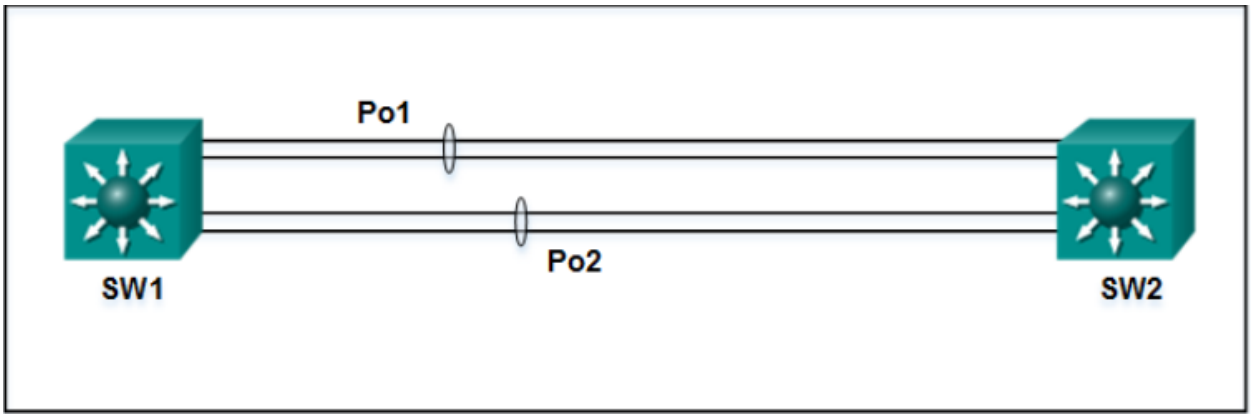
16. Match the description to the correct VLAN type. (Not all options are used.)



Explanation: A data VLAN is configured to carry user-generated traffic. A default VLAN is the VLAN where all switch ports belong after the initial boot up of a switch loading the default configuration. A native VLAN is assigned to an 802.1Q trunk port, and untagged traffic is placed on it. A management VLAN is any

VLAN that is configured to access the management capabilities of a switch. An IP address and subnet mask are assigned to it, allowing the switch to be managed via HTTP, Telnet, SSH, or SNMP.

17. Refer to the exhibit. A network administrator has connected two switches together using EtherChannel technology. If STP is running, what will be the end result?



- **STP will block one of the redundant links.**
- The switches will load balance and utilize both EtherChannels to forward packets.
- The resulting loop will create a broadcast storm.
- Both port channels will shutdown.

Explanation: Cisco switches support two protocols for negotiating a channel between two switches: LACP and PAgP. PAgP is Cisco-proprietary. In the topology shown, the switches are connected to each other using redundant links. By default, STP is enabled on switch devices. STP will block redundant links to prevent loops.

18. What is a secure configuration option for remote access to a network device?

- Configure an ACL and apply it to the VTY lines.
- Configure 802.1x.
- **Configure SSH.**
- Configure Telnet.

19. Which wireless encryption method is the most secure?

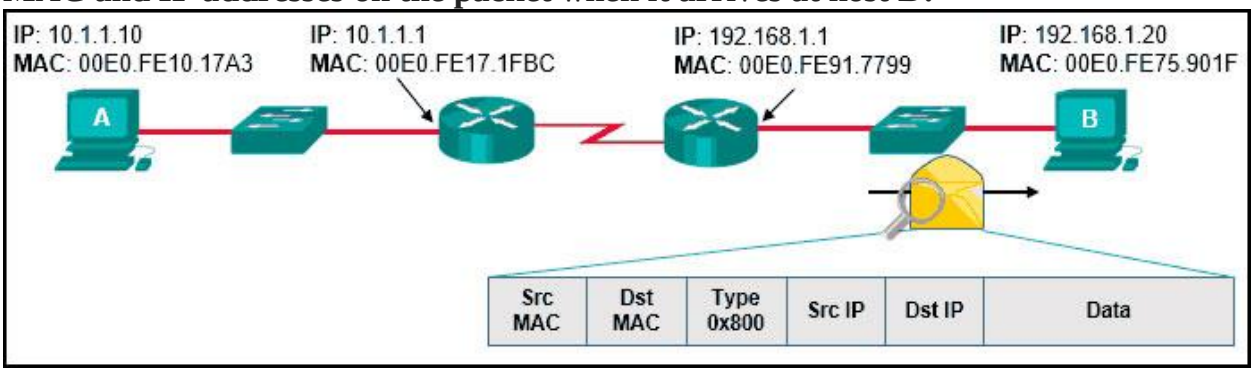
- **WPA2 with AES**
- WPA2 with TKIP
- WEP
- WPA

20. After attaching four PCs to the switch ports, configuring the SSID and setting authentication properties for a small office network, a technician successfully tests the connectivity of all PCs that are connected to the switch and WLAN. A firewall is then configured on the device prior to connecting it to the Internet. What type of network device includes all of the described features?

- firewall appliance

- **wireless router**
- switch
- standalone wireless access point

21. Refer to the exhibit. Host A has sent a packet to host B. What will be the source MAC and IP addresses on the packet when it arrives at host B?



CCNA 2 v7 Switching Routing and Wireless Essentials-Version-Final-Answers-21

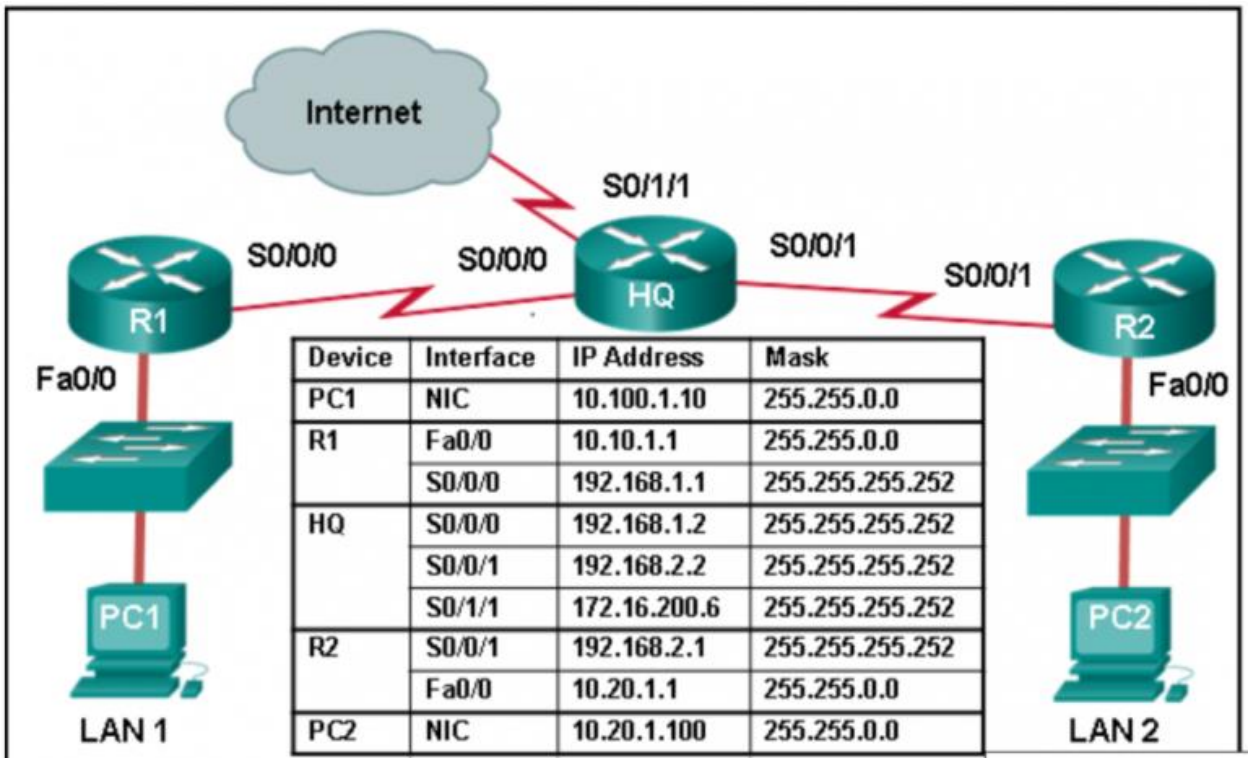
- **Source MAC: 00E0.FE91.7799**
  Source IP: 10.1.1.10
- Source MAC: 00E0.FE10.17A3
  Source IP: 10.1.1.10
- Source MAC: 00E0.FE10.17A3
  Source IP: 192.168.1.1
- Source MAC: 00E0.FE91.7799
  Source IP: 10.1.1.1
- Source MAC: 00E0.FE91.7799
  Source IP: 192.168.1.1

Explanation: As a packet traverses the network, the Layer 2 addresses will change at every hop as the packet is de-encapsulated and re-encapsulated, but the Layer 3 addresses will remain the same.

23. Refer to the exhibit. In addition to static routes directing traffic to networks 10.10.0.0/16 and 10.20.0.0/16, Router HQ is also configured with the following command:

```
ip route 0.0.0.0 0.0.0.0 serial 0/1/1
```

What is the purpose of this command?



Device	Interface	IP Address	Mask
PC1	NIC	10.100.1.10	255.255.0.0
R1	Fa0/0	10.10.1.1	255.255.0.0
	S0/0/0	192.168.1.1	255.255.255.252
HQ	S0/0/0	192.168.1.2	255.255.255.252
	S0/0/1	192.168.2.2	255.255.255.252
	S0/1/1	172.16.200.6	255.255.255.252
R2	S0/0/1	192.168.2.1	255.255.255.252
	Fa0/0	10.20.1.1	255.255.0.0
PC2	NIC	10.20.1.100	255.255.0.0

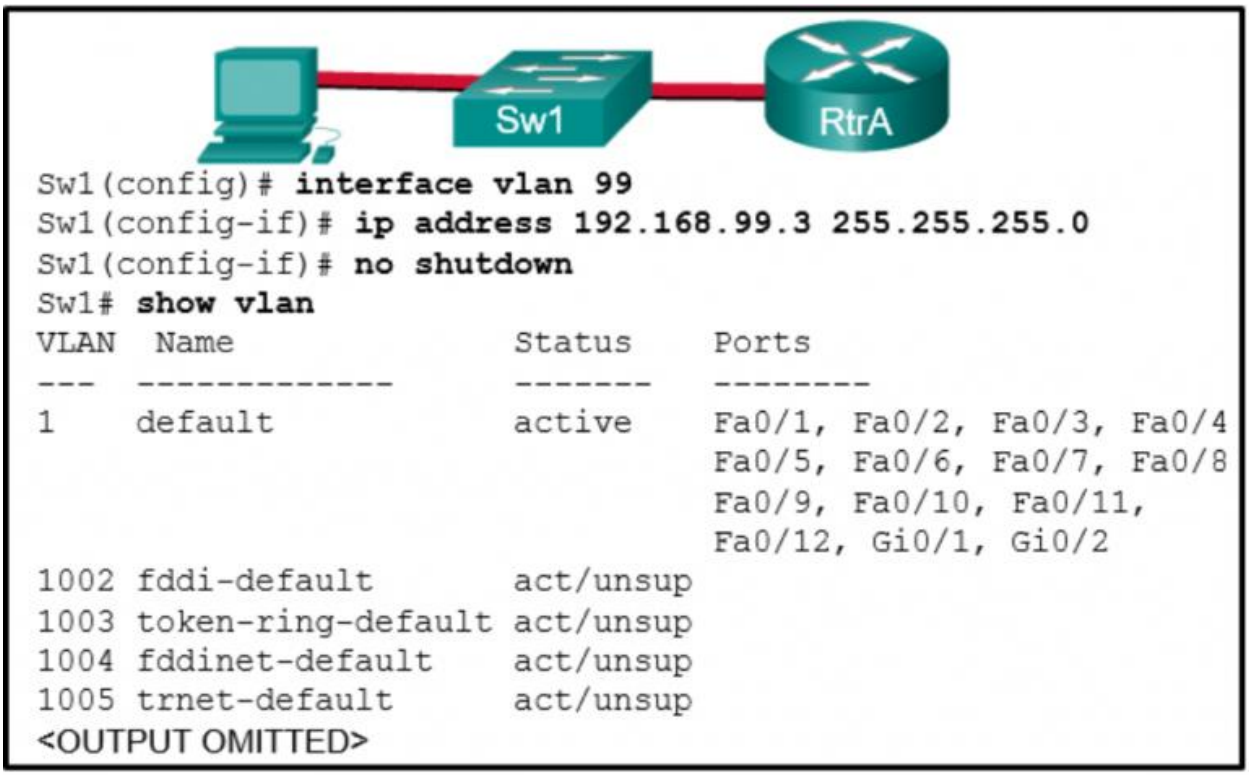
CCNA 2 v7 Switching Routing and Wireless Essentials-Version-Final-Answers-23

- Packets that are received from the Internet will be forwarded to one of the LANs connected to R1 or R2.
- **Packets with a destination network that is not 10.10.0.0/16 or is not 10.20.0.0/16 or is not a directly connected network will be forwarded to the Internet.**
- Packets from the 10.10.0.0/16 network will be forwarded to network 10.20.0.0/16, and packets from the 10.20.0.0/16 network will be forwarded to network 10.10.0.0/16.
- Packets that are destined for networks that are not in the routing table of HQ will be dropped.

24. What protocol or technology disables redundant paths to eliminate Layer 2 loops?

- VTP
- **STP**
- EtherChannel
- DTP

25. Refer to the exhibit. Based on the exhibited configuration and output, why is VLAN 99 missing?



CCNA 2 v7 Switching Routing and Wireless Essentials-Version-Final-Answers-25

- because VLAN 99 is not a valid management VLAN
- because there is a cabling problem on VLAN 99
- because VLAN 1 is up and there can only be one management VLAN on the switch
- **because VLAN 99 has not yet been created**

26. Which two VTP modes allow for the creation, modification, and deletion of VLANs on the local switch? (Choose two.)

- client
- master
- distribution
- slave
- **server**
- **transparent**

27. Which three steps should be taken before moving a Cisco switch to a new VTP management domain? (Choose three.)

- **Configure the switch with the name of the new management domain.**
- Reset the VTP counters to allow the switch to synchronize with the other switches in the domain.
- Configure the VTP server in the domain to recognize the BID of the new switch.
- Download the VTP database from the VTP server in the new domain.
- **Select the correct VTP mode and version.**

- **Reboot the switch.**

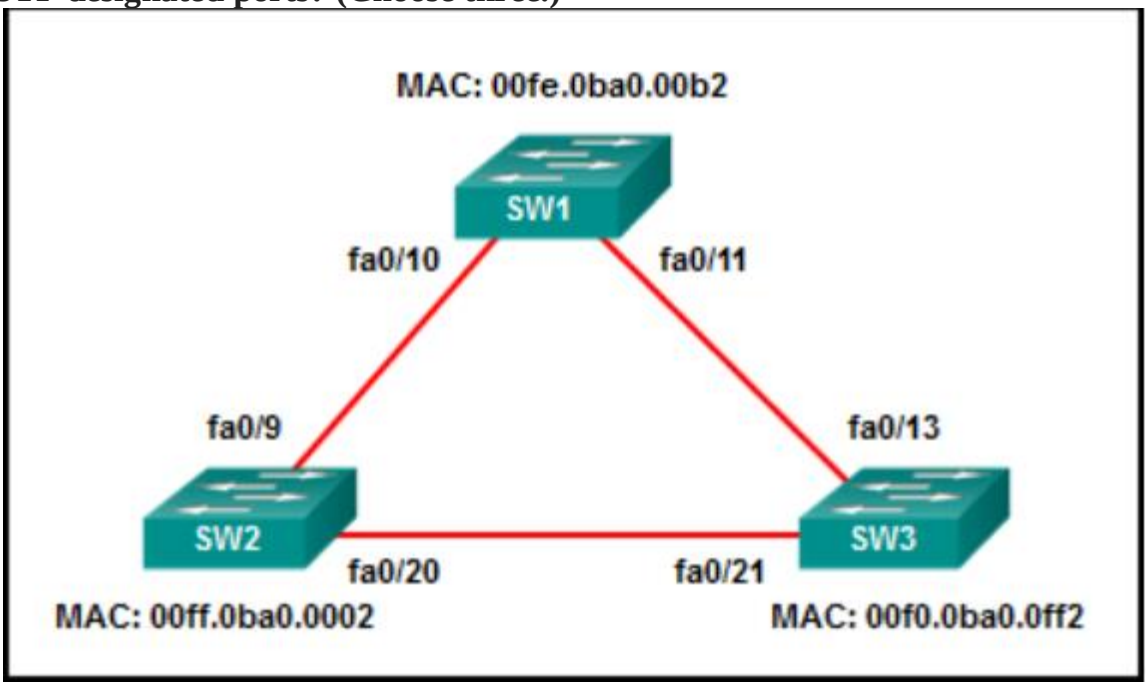
Explanation: When adding a new switch to a VTP domain, it is critical to configure the switch with a new domain name, the correct VTP mode, VTP version number, and password. A switch with a higher revision number can propagate invalid VLANs and erase valid VLANs thus preventing connectivity for multiple devices on the valid VLANs.

28. A network administrator is preparing the implementation of Rapid PVST+ on a production network. How are the Rapid PVST+ link types determined on the switch interfaces?

- Link types can only be configured on access ports configured with a single VLAN.
- Link types can only be determined if PortFast has been configured.
- **Link types are determined automatically.**
- Link types must be configured with specific port configuration commands.

Explanation: When Rapid PVST+ is being implemented, link types are automatically determined but can be specified manually. Link types can be either point-to-point, shared, or edge.

29. Refer to the exhibit. All the displayed switches are Cisco 2960 switches with the same default priority and operating at the same bandwidth. Which three ports will be STP designated ports? (Choose three.)



CCNA 2 v7 Switching Routing and Wireless Essentials-Version-Final-Answers-29

- fa0/9
- **fa0/13**
- **fa0/10**

- fa0/20
- **fa0/21**
- fa0/11

30. How will a router handle static routing differently if Cisco Express Forwarding is disabled?

- It will not perform recursive lookups.
- **Ethernet multiaccess interfaces will require fully specified static routes to avoid routing inconsistencies.**
- Static routes that use an exit interface will be unnecessary.
- Serial point-to-point interfaces will require fully specified static routes to avoid routing inconsistencies.

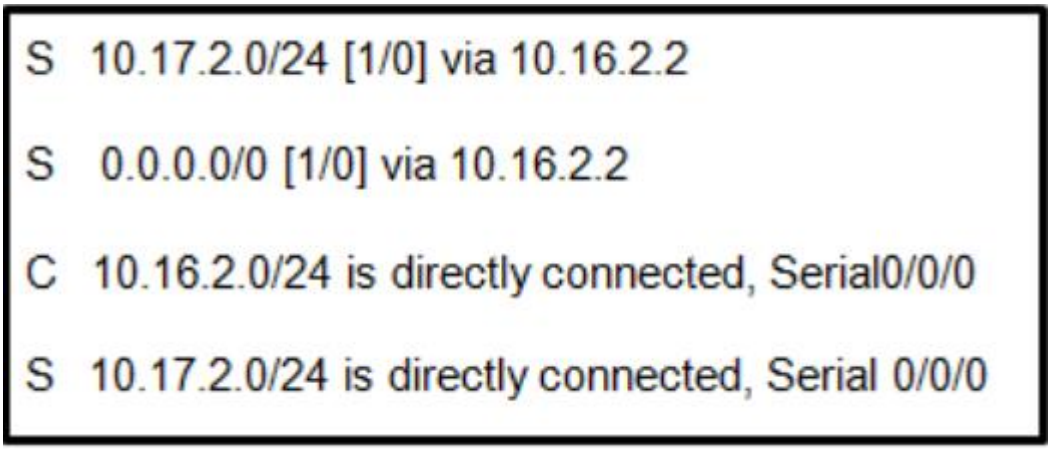
Explanation: In most platforms running IOS 12.0 or later, Cisco Express Forwarding is enabled by default. Cisco Express Forwarding eliminates the need for the recursive lookup. If Cisco Express Forwarding is disabled, multiaccess network interfaces require fully specified static routes in order to avoid inconsistencies in their routing tables. Point-to-point interfaces do not have this problem, because multiple end points are not present. With or without Cisco Express Forwarding enabled, using an exit interface when configuring a static route is a viable option.

31. Compared with dynamic routes, what are two advantages of using static routes on a router? (Choose two.)

- **They improve network security.**
- They take less time to converge when the network topology changes.
- They improve the efficiency of discovering neighboring networks.
- **They use fewer router resources.**

Explanation: Static routes are manually configured on a router. Static routes are not automatically updated and must be manually reconfigured if the network topology changes. Thus static routing improves network security because it does not make route updates among neighboring routers. Static routes also improve resource efficiency by using less bandwidth, and no CPU cycles are used to calculate and communicate routes.

32. Refer to the exhibit. Which route was configured as a static route to a specific network using the next-hop address?



- **S 10.17.2.0/24 [1/0] via 10.16.2.2**
- S 0.0.0.0/0 [1/0] via 10.16.2.2
- S 10.17.2.0/24 is directly connected, Serial 0/0/0
- C 10.16.2.0/24 is directly connected, Serial0/0/0

Explanation: The C in a routing table indicates an interface that is up and has an IP address assigned. The S in a routing table signifies that a route was installed using the ip route command. Two of the routing table entries shown are static routes to a specific destination (the 192.168.2.0 network). The entry that has the S denoting a static route and [1/0] was configured using the next-hop address. The other entry (S 192.168.2.0/24 is directly connected, Serial 0/0/0) is a static route configured using the exit interface. The entry with the 0.0.0.0 route is a default static route which is used to send packets to any destination network that is not specifically listed in the routing table.

33. What is the effect of entering the spanning-tree portfast configuration command on a switch?

- It disables an unused port.
- It disables all trunk ports.
- **It enables portfast on a specific switch interface.**
- It checks the source L2 address in the Ethernet header against the sender L2 address in the ARP body.

34. What is the IPv6 prefix that is used for link-local addresses?

- FF01::/8
- 2001::/3
- FC00::/7
- **FE80::/10**

Explanation: The IPv6 link-local prefix is FE80::/10 and is used to create a link-local IPv6 address on an interface.

35. Which two statements are characteristics of routed ports on a multilayer switch? (Choose two.)

- **In a switched network, they are mostly configured between switches at the core and distribution layers.**
- The interface vlan command has to be entered to create a VLAN on routed ports.
- They support subinterfaces, like interfaces on the Cisco IOS routers.
- They are used for point-to-multipoint links.
- **They are not associated with a particular VLAN.**

36. Successful inter-VLAN routing has been operating on a network with multiple VLANs across multiple switches for some time. When an inter-switch trunk link fails and Spanning Tree Protocol brings up a backup trunk link, it is reported that hosts on two VLANs can access some, but not all the network resources that could be accessed previously. Hosts on all other VLANS do not have this problem. What is the most likely cause of this problem?

- **The protected edge port function on the backup trunk interfaces has been disabled.**
- The allowed VLANs on the backup link were not configured correctly.
- Dynamic Trunking Protocol on the link has failed.
- Inter-VLAN routing also failed when the trunk link failed.

37. Which command will start the process to bundle two physical interfaces to create an EtherChannel group via LACP?

- interface port-channel 2
- channel-group 1 mode desirable
- **interface range GigabitEthernet 0/4 – 5**
- channel-group 2 mode auto

38. What action takes place when a frame entering a switch has a multicast destination MAC address?

- **The switch will forward the frame out all ports except the incoming port.**
- The switch forwards the frame out of the specified port.
- The switch adds a MAC address table entry mapping for the destination MAC address and the ingress port.
- The switch replaces the old entry and uses the more current port.

Explanation: If the destination MAC address is a broadcast or a multicast, the frame is also flooded out all ports except the incoming port.

39. A junior technician was adding a route to a LAN router. A traceroute to a device on the new network revealed a wrong path and unreachable status. What should be done or checked?

- Verify that there is not a default route in any of the edge router routing tables.
- Check the configuration on the floating static route and adjust the AD.
- Create a floating static route to that network.
- **Check the configuration of the exit interface on the new static route.**

40. Select the three PAgP channel establishment modes. (Choose three.)

- **auto**

- default
- passive
- **desirable**
- extended
- **on**

41. A static route has been configured on a router. However, the destination network no longer exists. What should an administrator do to remove the static route from the routing table?

- **Remove the route using the no ip route command.**
- Change the administrative distance for that route.
- Change the routing metric for that route.
- Nothing. The static route will go away on its own.

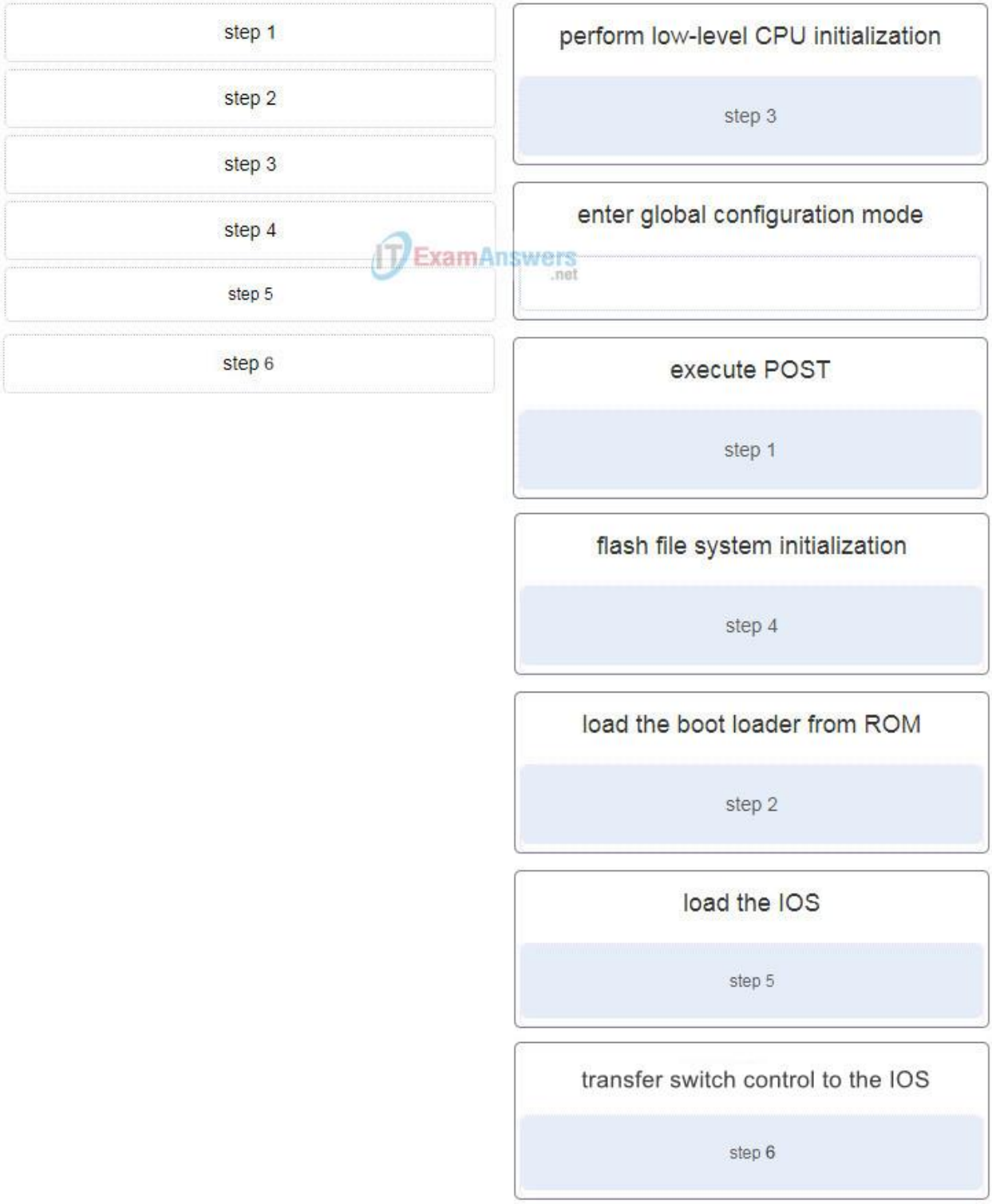
Explanation: When the destination network specified in a static route does not exist anymore, the static route stays in the routing table until it is manually removed by using the **no ip route** command.

42. Refer to the exhibit. What can be concluded about the configuration shown on R1?

```
R1# show running-config

<output omitted>
interface GigabitEthernet0/0
 ip address 172.16.1.5 255.255.255.0
 ip helper-address 10.10.10.8
 duplex auto
 speed auto

R1#
```

- **R1 is configured as a DHCPv4 relay agent.**
- R1 is operating as a DHCPv4 server.
- R1 will broadcast DHCPv4 requests on behalf of local DHCPv4 clients.
- R1 will send a message to a local DHCPv4 client to contact a DHCPv4 server at 10.10.10.8.

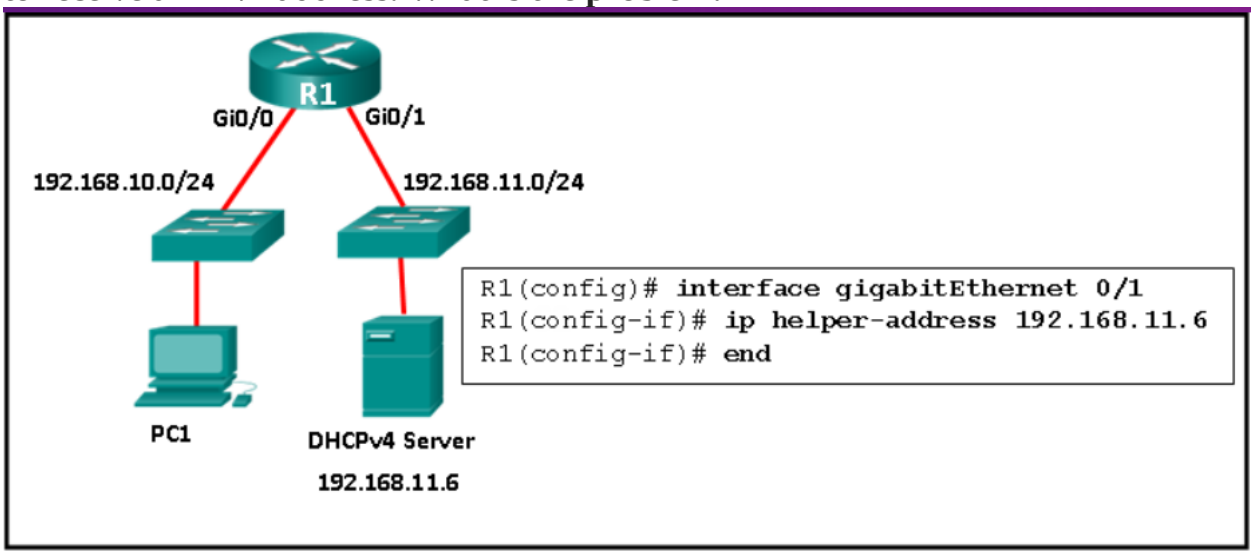
43. Match the step to each switch boot sequence description. (Not all options are used.)



Explanation: The steps are:
1. execute POST

2. load the boot loader from ROM
3. CPU register initializations
4. flash file system initialization
5. load the IOS
6. transfer switch control to the IOS

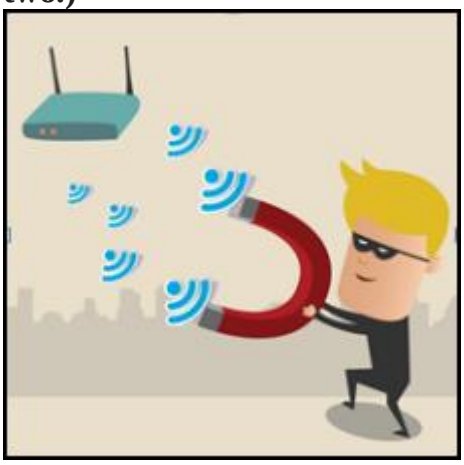
44. Refer to the exhibit. R1 has been configured as shown. However, PC1 is not able to receive an IPv4 address. What is the problem?



- **The ip helper-address command was applied on the wrong interface.**
- R1 is not configured as a DHCPv4 server.
- A DHCP server must be installed on the same LAN as the host that is receiving the IP address.
- The ip address dhcp command was not issued on the interface Gi0/1.

Explanation: The ip helper-address command has to be applied on interface Gi0/0. This command must be present on the interface of the LAN that contains the DHCPv4 client PC1 and must be directed to the correct DHCPv4 server.

45. What two default wireless router settings can affect network security? (Choose two.)



- **The SSID is broadcast.**
- MAC address filtering is enabled.
- WEP encryption is enabled.
- The wireless channel is automatically selected.
- **A well-known administrator password is set.**

Explanation: Default settings on wireless routers often include broadcasting the SSID and using a well-known administrative password. Both of these pose a security risk to wireless networks. WEP encryption and MAC address filtering are not set by default. The automatic selection of the wireless channel poses no security risks.

46. What is the common term given to SNMP log messages that are generated by network devices and sent to the SNMP server?

- **traps**
- acknowledgments
- auditing
- warnings

47. A network administrator is adding a new WLAN on a Cisco 3500 series WLC. Which tab should the administrator use to create a new VLAN interface to be used for the new WLAN?

- WIRELESS
- MANAGEMENT
- **CONTROLLER**
- WLANs

48. A network administrator is configuring a WLAN. Why would the administrator change the default DHCP IPv4 addresses on an AP?

- to restrict access to the WLAN by authorized, authenticated users only
- to monitor the operation of the wireless network

- **to reduce outsiders intercepting data or accessing the wireless network by using a well-known address range**
- to reduce the risk of interference by external devices such as microwave ovens

49. Which two functions are performed by a WLC when using split media access control (MAC)? (Choose two.)

- packet acknowledgments and retransmissions
- frame queuing and packet prioritization
- beacons and probe responses
- **frame translation to other protocols**
- **association and re-association of roaming clients**

50. On what switch ports should BPDU guard be enabled to enhance STP stability?

- **all PortFast-enabled ports**
- only ports that are elected as designated ports
- only ports that attach to a neighboring switch
- all trunk ports that are not root ports

51. Which network attack is mitigated by enabling BPDU guard?

- **rogue switches on a network**
- CAM table overflow attacks
- MAC address spoofing
- rogue DHCP servers on a network

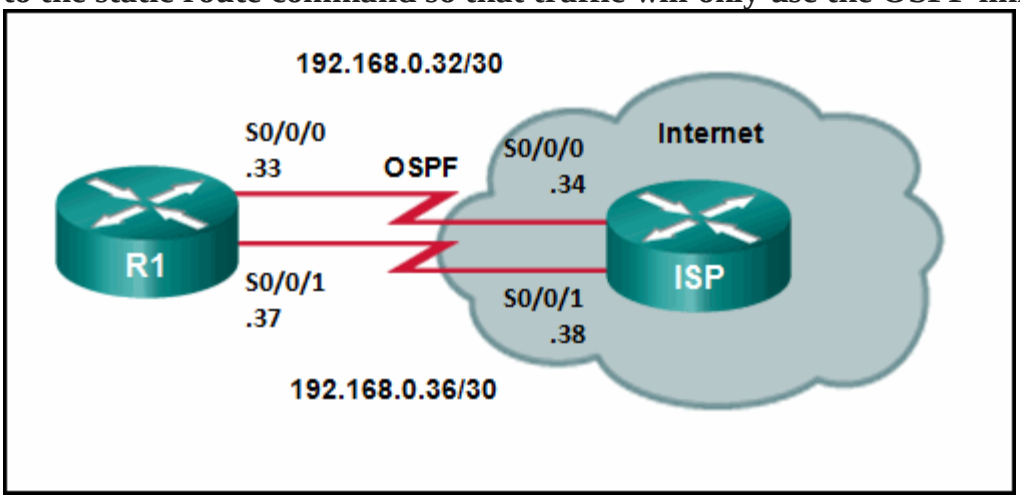
Explanation: There are several recommended STP stability mechanisms to help mitigate STP manipulation attacks:
PortFast – used to immediately bring an interface configured as an access or trunk port to the forwarding state from a blocking state. Applied to all end-user ports.
BPDU guard – immediately error-disables a port that receives a BPDU. Applied to all end-user ports.The receipt of BPDUs may be part of an unauthorized attempt to add a switch to the network.
Root guard – prevents a switch from becoming the root switch. Applied to all ports where the root switch should not be located.
Loop guard – detects unidirectional links to prevent alternate or root ports from becoming designated ports. Applied to all ports that are or can become nondesignated.

52. Why is DHCP snooping required when using the Dynamic ARP Inspection feature?

- It relies on the settings of trusted and untrusted ports set by DHCP snooping.
- It uses the MAC address table to verify the default gateway IP address.
- It redirects ARP requests to the DHCP server for verification.
- **It uses the MAC-address-to-IP-address binding database to validate an ARP packet.**

Explain: DAI relies on DHCP snooping. DHCP snooping listens to DHCP message exchanges and builds a bindings database of valid tuples (MAC address, IP address, VLAN interface).
When DAI is enabled, the switch drops ARP packet if the sender MAC address and sender IP address do not match an entry in the DHCP snooping bindings database. However, it can be overcome through static mappings. Static mappings are useful when hosts configure static IP addresses, DHCP snooping cannot be run, or other switches in the network do not run dynamic ARP inspection. A static mapping associates an IP address to a MAC address on a VLAN.

53. Refer to the exhibit. Router R1 has an OSPF neighbor relationship with the ISP router over the 192.168.0.32 network. The 192.168.0.36 network link should serve as a backup when the OSPF link goes down. The floating static route command ip route 0.0.0.0 0.0.0.0 S0/0/1 100 was issued on R1 and now traffic is using the backup link even when the OSPF link is up and functioning. Which change should be made to the static route command so that traffic will only use the OSPF link when it is up?



- **Change the administrative distance to 120.**
- Add the next hop neighbor address of 192.168.0.36.
- Change the destination network to 192.168.0.34.
- Change the administrative distance to 1.

Explain: The problem with the current floating static route is that the administrative distance is set too low. The administrative distance will need to be higher than that of OSPF, which is 110, so that the router will only use the OSPF link when it is up.

54. Refer to the exhibit. What is the metric to forward a data packet with the IPv6 destination address 2001:DB8:ACAD:E:240:BFF:FED4:9DD2?

```
R1# show ipv6 route
<output omitted>

D   2001:DB8:ACAD:3::/64 [90/2681856]
     via FE80::3, Serial0/0/0
D   2001:DB8:ACAD:4::/64 [90/2681856]
     via FE80::5, Serial0/0/1
D   2001:DB8:ACAD:5::/64 [90/3193856]
     via FE80::3, Serial0/0/0
C   2001:DB8:ACAD:A::/64 [0/0]
     via ::, GigabitEthernet0/0
L   2001:DB8:ACAD:A::1/128 [0/0]
     via ::, GigabitEthernet0/0
C   2001:DB8:ACAD:B::/64 [0/0]
     via ::, GigabitEthernet0/1
L   2001:DB8:ACAD:B::1/128 [0/0]
     via ::, GigabitEthernet0/1
D   2001:DB8:ACAD:C::/64 [90/2682112]
     via FE80::3, Serial0/0/0
D   2001:DB8:ACAD:D::/64 [90/2170112]
     via FE80::5, Serial0/0/1
D   2001:DB8:ACAD:E::/64 [90/2682112]
     via FE80::5, Serial0/0/1
```

- 90
- 128
- 2170112
- 2681856
- **2682112**
- 3193856

Explain: The IPv6 destination address 2001:DB8:ACAD:E:240:BFF:FED4:9DD2 belongs to the network of 2001:DB8:ACAD:E::/64. In the routing table, the route to forward the packet has Serial 0/0/1 as an exit interface and 2682112 as the cost.

55. A network administrator is configuring a new Cisco switch for remote management access. Which three items must be configured on the switch for the task? (Choose three.)

- **IP address**
- VTP domain
- **vty lines**
- default VLAN
- **default gateway**
- loopback address

Explain: To enable the remote management access, the Cisco switch must be configured with an IP address and a default gateway. In addition, vty lines must configured to enable either Telnet or SSH connections. A loopback address, default VLAN, and VTP domain configurations are not necessary for the purpose of remote switch management.

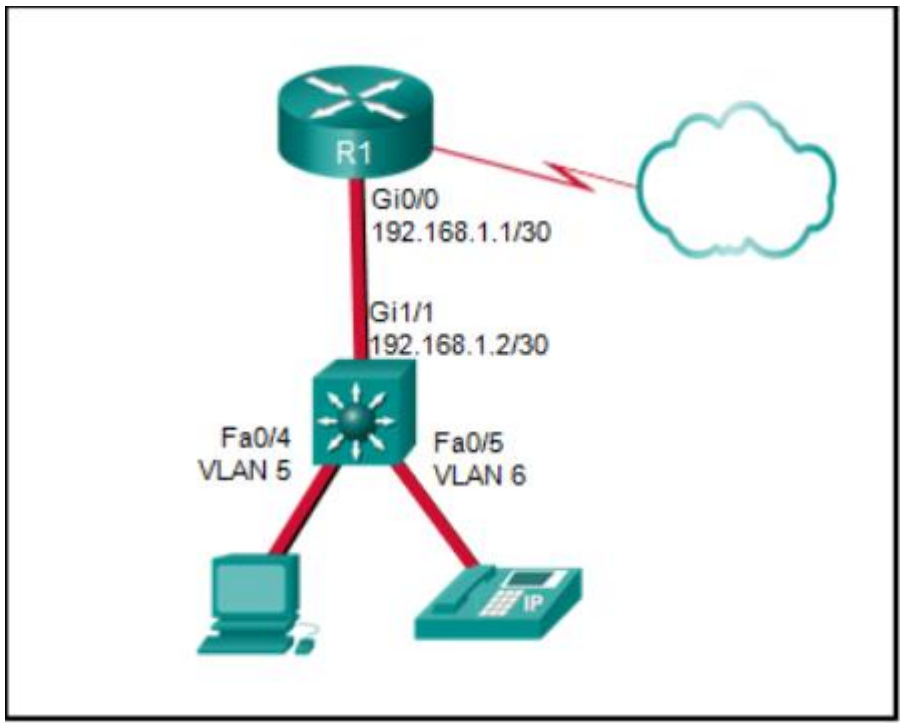
56. Refer to the exhibit. Which statement shown in the output allows router R1 to respond to stateless DHCPv6 requests?

```
R1# show running-config
<output omitted>
ipv6 unicast-routing
!
ipv6 dhcp pool LAN1
 prefix-delegation 2001:DB8:8::/48 00030001000E84244E70
 dns-server 2001:DB8:8::8
 domain-name cisco.com
!
interface FastEthernet0/0
 no ip address
 ipv6 address 2001:DB8:8::100/48
 ipv6 nd other-config-flag
 ipv6 dhcp server LAN1
```

- **ipv6 nd other-config-flag**
- prefix-delegation 2001:DB8:8::/48 00030001000E84244E70
- ipv6 dhcp server LAN1
- ipv6 unicast-routing
- dns-server 2001:DB8:8::8

Explain: The interface command ipv6 nd other-config-flag allows RA messages to be sent on this interface, indicating that additional information is available from a stateless DHCPv6 server.

57. Refer to the exhibit. A Layer 3 switch routes for three VLANs and connects to a router for Internet connectivity. Which two configurations would be applied to the switch? (Choose two.)



CCNA-2-v7-exam-answers-57

(config)# interface gigabitethernet1/1
(config-if)# switchport mode trunk

(config)# interface gigabitethernet 1/1
(config-if)# no switchport
(config-if)# ip address 192.168.1.2 255.255.255.252
(config)# interface vlan 1
(config-if)# ip address 192.168.1.2 255.255.255.0
(config-if)# no shutdown

(config)# ip routing
(config)# interface fastethernet0/4
(config-if)# switchport mode trunk

58. A technician is troubleshooting a slow WLAN and decides to use the split-the-traffic approach. Which two parameters would have to be configured to do this? (Choose two.)

- **Configure the 5 GHz band for streaming multimedia and time sensitive traffic.**
- Configure the security mode to WPA Personal TKIP/AES for one network and WPA2 Personal AES for the other network
- **Configure the 2.4 GHz band for basic internet traffic that is not time sensitive.**
- Configure the security mode to WPA Personal TKIP/AES for both networks.
- Configure a common SSID for both split networks.

59. A company has just switched to a new ISP. The ISP has completed and checked the connection from its site to the company. However, employees at the company are not able to access the internet. What should be done or checked?

- Verify that the static route to the server is present in the routing table.
- Check the configuration on the floating static route and adjust the AD.
- **Ensure that the old default route has been removed from the company edge routers.**
- Create a floating static route to that network.

60. Which information does a switch use to populate the MAC address table?

- the destination MAC address and the incoming port
- the destination MAC address and the outgoing port
- the source and destination MAC addresses and the incoming port
- the source and destination MAC addresses and the outgoing port
- **the source MAC address and the incoming port**
- the source MAC address and the outgoing port

Explain: To maintain the MAC address table, the switch uses the source MAC address of the incoming packets and the port that the packets enter. The destination address is used to select the outgoing port.

61. Refer to the exhibit. A network administrator is reviewing the configuration of switch S1. Which protocol has been implemented to group multiple physical ports into one logical link?

```
S1# show run | begin interface
<output omitted>
!
interface FastEthernet0/8
 channel-group 1 mode auto
 switchport mode trunk
!
interface FastEthernet0/9
 channel-group 1 mode auto
 switchport mode trunk
!
interface Port-channel 1
 switchport trunk allowed vlan 1,10,20,30
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
```


- **PAgP**
- DTP
- LACP
- STP

62. Which type of static route is configured with a greater administrative distance to provide a backup route to a route learned from a dynamic routing protocol?

- **floating static route**

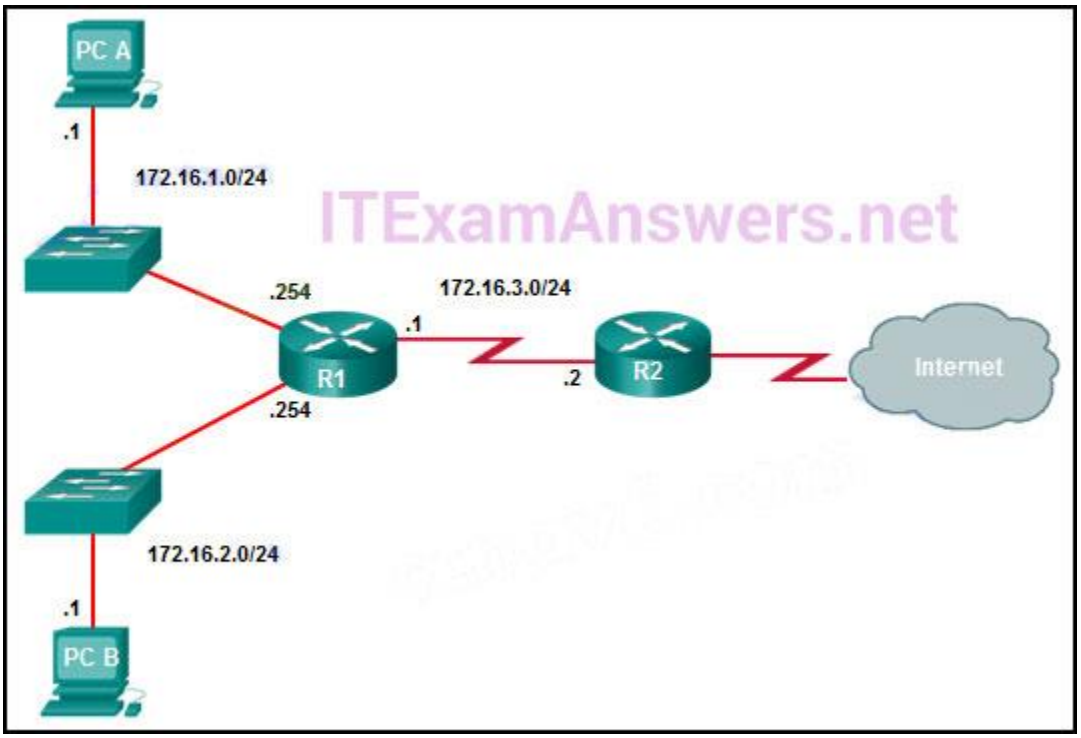
- default static route
- summary static route
- standard static route

Explain: There are four basic types of static routes. Floating static routes are backup routes that are placed into the routing table if a primary route is lost. A summary static route aggregates several routes into one, reducing the of the routing table. Standard static routes are manually entered routes into the routing table. Default static routes create a gateway of last resort.

63. What action takes place when a frame entering a switch has a unicast destination MAC address appearing in the MAC address table?

- The switch updates the refresh timer for the entry.
- **The switch forwards the frame out of the specified port.**
- The switch purges the entire MAC address table.
- The switch replaces the old entry and uses the more current port.

64. The exhibit shows two PCs called PC A and PC B, two routes called R1 and R2, and two switches. PC A has the address 172.16.1.1/24 and is connected to a switch and into an interface on R1 that has the IP address 172.16.1.254. PC B has the address 172.16.2.1/24 and is connected to a switch that is connected to another interface on R1 with the IP address 172.16.2.254. The serial interface on R1 has the address 172.16.3.1 and is connected to the serial interface on R2 that has the address 172.16.3.2/24. R2 is connected to the internet cloud. Which command will create a static route on R2 in order to reach PC B?



- R2(config)# ip route 172.16.2.1 255.255.255.0 172.16.3.1
- R2(config)# ip route 172.16.2.0 255.255.255.0 172.16.2.254

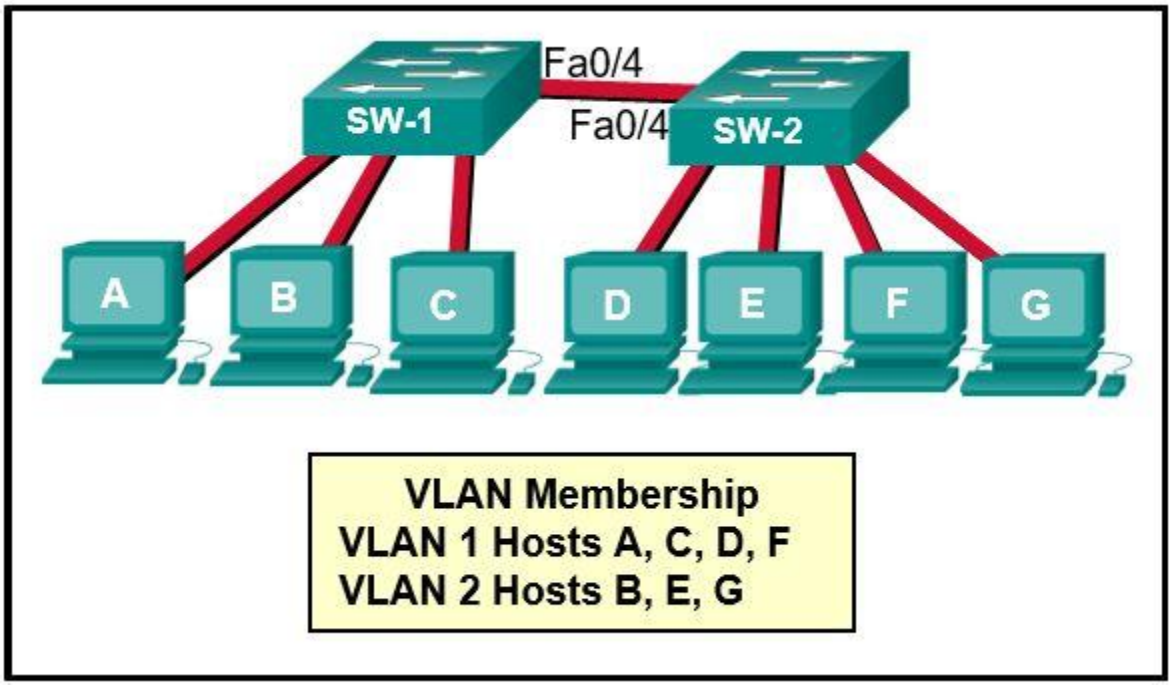
- **R2(config)# ip route 172.16.2.0 255.255.255.0 172.16.3.1**
- R2(config)# ip route 172.16.3.0 255.255.255.0 172.16.2.254

Explain: The correct syntax is:
router(config)# ip route destination-network destination-mask {next-hop-ip-address | exit-interface}
If the local exit interface instead of the next-hop IP address is used then the route will be displayed as a directly connected route instead of a static route in the routing table. Because the network to be reached is 172.16.2.0 and the next-hop IP address is 172.16.3.1, the command is R2(config)# ip route 172.16.2.0 255.255.255.0 172.16.3.1

65. What protocol or technology allows data to transmit over redundant switch links?

- **EtherChannel**
- DTP
- STP
- VTP

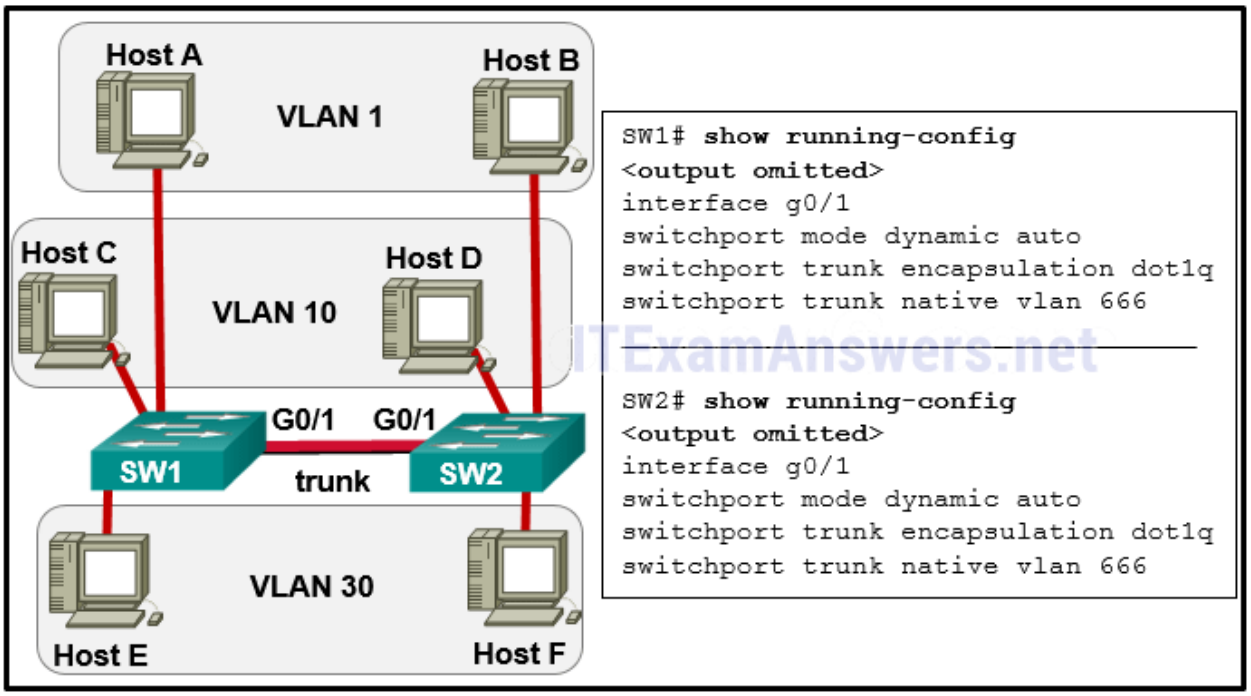
66. Refer to the exhibit. Which three hosts will receive ARP requests from host A, assuming that port Fa0/4 on both switches is configured to carry traffic for multiple VLANs? (Choose three.)



- host B
- **host C**
- **host D**
- host E
- **host F**
- host G

Explain: ARP requests are sent out as broadcasts. That means the ARP request is sent only throughout a specific VLAN. VLAN 1 hosts will only hear ARP requests from hosts on VLAN 1. VLAN 2 hosts will only hear ARP requests from hosts on VLAN 2.

67. Refer to the exhibit. The network administrator configures both switches as displayed. However, host C is unable to ping host D and host E is unable to ping host F. What action should the administrator take to enable this communication?



- Associate hosts A and B with VLAN 10 instead of VLAN 1.
- **Configure either trunk port in the dynamic desirable mode.**
- Include a router in the topology.
- Remove the native VLAN from the trunk.
- Add the switchport nonegotiate command to the configuration of SW2.

68. What is the effect of entering the shutdown configuration command on a switch?

- It enables BPDU guard on a specific port.
- **It disables an unused port.**
- It enables portfast on a specific switch interface.
- It disables DTP on a non-trunking interface.

69. What would be the primary reason an attacker would launch a MAC address overflow attack?

- so that the switch stops forwarding traffic
- so that legitimate hosts cannot obtain a MAC address
- **so that the attacker can see frames that are destined for other hosts**
- so that the attacker can execute arbitrary code on the switch

70. During the AAA process, when will authorization be implemented?

- **Immediately after successful authentication against an AAA data source**

- Immediately after AAA accounting and auditing receives detailed reports
- Immediately after an AAA client sends authentication information to a centralized server
- Immediately after the determination of which resources a user can access

Explain: A. AAA authorization is implemented immediately after the user is authenticated against a specific AAA data source.

71. A company security policy requires that all MAC addressing be dynamically learned and added to both the MAC address table and the running configuration on each switch. Which port security configuration will accomplish this?

- auto secure MAC addresses
- dynamic secure MAC addresses
- static secure MAC addresses
- **sticky secure MAC addresses**

Explain: With sticky secure MAC addressing, the MAC addresses can be either dynamically learned or manually configured and then stored in the address table and added to the running configuration file. In contrast, dynamic secure MAC addressing provides for dynamically learned MAC addressing that is stored only in the address table.

72. Which three Wi-Fi standards operate in the 2.4GHz range of frequencies? (Choose three.)

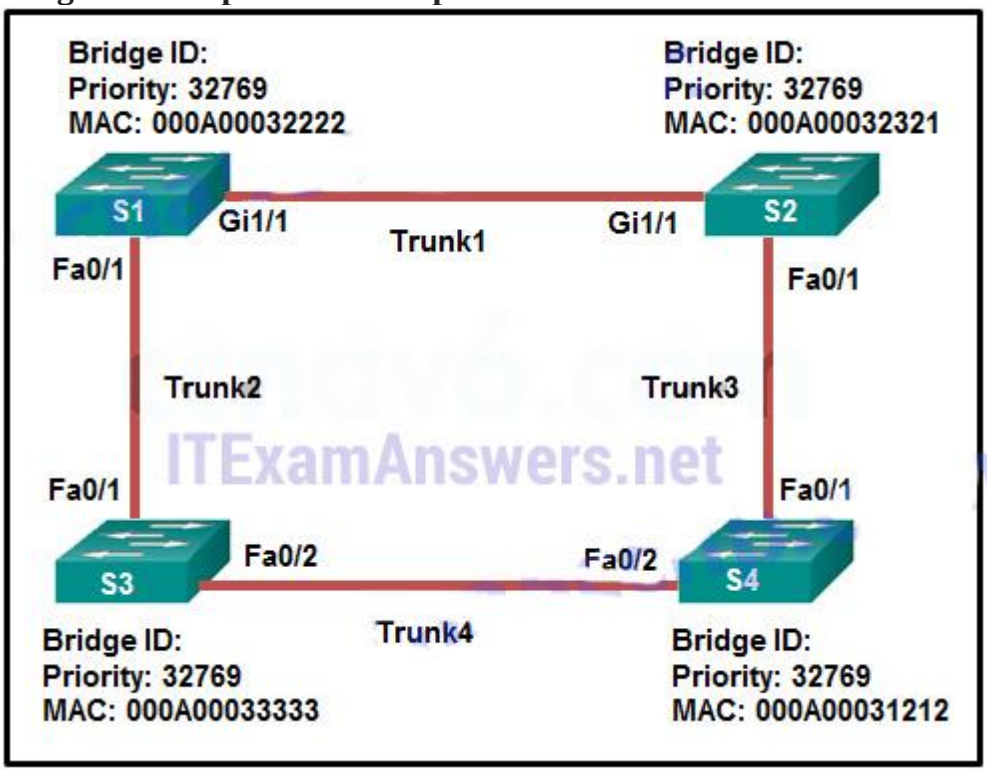
- 802.11a
- **802.11b**
- **802.11g**
- **802.11n**
- 802.11ac

Explanation: 802.11b and 802.11g operate in the 2.4GHz range, and 802.11n can operate in either the 2.4GHz or the 5GHz range. 802.11a and 802.11ac operate only in the 5GHz range of frequencies.

73. To obtain an overview of the spanning tree status of a switched network, a network engineer issues the show spanning-tree command on a switch. Which two items of information will this command display? (Choose two.)

- **The root bridge BID.**
- **The role of the ports in all VLANs.**
- The status of native VLAN ports.
- The number of broadcasts received on each root port.
- The IP address of the management VLAN interface.

74. Refer to the exhibit. Which trunk link will not forward any traffic after the root bridge election process is complete?



- Trunk1
- **Trunk2**
- Trunk3
- Trunk4

75. Which method of IPv6 prefix assignment relies on the prefix contained in RA messages?

- EUI-64
- **SLAAC**
- static
- stateful DHCPv6

Explanation: Stateless Address Autoconfiguration (SLAAC) relies on information received in router advertisement (RA) messages in order to automatically create an IPv6 address. The RA messages contain information such as the network prefix and prefix length, which the host combines with an interface ID in order to make a unique IPv6 unicast address.

76. Which two protocols are used to provide server-based AAA authentication? (Choose two.)

- 802.1x
- SSH
- SNMP
- **TACACS+**

- **RADIUS**

Explanation: Server-based AAA authentication uses an external TACACS or RADIUS authentication server to maintain a username and password database. When a client establishes a connection with an AAA enabled device, the device authenticates the client by querying the authentication servers.

77. A network administrator is configuring a WLAN. Why would the administrator disable the broadcast feature for the SSID?

- **to eliminate outsiders scanning for available SSIDs in the area**
- to reduce the risk of interference by external devices such as microwave ovens
- to reduce the risk of unauthorized APs being added to the network
- to provide privacy and integrity to wireless traffic by using encryption

78. Which mitigation technique would prevent rogue servers from providing false IP configuration parameters to clients?

- implementing port security
- **turning on DHCP snooping**
- disabling CDP on edge ports
- implementing port-security on edge ports

Explanation: Like Dynamic ARP Inspection (DAI), IP Source Guard (IPSG) needs to determine the validity of MAC-address-to-IP-address bindings. To do this IPSG uses the bindings database built by DHCP snooping.

79. A network administrator configures the port security feature on a switch. The security policy specifies that each access port should allow up to two MAC addresses. When the maximum number of MAC addresses is reached, a frame with the unknown source MAC address is dropped and a notification is sent to the syslog server. Which security violation mode should be configured for each access port?

- shutdown
- **restrict**
- warning
- protect

Explanation: In port security implementation, an interface can be configured for one of three violation modes:
Protect – a port security violation causes the interface to drop packets with unknown source addresses and no notification is sent that a security violation has occurred.
Restrict – a port security violation causes the interface to drop packets with unknown source addresses and to send a notification that a security violation has occurred.
Shutdown – a port security violation causes the interface to immediately become error-disabled and turns off the port LED. No notification is sent that a security violation has occurred.

80. What protocol or technology defines a group of routers, one of them defined as active and another one as standby?

- EtherChannel
- VTP
- **HSRP**
- DTP

81. Refer to the exhibit. After attempting to enter the configuration that is shown in router RTA, an administrator receives an error and users on VLAN 20 report that they are unable to reach users on VLAN 30. What is causing the problem?

```
RTA# configure terminal
RTA(config)# interface Fa0/0
RTA(config-if)# no shutdown
RTA(config-if)# interface Fa0/0.10
RTA(config-subif)# encapsulation dot1q  10
RTA(config-subif)# ip address 192.168.3.30 255.255.255.224
RTA(config-subif)# interface Fa0/0.20
RTA(config-subif)# encapsulation dot1q  20
RTA(config-subif)# ip address 192.168.3.49 255.255.255.224
RTA(config-subif)# interface Fa0/0.30
RTA(config-subif)# encapsulation dot1q  30
RTA(config-subif)# ip address 192.168.3.62 255.255.255.224
```


- There is no address on Fa0/0 to use as a default gateway.
- **RTA is using the same subnet for VLAN 20 and VLAN 30.**
- Dot1q does not support subinterfaces.
- The no shutdown command should have been issued on Fa0/0.20 and Fa0/0.30.

82. Which three pairs of trunking modes will establish a functional trunk link between two Cisco switches? (Choose three.)

dynamic auto - dynamic auto

access - trunk

dynamic desirable - trunk

access - dynamic auto

dynamic desirable - dynamic desirable

dynamic desirable - dynamic auto

83. A technician is configuring a router for a small company with multiple WLANs and doesn't need the complexity of a dynamic routing protocol. What should be done or checked?

- Verify that there is not a default route in any of the edge router routing tables.
- **Create static routes to all internal networks and a default route to the internet.**
- Create extra static routes to the same location with an AD of 1.
- Check the statistics on the default route for oversaturation.

84. A company is deploying a wireless network in the distribution facility in a Boston suburb. The warehouse is quite large and it requires multiple access points to be used. Because some of the company devices still operate at 2.4GHz, the network administrator decides to deploy the 802.11g standard. Which channel assignments on the multiple access points will make sure that the wireless channels are not overlapping?

- channels 1, 5, and 9
- **channels 1, 6, and 11**
- channels 1, 7, and 13
- channels 2, 6, and 10

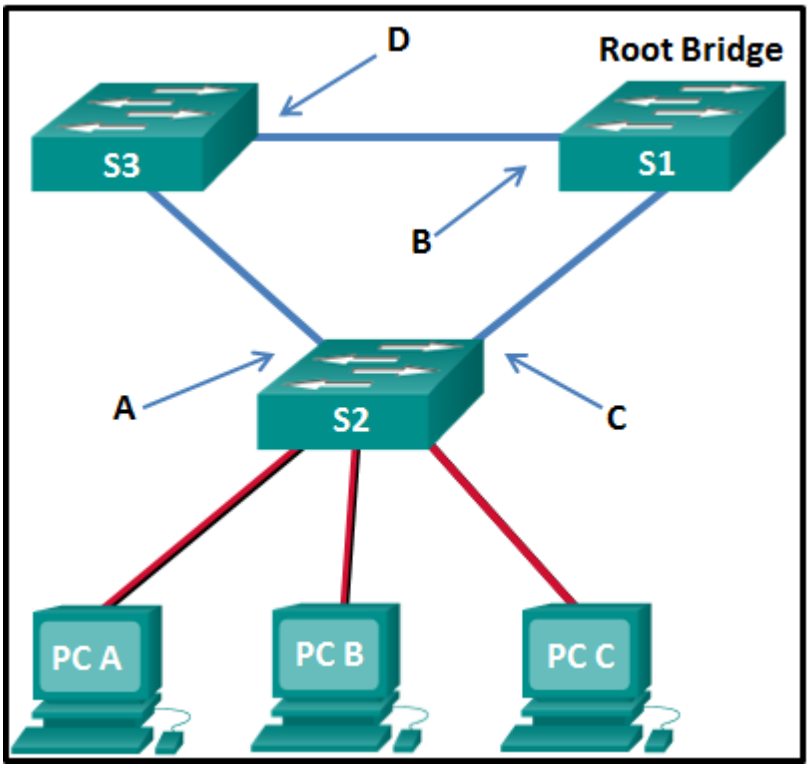
Explanation: In the North America domain, 11 channels are allowed for 2.4GHz wireless networking. Among these 11 channels, the combination of channels 1, 6, and 11 are the only non-overlapping channel combination.

85. A network administrator of a small advertising company is configuring WLAN security by using the WPA2 PSK method. Which credential do office users need in order to connect their laptops to the WLAN?

- the company username and password through Active Directory service
- **a key that matches the key on the AP**
- a user passphrase
- a username and password configured on the AP

Explanation: When a WLAN is configured with WPA2 PSK, wireless users must know the pre-shared key to associate and authenticate with the AP.

86. Refer to the exhibit. What are the possible port roles for ports A, B, C, and D in this RSTP-enabled network?



- **alternate, designated, root, root**
- designated, alternate, root, root
- alternate, root, designated, root
- designated, root, alternate, root

Explanation: Because S1 is the root bridge, B is a designated port, and C and D root ports. RSTP supports a new port type, alternate port in discarding state, that can be port A in this scenario.

87. Refer to the exhibit. Which static route would an IT technician enter to create a backup route to the 172.16.1.0 network that is only used if the primary RIP learned

route fails?

```
R1(config)# do show ip route
<output omitted>

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.0.0.0/30 is directly connected, Serial0/0/0
L 10.0.0.1/32 is directly connected, Serial0/0/0
172.16.0.0/24 is subnetted, 1 subnets
R 172.16.1.0/24 [120/1] via 10.0.0.2, 00:00:04, Serial0/0/0
192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.10.0/24 is directly connected, GigabitEthernet0/1
L 192.168.10.1/32 is directly connected, GigabitEthernet0/1
192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.11.0/24 is directly connected, GigabitEthernet0/0
L 192.168.11.1/32 is directly connected, GigabitEthernet0/0
S* 0.0.0.0/0 is directly connected, Serial0/0/0
```

- ip route 172.16.1.0 255.255.255.0 s0/0/0
- **ip route 172.16.1.0 255.255.255.0 s0/0/0 121**
- ip route 172.16.1.0 255.255.255.0 s0/0/0 111
- ip route 172.16.1.0 255.255.255.0 s0/0/0 91

Explanation: A backup static route is called a floating static route. A floating static route has an administrative distance greater than the administrative distance of another static route or dynamic route.

88. What mitigation plan is best for thwarting a DoS attack that is creating a MAC address table overflow?

- Disable DTP.
- Disable STP.
- **Enable port security.**
- Place unused ports in an unused VLAN.

Explanation: A MAC address (CAM) table overflow attack, buffer overflow, and MAC address spoofing can all be mitigated by configuring port security. A network administrator would typically not want to disable STP because it prevents Layer 2 loops. DTP is disabled to prevent VLAN hopping. Placing unused ports in an unused VLAN prevents unauthorized wired connectivity.

89. A network engineer is troubleshooting a newly deployed wireless network that is using the latest 802.11 standards. When users access high bandwidth services such as streaming video, the wireless network performance is poor. To improve performance the network engineer decides to configure a 5 Ghz frequency band SSID and train users to use that SSID for streaming media services. Why might this solution improve the wireless network performance for that type of service?

- Requiring the users to switch to the 5 GHz band for streaming media is inconvenient and will result in fewer users accessing these services.
- **The 5 GHz band has more channels and is less crowded than the 2.4 GHz band, which makes it more suited to streaming multimedia.**
- The 5 GHz band has a greater range and is therefore likely to be interference-free.
- The only users that can switch to the 5 GHz band will be those with the latest wireless NICs, which will reduce usage.

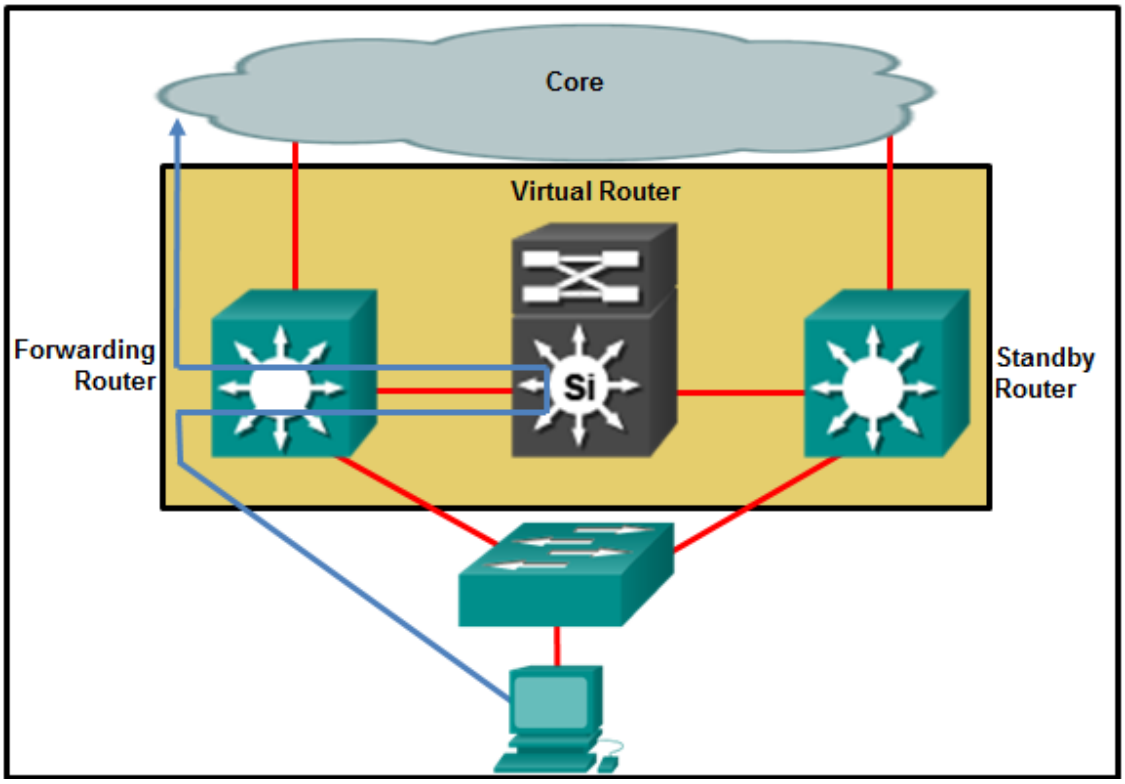
Explanation: Wireless range is determined by the access point antenna and output power, not the frequency band that is used. In this scenario it is stated that all users have wireless NICs that comply with the latest standard, and so all can access the 5 GHz band. Although some users may find it inconvenient to switch to the 5 Ghz band to access streaming services, it is the greater number of channels, not just fewer users, that will improve network performance.

90. Which DHCPv4 message will a client send to accept an IPv4 address that is offered by a DHCP server?

- broadcast DHCPACK
- **broadcast DHCPREQUEST**
- unicast DHCPACK
- unicast DHCPREQUEST

Explanation: When a DHCP client receives DHCPOFFER messages, it will send a broadcast DHCPREQUEST message for two purposes. First, it indicates to the offering DHCP server that it would like to accept the offer and bind the IP address. Second, it notifies any other responding DHCP servers that their offers are declined.

91. Refer to the exhibit. Which destination MAC address is used when frames are sent from the workstation to the default gateway?



- **MAC address of the virtual router**
- MAC address of the standby router
- MAC addresses of both the forwarding and standby routers
- MAC address of the forwarding router

Explanation: The IP address of the virtual router acts as the default gateway for all the workstations. Therefore, the MAC address that is returned by the Address Resolution Protocol to the workstation will be the MAC address of the virtual router.

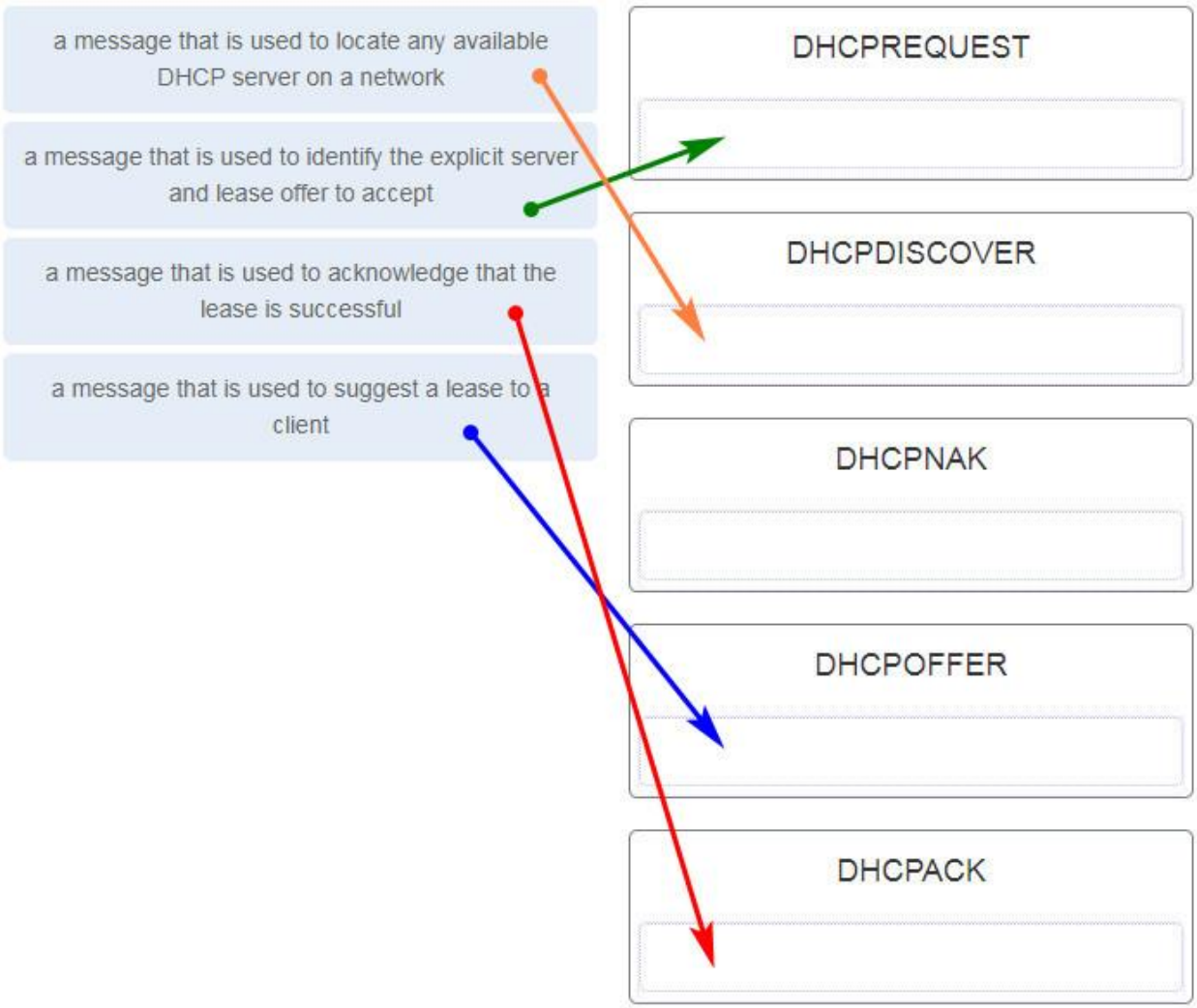
92. After a host has generated an IPv6 address by using the DHCPv6 or SLAAC process, how does the host verify that the address is unique and therefore usable?

- The host sends an ICMPv6 echo request message to the DHCPv6 or SLAAC-learned address and if no reply is returned, the address is considered unique.
- **The host sends an ICMPv6 neighbor solicitation message to the DHCP or SLAAC-learned address and if no neighbor advertisement is returned, the address is considered unique.**
- The host checks the local neighbor cache for the learned address and if the address is not cached, it it considered unique.
- The host sends an ARP broadcast to the local link and if no hosts send a reply, the address is considered unique.

Explanation: Before a host can actually configure and use an IPv6 address learned through SLAAC or DHCP, the host must verify that no other host is

already using that address. To verify that the address is indeed unique, the host sends an ICMPv6 neighbor solicitation to the address. If no neighbor advertisement is returned, the host considers the address to be unique and configures it on the interface.

93. Match the purpose with its DHCP message type. (Not all options are used.)

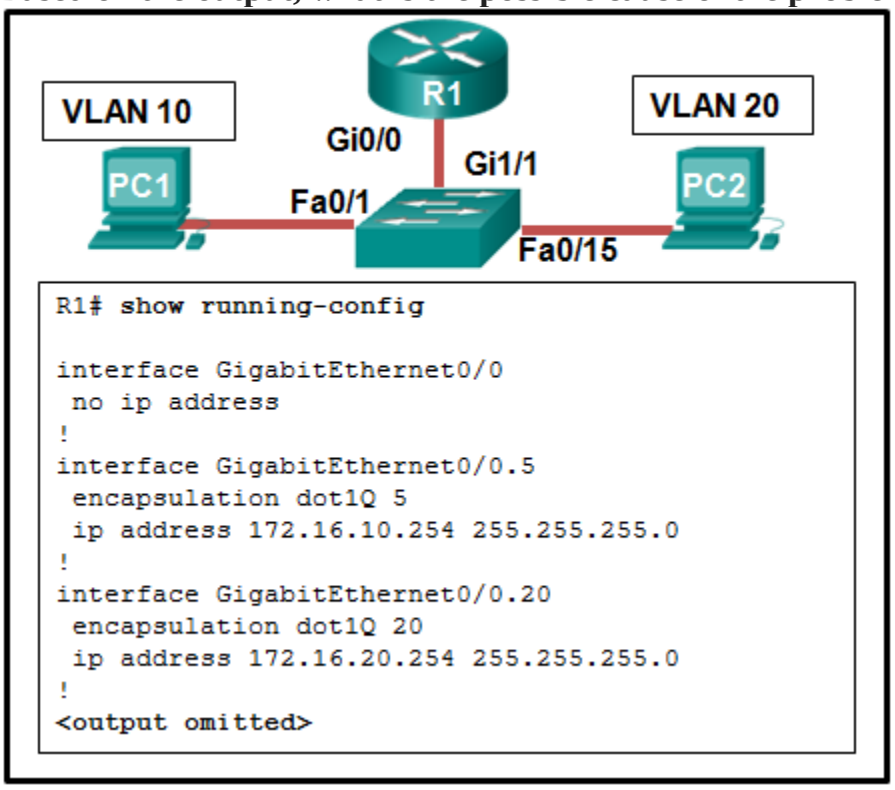


94. Which protocol adds security to remote connections?

- FTP
- HTTP
- NetBEUI
- POP
- **SSH**

Explanation: SSH allows a technician to securely connect to a remote network device for monitoring and troubleshooting. HTTP establishes web page requests. FTP manages file transfer. NetBEUI is not routed on the Internet. POP downloads email messages from email servers.

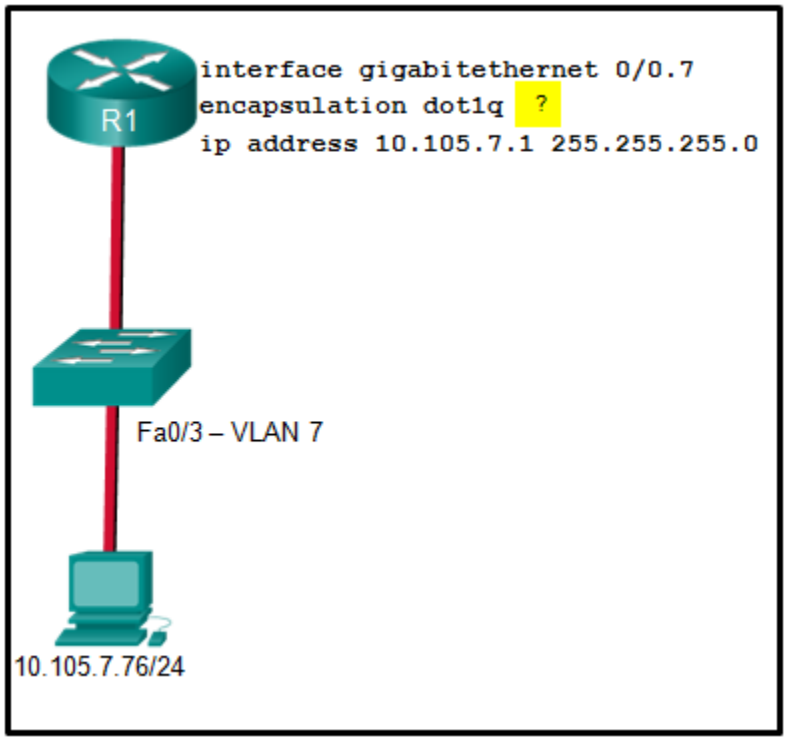
95. Refer to the exhibit. A network administrator is verifying the configuration of inter-VLAN routing. Users complain that PC2 cannot communicate with PC1. Based on the output, what is the possible cause of the problem?



- Gi0/0 is not configured as a trunk port.
- The command interface GigabitEthernet0/0.5 was entered incorrectly.
- There is no IP address configured on the interface Gi0/0.
- The no shutdown command is not entered on subinterfaces.
- **The encapsulation dot1Q 5 command contains the wrong VLAN.**

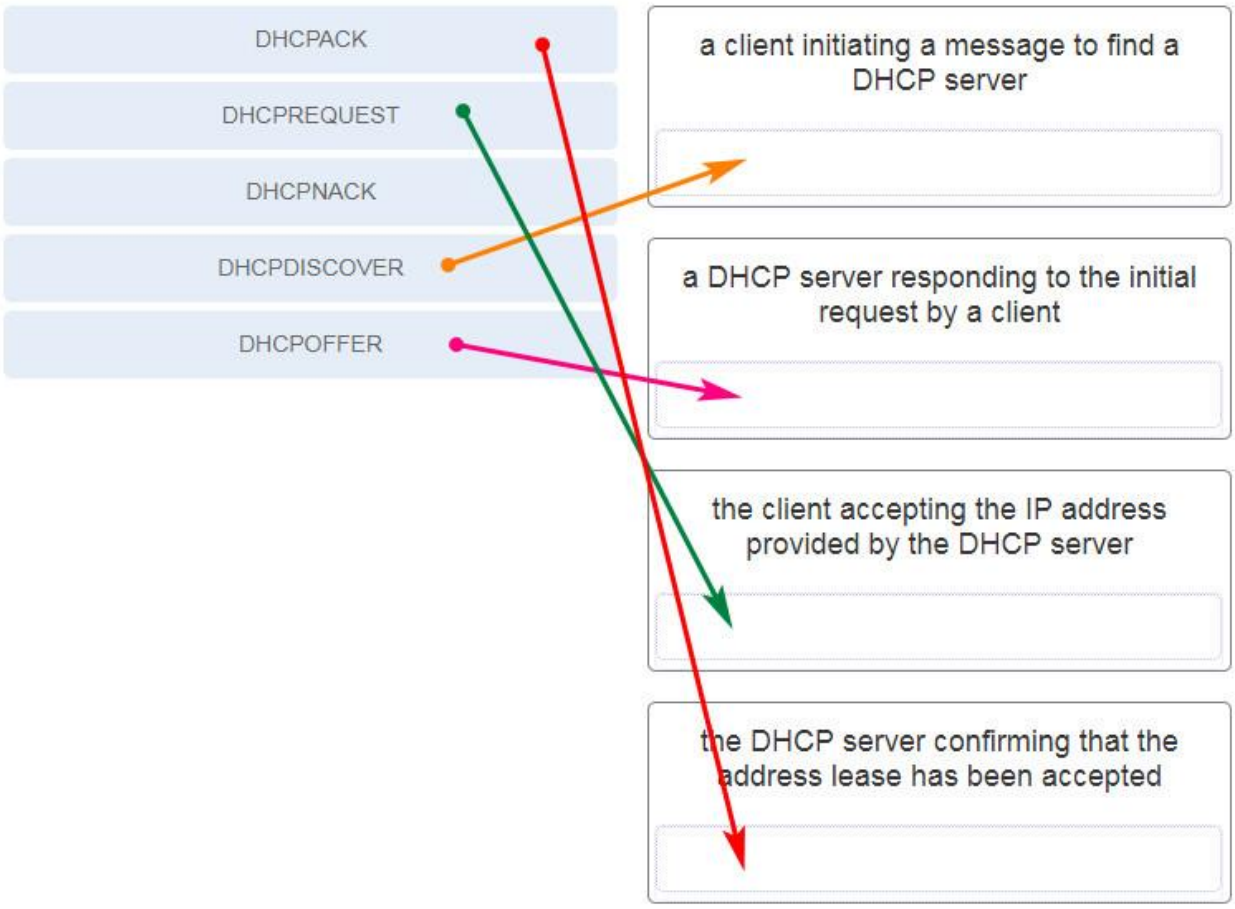
96. Refer to the exhibit. A network administrator is configuring inter-VLAN routing on a network. For now, only one VLAN is being used, but more will be added soon. What is the missing parameter that is shown as the highlighted question mark in the

graphic?



- It identifies the subinterface.
- **It identifies the VLAN number.**
- It identifies the native VLAN number.
- It identifies the type of encapsulation that is used.
- It identifies the number of hosts that are allowed on the interface.

97. Match each DHCP message type with its description. (Not all options are used.)



Explanation: Place the options in the following order:

- a client initiating a message to find a DHCP server – DHCPDISCOVER
- a DHCP server responding to the initial request by a client – DHCPOFFER
- the client accepting the IP address provided by the DHCP server – DHCPREQUEST
- the DHCP server confirming that the lease has been accepted – DHCPACK

98. What network attack seeks to create a DoS for clients by preventing them from being able to obtain a DHCP lease?

- IP address spoofing
- **DHCP starvation**
- CAM table attack
- DHCP spoofing

Explanation: DCHP starvation attacks are launched by an attacker with the intent to create a DoS for DHCP clients. To accomplish this goal, the attacker uses a tool that sends many DHCPDISCOVER messages in order to lease the entire pool of available IP addresses, thus denying them to legitimate hosts.

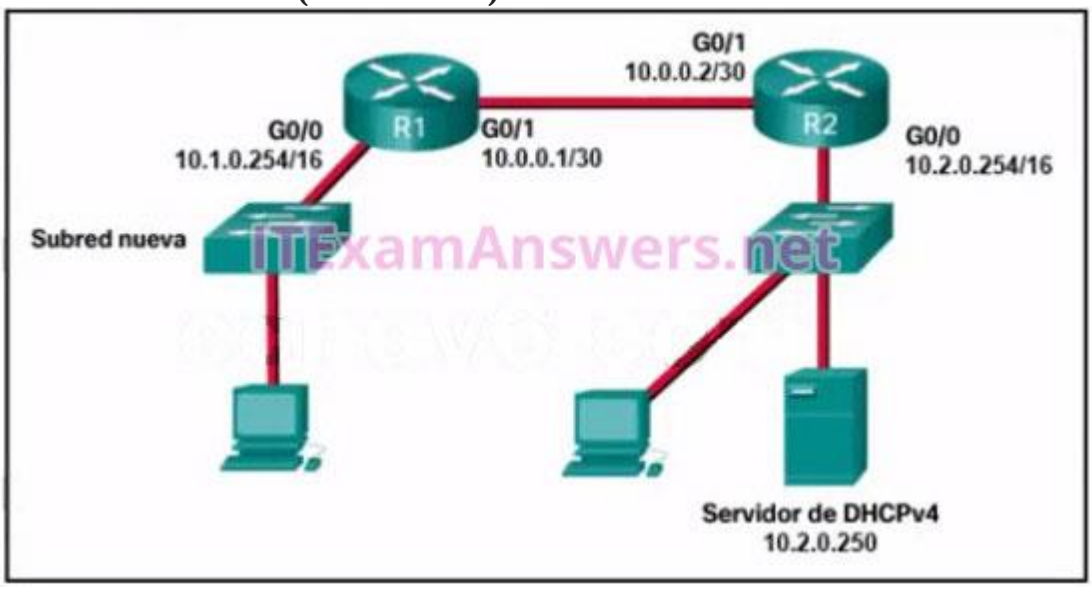
99. Refer to the exhibit. If the IP addresses of the default gateway router and the DNS server are correct, what is the configuration problem?

```
R1(config)# ip dhcp excluded-address 192.168.10.2 192.168.10.9
R1(config)# ip dhcp excluded-address 192.168.10.254
R1(config)# ip dhcp pool LAN-POOL-1
R1(dhcp-config)# network 192.168.10.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.10.1
R1(dhcp-config)# dns-server 192.168.11.5
R1(dhcp-config)# domain-name example.com
R1(dhcp-config)# end
```


- The DNS server and the default gateway router should be in the same subnet.
- **The IP address of the default gateway router is not contained in the excluded address list.**
- The default-router and dns-server commands need to be configured with subnet masks.
- The IP address of the DNS server is not contained in the excluded address list.

Explanation: In this configuration, the excluded address list should include the address that is assigned to the default gateway router. So the command should be ip dhcp excluded-address 192.168.10.1 192.168.10.9.

100. Refer to the exhibit. A network administrator has added a new subnet to the network and needs hosts on that subnet to receive IPv4 addresses from the DHCPv4 server.
What two commands will allow hosts on the new subnet to receive addresses from the DHCP4 server? (Choose two.)



- **R1(config-if)# ip helper-address 10.2.0.250**
- R1(config)# interface G0/1
- **R1(config)# interface G0/0**
- R2(config-if)# ip helper-address 10.2.0.250
- R2(config)# interface G0/0
- R1(config-if)# ip helper-address 10.1.0.254

Explanation: You need the router interface that is connected to the new subnet and the dhcp server address.
The ip helper-address command is used to configure a router to be a DHCPv4 relay. The command should be placed on the interface facing the DHCPv4 clients. When the command is applied on the router interface, the interface will receive DHCPv4 broadcast messages and forward them as unicast to the IP address of the DHCPv4 server.

101. What protocol or technology uses source IP to destination IP as a load-balancing mechanism?

- VTP
- **EtherChannel**
- DTP
- STP

102. What protocol should be disabled to help mitigate VLAN attacks?

- CDP
- ARP
- STP
- **DTP**

103. What protocol or technology requires switches to be in server mode or client mode?

- EtherChannel
- STP
- **VTP**
- DTP

104. What are two reasons a network administrator would segment a network with a Layer 2 switch? (Choose two.)

- to create fewer collision domains
- **to enhance user bandwidth**
- to create more broadcast domains
- to eliminate virtual circuits
- **to isolate traffic between segments**
- to isolate ARP request messages from the rest of the network

Explanation: A switch has the ability of creating temporary point-to-point connections between the directly-attached transmitting and receiving network devices. The two devices have full-bandwidth full-duplex connectivity during the transmission.

105. What command will enable a router to begin sending messages that allow it to configure a link-local address without using an IPv6 DHCP server?

- a static route
- the ipv6 route ::/0 command
- **the ipv6 unicast-routing command**
- the ip routing command

Explanation: To enable IPv6 on a router you must use the ipv6 unicast-routing global configuration command or use the ipv6 enable interface configuration command. This is equivalent to entering ip routing to enable IPv4 routing on a router when it has been turned off. Keep in mind that IPv4 is enabled on a router by default. IPv6 is not enabled by default.

106. A network administrator is using the router-on-a-stick model to configure a switch and a router for inter-VLAN routing. What configuration should be made on the switch port that connects to the router?

- Configure it as a trunk port and allow only untagged traffic.
- Configure the port as an access port and a member of VLAN1.
- **Configure the port as an 802.1q trunk port.**
- Configure the port as a trunk port and assign it to VLAN1.

Explanation: The port on the switch that connects to the router interface should be configured as a trunk port. Once it becomes a trunk port, it does not belong to any particular VLAN and will forward traffic from various VLANs.

107. What are three techniques for mitigating VLAN attacks? (Choose three.)

- Use private VLANs.
- Enable BPDU guard.
- **Enable trunking manually**
- Enable Source Guard.
- **Disable DTP.**
- **Set the native VLAN to an unused VLAN.**

Explanation: Mitigating a VLAN attack can be done by disabling Dynamic Trunking Protocol (DTP), manually setting ports to trunking mode, and by setting the native VLAN of trunk links to VLANs not in use.

108. Match the DHCP message types to the order of the DHCPv4 process. (Not all options are used.)

Step 1	DHCPACK → Step 4
Step 2	DHCPREQUEST → Step 3
Step 3	DHCPDISCOVER → Step 1
Step 4	DHCPREPLY →
	DHCPINFORMATION-REQUEST →
	DHCPOFFER → Step 2

Explanation: The broadcast DHCPDISCOVER message finds DHCPv4 servers on the network. When the DHCPv4 server receives a DHCPDISCOVER message, it reserves an available IPv4 address to lease to the client and sends the unicast DHCPOFFER message to the requesting client. When the client receives the DHCPOFFER from the server, it sends back a DHCPREQUEST. On receiving the DHCPREQUEST message the server replies with a unicast DHCPACK message. DHCPREPLY and DHCPINFORMATION-REQUEST are DHCPv6 messages.

109. In which situation would a technician use the show interfaces switch command?

- to determine if remote access is enabled
- **when packets are being dropped from a particular directly attached host**
- when an end device can reach local devices, but not remote devices
- to determine the MAC address of a directly attached network device on a particular interface

Explanation: The show interfaces command is useful to detect media errors, to see if packets are being sent and received, and to determine if any runts, giants, CRCs, interface resets, or other errors have occurred. Problems with reachability to a remote network would likely be caused by a misconfigured default gateway or other routing issue, not a switch issue. The show mac address-table command shows the MAC address of a directly attached device.

110. What is a drawback of the local database method of securing device access that can be solved by using AAA with centralized servers?

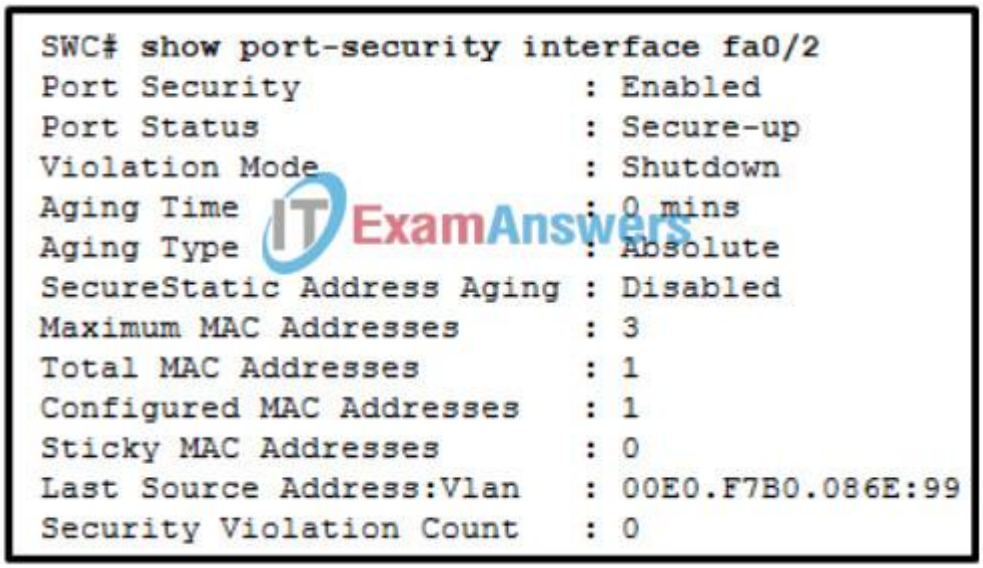
- There is no ability to provide accountability.
- **User accounts must be configured locally on each device, which is an unscalable authentication solution.**
- It is very susceptible to brute-force attacks because there is no username.
- The passwords can only be stored in plain text in the running configuration.

Explanation: The local database method of securing device access utilizes usernames and passwords that are configured locally on the router. This allows administrators to keep track of who logged in to the device and when. The passwords can also be encrypted in the configuration. However, the account information must be configured on each device where that account should have access, making this solution very difficult to scale.

111. What action does a DHCPv4 client take if it receives more than one DHCPOFFER from multiple DHCP servers?

- **It sends a DHCPREQUEST that identifies which lease offer the client is accepting.**
- It sends a DHCPNAK and begins the DHCP process over again.
- It discards both offers and sends a new DHCPDISCOVER.
- It accepts both DHCPOFFER messages and sends a DHCPACK.

112. Refer to the exhibit. The network administrator is configuring the port security feature on switch SWC. The administrator issued the command show port-security interface fa 0/2 to verify the configuration. What can be concluded from the output that is shown? (Choose three.)



- Three security violations have been detected on this interface.
- **This port is currently up.**
- The port is configured as a trunk link.
- **Security violations will cause this port to shut down immediately.**
- There is no device currently connected to this port.
- **The switch port mode for this interface is access mode.**

Explanation: Because the security violation count is at 0, no violation has occurred. The system shows that 3 MAC addresses are allowed on port fa0/2, but only one has been configured and no sticky MAC addresses have been learned. The port is up because of the port status of secure-up. The violation mode is what happens when an unauthorized device is attached to the port. A port must be in access mode in order to activate and use port security.

113. What method of wireless authentication is dependent on a RADIUS authentication server?

- WEP
- WPA Personal
- WPA2 Personal
- **WPA2 Enterprise**

114. A network administrator has found a user sending a double-tagged 802.1Q frame to a switch. What is the best solution to prevent this type of attack?

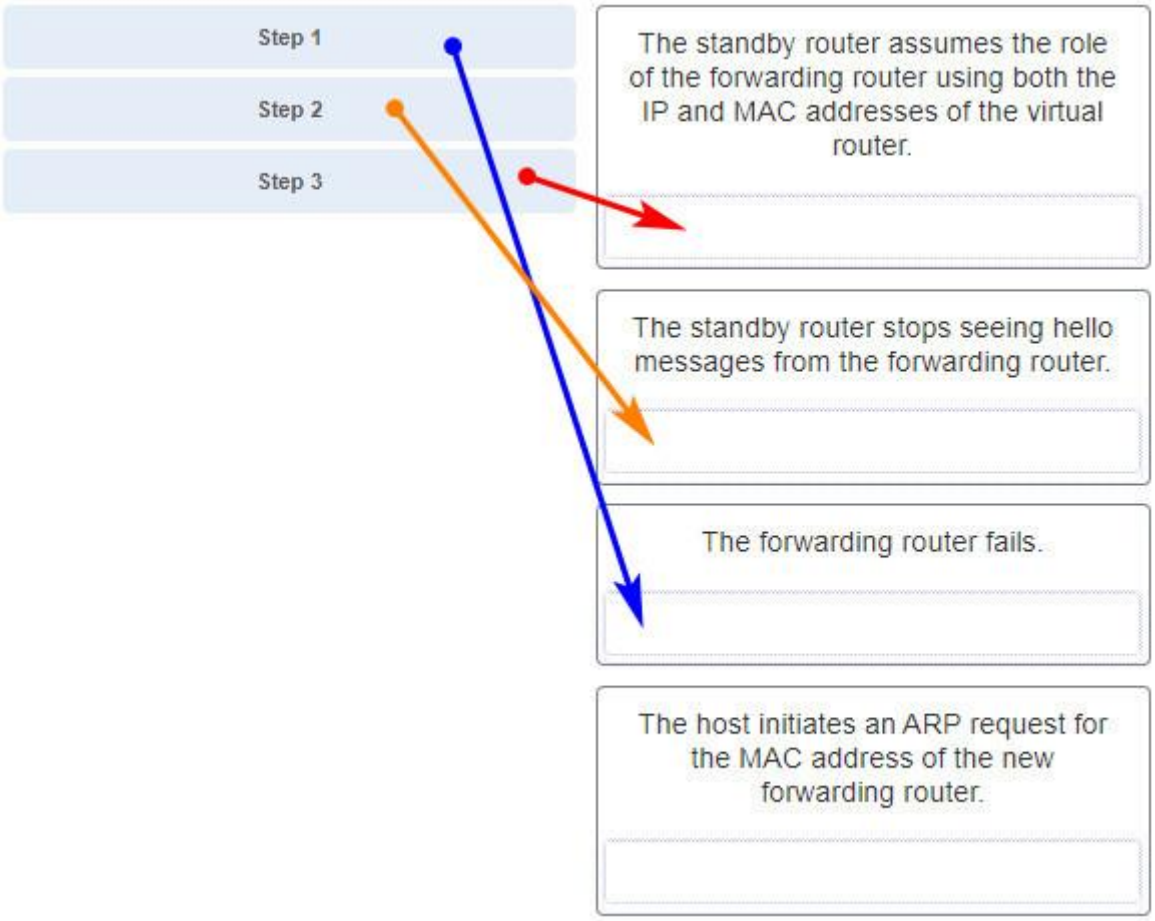
- The native VLAN number used on any trunk should be one of the active data VLANs.
- **The VLANs for user access ports should be different VLANs than any native VLANs used on trunk ports.**
- Trunk ports should be configured with port security.
- Trunk ports should use the default VLAN as the native VLAN number.

115. Refer to the exhibit. Which two conclusions can be drawn from the output? (Choose two.)

```
S1# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-------------------------------
1      Po2(SD)           -        Fa0/1(D)     Fa0/2(D)
```


- **The EtherChannel is down.**
- **The port channel ID is 2.**
- The port channel is a Layer 3 channel.
- The bundle is fully operational.
- The load-balancing method used is source port to destination port.

116. Match the step number to the sequence of stages that occur during the HSRP failover process. (Not all options are used.)



Explanation: Hot Standby Router Protocol (HSRP) is a Cisco-proprietary protocol that is designed to allow for transparent failover of a first-hop IPv4 device.

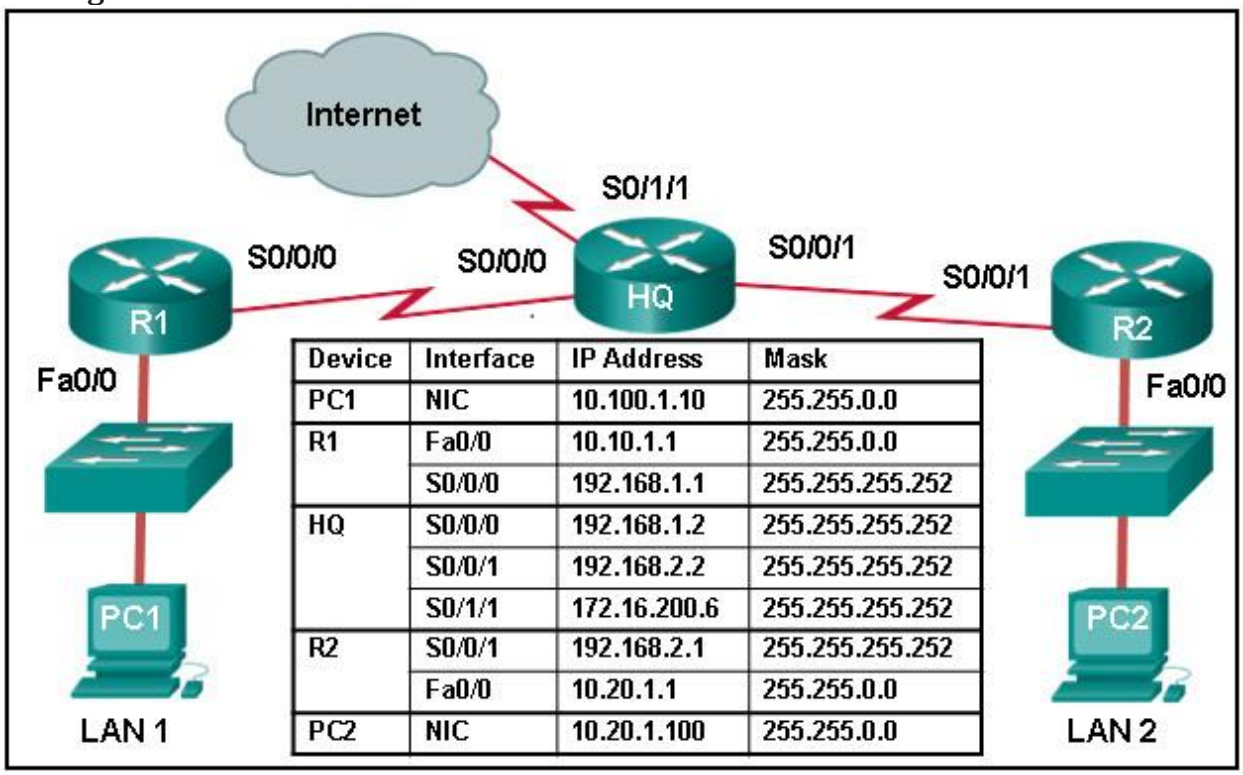
117. On a Cisco 3504 WLC Summary page (Advanced > Summary), which tab allows a network administrator to configure a particular WLAN with a WPA2 policy?

- **WLANs**
- SECURITY
- WIRELESS
- MANAGEMENT

Explanation: The **WLANs** tab in the Cisco 3504 WLC advanced **Summary** page allows a user to access the configuration of WLANs including security, QoS, and policy-mapping.

118. Refer to the exhibit. A network engineer is configuring IPv6 routing on the network. Which command issued on router HQ will configure a default route to the Internet to forward packets to an IPv6 destination network that is not listed in the

routing table?



Device	Interface	IP Address	Mask
PC1	NIC	10.100.1.10	255.255.0.0
R1	Fa0/0	10.10.1.1	255.255.0.0
	S0/0/0	192.168.1.1	255.255.255.252
HQ	S0/0/0	192.168.1.2	255.255.255.252
	S0/0/1	192.168.2.2	255.255.255.252
	S0/1/1	172.16.200.6	255.255.255.252
R2	S0/0/1	192.168.2.1	255.255.255.252
	Fa0/0	10.20.1.1	255.255.0.0
PC2	NIC	10.20.1.100	255.255.0.0

- ipv6 route ::/0 serial 0/0/0
- ip route 0.0.0.0 0.0.0.0 serial 0/1/1
- ipv6 route ::1/0 serial 0/1/1
- **ipv6 route ::/0 serial 0/1/1**

119. Users are complaining of sporadic access to the internet every afternoon. What should be done or checked?

- Create static routes to all internal networks and a default route to the internet.
- Verify that there is not a default route in any of the edge router routing tables.
- Create a floating static route to that network.
- **Check the statistics on the default route for oversaturation.**

120. What action takes place when the source MAC address of a frame entering a switch appears in the MAC address table associated with a different port?

- The switch purges the entire MAC address table.
- **The switch replaces the old entry and uses the more current port.**
- The switch updates the refresh timer for the entry.
- The switch forwards the frame out of the specified port.

121. A network administrator is configuring a WLAN. Why would the administrator use a WLAN controller?

- to centralize management of multiple WLANs
- to provide privacy and integrity to wireless traffic by using encryption
- **to facilitate group configuration and management of multiple WLANs through a WLC**

- to provide prioritized service for time-sensitive applications

122. A new Layer 3 switch is connected to a router and is being configured for interVLAN routing. What are three of the five steps required for the configuration? (Choose three.)

Case 1:

- installing a static route
- assigning the ports to the native VLAN
- **entering "no switchport" on the port connected to the router**
- modifying the default VLAN
- **assigning ports to VLANs**
- **enabling IP routing**
- adjusting the route metric

Case 2:

- establishing adjacencies
- adjusting the route metric
- **assigning ports to VLANs**
- implementing a routing protocol
- **creating SVI interfaces**
- installing a static route
- **creating VLANs**

Case 3:

- **assigning ports to VLANs**
- assigning the ports to the native VLAN
- modifying the default VLAN
- deleting the default VLAN
- **enabling IP routing**
- installing a static route
- **entering "no switchport" on the port connected to the router**

Case 4:

- installing a static route
- **enabling IP routing**
- modifying the default VLAN
- implementing a routing protocol
- **assigning ports to VLANs**
- assigning the ports to the native VLAN
- **creating SVI interfaces**

Case 5:

- **assigning ports to VLANs**
- assigning the ports to the native VLAN
- **enabling IP routing**
- modifying the default VLAN
- installing a static route
- implementing a routing protocol

- **creating SVI interfaces**

Case 6:

- establishing adjacencies
- **enabling IP routing**
- assigning the ports to the native VLAN
- adjusting the route metric
- modifying the default VLAN
- **entering "no switchport" on the port connected to the router**
- **assigning ports to VLANs**

Explanation: Steps to configure Layer 3 switch to route with a router:
Step 1. Configure the routed port.
Step 2. Enable routing.
Step 3. Configure routing.
Step 4. Verify routing.
Step 5. Verify connectivity.
Reference: 4.3.8 Packet Tracer Configure Layer 3 Switching and inter VLAN Routing

123. Which three statements accurately describe duplex and speed settings on Cisco 2960 switches? (Choose three.)

- **An autonegotiation failure can result in connectivity issues.**
- **When the speed is set to 1000 Mb/s, the switch ports will operate in full-duplex mode.**
- **The duplex and speed settings of each switch port can be manually configured.**
- Enabling autonegotiation on a hub will prevent mismatched port speeds when connecting the hub to the switch.
- By default, the speed is set to 100 Mb/s and the duplex mode is set to autonegotiation.
- By default, the autonegotiation feature is disabled.

124. Refer to the exhibit. A network administrator configures R1 for inter-VLAN routing between VLAN 10 and VLAN 20. However, the devices in VLAN 10 and VLAN 20 cannot communicate. Based on the configuration in the exhibit, what is a

possible cause for the problem?

```
R1# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# interface gigabitEthernet 0/0.1
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip add 192.168.10.254 255.255.255.0
R1(config-subif)# interface gigabitEthernet 0/0.20
R1(config-subif)# encapsulation dot1Q 2
R1(config-subif)# ip add 192.168.20.254 255.255.255.0
R1(config-subif)# exit
R1(config)# interface gigabitEthernet 0/0
R1(config-if)# no shutdown
```

- A. The port Gi0/0 should be configured as trunk port.
- **B. The encapsulation is misconfigured on a subinterface.**
- C. A no shutdown command should be added in each subinterface configuration.
- D. The command interface gigabitEthernet 0/0.1 is wrong.

125. A network administrator uses the spanning-tree portfast bpduguard default global configuration command to enable BPDU guard on a switch. However, BPDU guard is not activated on all access ports. What is the cause of the issue?

- BPDU guard needs to be activated in the interface configuration command mode.
- Access ports configured with root guard cannot be configured with BPDU guard.
- Access ports belong to different VLANs.
- **PortFast is not configured on all access ports.**

126. Which two types of spanning tree protocols can cause suboptimal traffic flows because they assume only one spanning-tree instance for the entire bridged network? (Choose two.)

- MSTP
- **RSTP**
- Rapid PVST+
- PVST+
- **STP**

127. Refer to the exhibit. A network administrator is configuring the router R1 for IPv6 address assignment. Based on the partial configuration, which IPv6 global

unicast address assignment scheme does the administrator intend to implement?

```
R1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 dhcp pool CORP_LAN

<output omitted>

R1(config)# interface gigabitEthernet 0/0
R1(config-if)# ipv6 address 2001:db8:aaaa:1::1/64
R1(config-if)# ipv6 dhcp server CORP_LAN
R1(config-if)# ipv6 nd managed-config-flag
R1(config-if)#
```

- **stateful**
- stateless
- manual configuration
- SLAAC

128. A WLAN engineer deploys a WLC and five wireless APs using the CAPWAP protocol with the DTLS feature to secure the control plane of the network devices. While testing the wireless network, the WLAN engineer notices that data traffic is being exchanged between the WLC and the APs in plain-text and is not being encrypted. What is the most likely reason for this?

- DTLS only provides data security through authentication and does not provide encryption for data moving between a wireless LAN controller (WLC) and an access point (AP).
- **Although DTLS is enabled by default to secure the CAPWAP control channel, it is disabled by default for the data channel.**
- DTLS is a protocol that only provides security between the access point (AP) and the wireless client.
- Data encryption requires a DTLS license to be installed on each access point (AP) prior to being enabled on the wireless LAN controller (WLC).

Explanation: DTLS is a protocol which provides security between the AP and the WLC. It allows them to communicate using encryption and prevents eavesdropping or tampering.
DTLS is enabled by default to secure the CAPWAP control channel but is disabled by default for the data channel. All CAPWAP management and control traffic exchanged between an AP and WLC is encrypted and secured by default to provide control plane privacy and prevent Man-In-the-Middle (MITM) attacks.

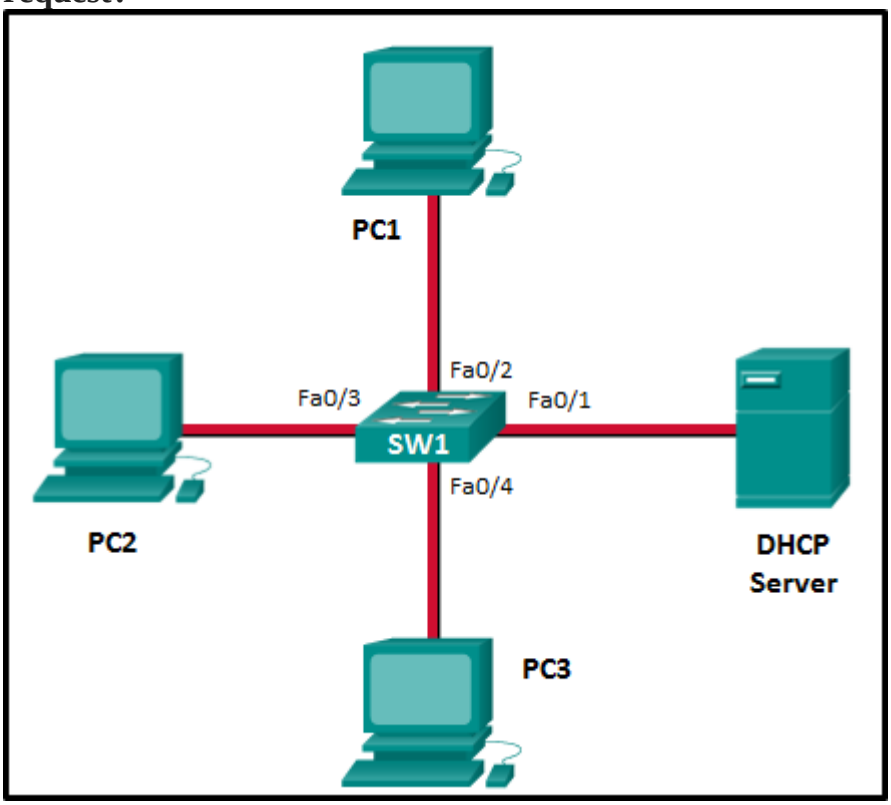
129. A new switch is to be added to an existing network in a remote office. The network administrator does not want the technicians in the remote office to be able to add new VLANs to the switch, but the switch should receive VLAN updates from

the VTP domain. Which two steps must be performed to configure VTP on the new switch to meet these conditions? (Choose two.)

- **Configure the new switch as a VTP client.**
- **Configure the existing VTP domain name on the new switch.**
- Configure an IP address on the new switch.
- Configure all ports of both switches to access mode.
- Enable VTP pruning.

Explanation: Before the switch is put in the correct VTP domain and in client mode, the switch must be connected to any other switch in the VTP domain through a trunk in order to receive/transmit VTP information.

130. Refer to the exhibit. Consider that the main power has just been restored. PC3 issues a broadcast IPv4 DHCP request. To which port will SW1 forward this request?



- **to Fa0/1, Fa0/2, and Fa0/3 only**
- to Fa0/1, Fa0/2, Fa0/3, and Fa0/4
- to Fa0/1 only
- to Fa0/1, Fa0/2, and Fa0/4 only
- to Fa0/1 and Fa0/2 only

131. What action takes place when the source MAC address of a frame entering a switch is not in the MAC address table?

- The switch adds a MAC address table entry for the destination MAC address and the egress port.

- **The switch adds the MAC address and incoming port number to the table.**
- The switch replaces the old entry and uses the more current port.
- The switch updates the refresh timer for the entry.

132. Employees are unable to connect to servers on one of the internal networks. What should be done or checked?

- **Use the "show ip interface brief" command to see if an interface is down.**
- Verify that there is not a default route in any of the edge router routing tables.
- Create static routes to all internal networks and a default route to the internet.
- Check the statistics on the default route for oversaturation.

133. What is the effect of entering the ip dhcp snooping configuration command on a switch?

- **It enables DHCP snooping globally on a switch.**
- It enables PortFast globally on a switch.
- It disables DTP negotiations on trunking ports.
- It manually enables a trunk link.

134. An administrator notices that large numbers of packets are being dropped on one of the branch routers. What should be done or checked?

- Create static routes to all internal networks and a default route to the internet.
- Create extra static routes to the same location with an AD of 1.
- Check the statistics on the default route for oversaturation.
- **Check the routing table for a missing static route.**

135. What are two switch characteristics that could help alleviate network congestion? (Choose two.)

- **fast internal switching**
- **large frame buffers**
- store-and-forward switching
- low port density
- frame check sequence (FCS) check

136. What is a result of connecting two or more switches together?

- The number of broadcast domains is increased.
- **The size of the broadcast domain is increased.**
- The number of collision domains is reduced.
- The size of the collision domain is increased.

Explanation:: When two or more switches are connected together, the size of the broadcast domain is increased and so is the number of collision domains. The number of broadcast domains is increased only when routers are added.

138. Branch users were able to access a site in the morning but have had no connectivity with the site since lunch time. What should be done or checked?

- Verify that the static route to the server is present in the routing table.
- **Use the "show ip interface brief" command to see if an interface is down.**

- Check the configuration on the floating static route and adjust the AD.
- Create a floating static route to that network.

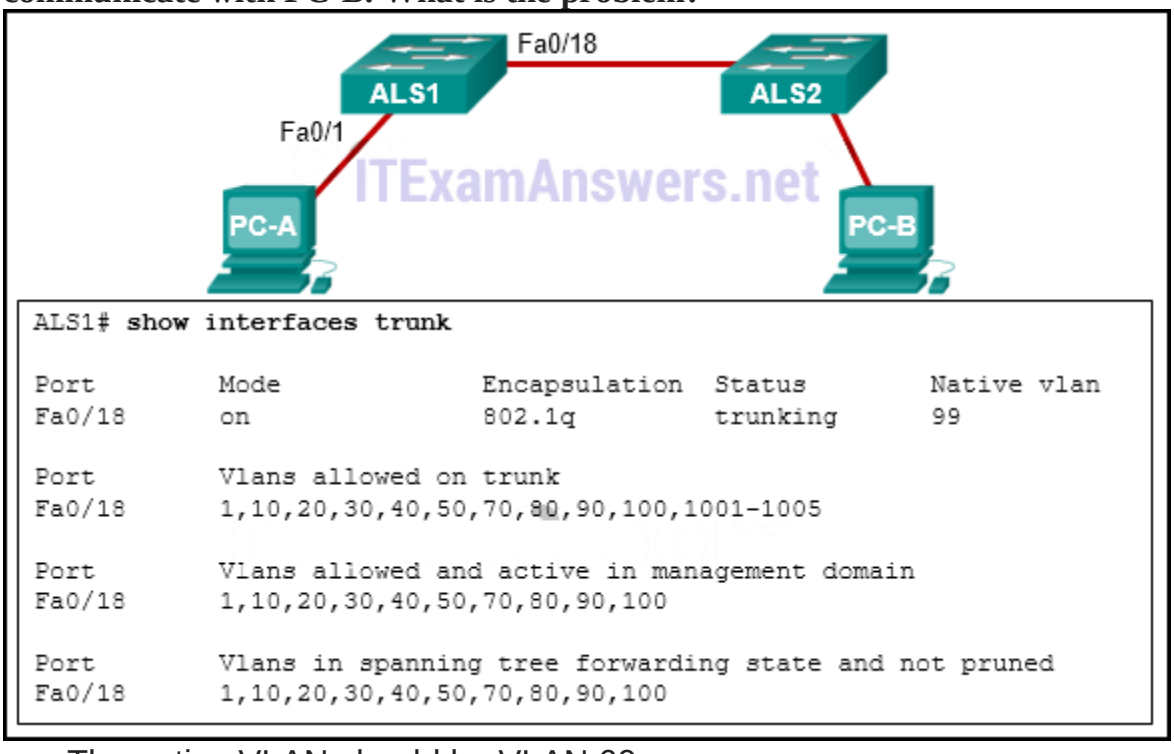
139. What is the effect of entering the switchport port-security configuration command on a switch?

- It dynamically learns the L2 address and copies it to the running configuration.
- **It enables port security on an interface.**
- It enables port security globally on the switch.
- It restricts the number of discovery messages, per second, to be received on the interface.

140. A network administrator is configuring a WLAN. Why would the administrator use multiple lightweight APs?

- to centralize management of multiple WLANs
- to monitor the operation of the wireless network
- to provide prioritized service for time-sensitive applications
- **to facilitate group configuration and management of multiple WLANs through a WLC**

141. Refer to the exhibit. PC-A and PC-B are both in VLAN 60. PC-A is unable to communicate with PC-B. What is the problem?




```
ALS1# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/18      on               802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/18      1,10,20,30,40,50,70,80,90,100,1001-1005

Port        Vlans allowed and active in management domain
Fa0/18      1,10,20,30,40,50,70,80,90,100

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/18      1,10,20,30,40,50,70,80,90,100
```

- The native VLAN should be VLAN 60.
- The native VLAN is being pruned from the link.
- The trunk has been configured with the switchport nonegotiate command.
- The VLAN that is used by PC-A is not in the list of allowed VLANs on the trunk.

Explanation: Because PC-A and PC-B are connected to different switches, traffic between them must flow over the trunk link. Trunks can be configured so that they only allow traffic for particular VLANs to cross the link. In this scenario, VLAN 60, the VLAN that is associated with PC-A and PC-B, has not been allowed across the link, as shown by the output of show interfaces trunk.

142. A network administrator is configuring a WLAN. Why would the administrator use RADIUS servers on the network?

- to centralize management of multiple WLANs
- **to restrict access to the WLAN by authorized, authenticated users only**
- to facilitate group configuration and management of multiple WLANs through a WLC
- to monitor the operation of the wireless network

143. What is the effect of entering the switchport mode access configuration command on a switch?

- It enables BPDU guard on a specific port.
- It manually enables a trunk link.
- It disables an unused port.
- **It disables DTP on a non-trunking interface.**

144. A network administrator has configured a router for stateless DHCPv6 operation. However, users report that workstations are not receiving DNS server information. Which two router configuration lines should be verified to ensure that stateless DHCPv6 service is properly configured? (Choose two.)

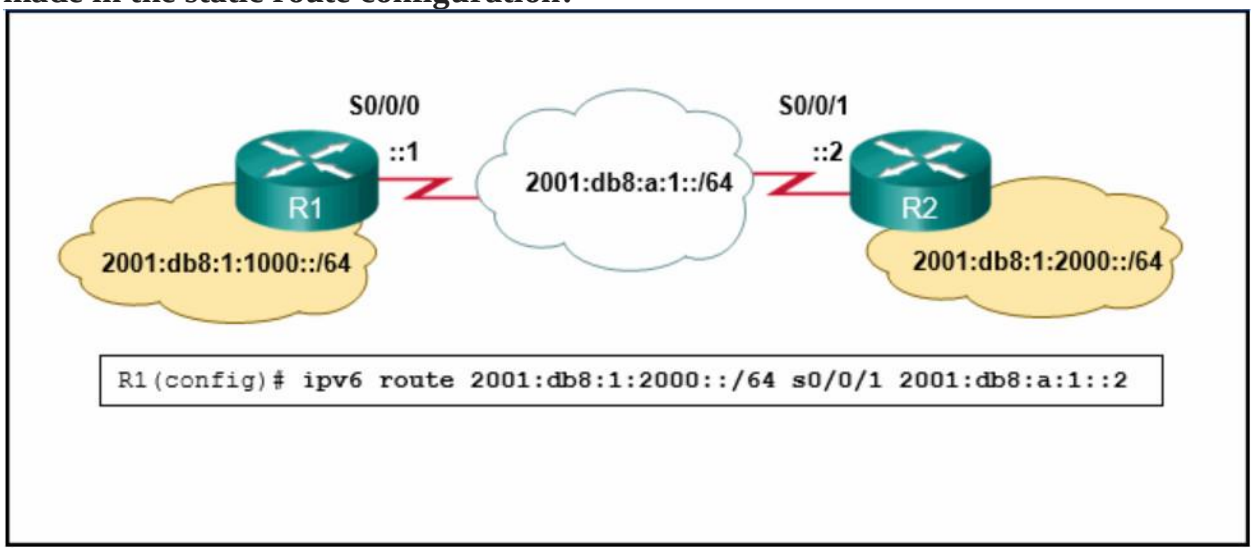
- The domain-name line is included in the `ipv6 dhcp pool` section.
- **The dns-server line is included in the `ipv6 dhcp pool` section.**
- **The `ipv6 nd other-config-flag` is entered for the interface that faces the LAN segment.**
- The address prefix line is included in the `ipv6 dhcp pool` section.
- The `ipv6 nd managed-config-flag` is entered for the interface that faces the LAN segment.

Explanation: To use the stateless DHCPv6 method, the router must inform DHCPv6 clients to configure a SLAAC IPv6 address and contact the DHCPv6 server for additional configuration parameters, such as the DNS server address. This is done through the command **ipv6 nd other-config-flag** entered at the interface configuration mode. The DNS server address is indicated in the **ipv6 dhcp pool** configuration.

145. A network administrator is configuring a WLAN. Why would the administrator disable the broadcast feature for the SSID?

- **to eliminate outsiders scanning for available SSIDs in the area**
- to centralize management of multiple WLANs
- to facilitate group configuration and management of multiple WLANs through a WLC
- to provide prioritized service for time-sensitive applications

146. Refer to the exhibit. An administrator is attempting to install an IPv6 static route on router R1 to reach the network attached to router R2. After the static route command is entered, connectivity to the network is still failing. What error has been made in the static route configuration?



- The next hop address is incorrect.
- **The interface is incorrect.**
- The destination network is incorrect.
- The network prefix is incorrect.

Explanation: In this example the interface in the static route is incorrect. The interface should be the exit interface on R1, which is s0/0/0.

147. What action takes place when a frame entering a switch has a unicast destination MAC address that is not in the MAC address table?

- The switch updates the refresh timer for the entry.
- The switch resets the refresh timer on all MAC address table entries.
- The switch replaces the old entry and uses the more current port.
- **The switch will forward the frame out all ports except the incoming port.**

148. A junior technician was adding a route to a LAN router. A traceroute to a device on the new network revealed a wrong path and unreachable status. What should be done or checked?

- Create a floating static route to that network.
- Check the configuration on the floating static route and adjust the AD.
- **Check the configuration of the exit interface on the new static route.**
- Verify that the static route to the server is present in the routing table.

149. What is the effect of entering the ip arp inspection vlan 10 configuration command on a switch?

- It specifies the maximum number of L2 addresses allowed on a port.
- **It enables DAI on specific switch interfaces previously configured with DHCP snooping.**

- It enables DHCP snooping globally on a switch.
- It globally enables BPDU guard on all PortFast-enabled ports.

150. What protocol or technology manages trunk negotiations between switches?

- VTP
- EtherChannel
- **DTP**
- STP

151. A network administrator is configuring a WLAN. Why would the administrator apply WPA2 with AES to the WLAN?

- to reduce the risk of unauthorized APs being added to the network
- to centralize management of multiple WLANs
- to provide prioritized service for time-sensitive applications
- **to provide privacy and integrity to wireless traffic by using encryption**

152. Users on a LAN are unable to get to a company web server but are able to get elsewhere. What should be done or checked?

- Ensure that the old default route has been removed from the company edge routers.
- **Verify that the static route to the server is present in the routing table.**
- Check the configuration on the floating static route and adjust the AD.
- Create a floating static route to that network.

153. What IPv6 prefix is designed for link-local communication?

- 2001::/3
- ff00::/8
- fc::/07
- **fe80::/10**

154. What is the effect of entering the `ip dhcp snooping limit rate 6` configuration command on a switch?

- It displays the IP-to-MAC address associations for switch interfaces.
- It enables port security globally on the switch.
- **It restricts the number of discovery messages, per second, to be received on the interface.**
- It dynamically learns the L2 address and copies it to the running configuration.

155. A network administrator is configuring a WLAN. Why would the administrator change the default DHCP IPv4 addresses on an AP?

- to eliminate outsiders scanning for available SSIDs in the area
- to reduce the risk of unauthorized APs being added to the network
- **to reduce outsiders intercepting data or accessing the wireless network by using a well-known address range**
- to reduce the risk of interference by external devices such as microwave ovens

156. What is the effect of entering the ip arp inspection validate src-mac configuration command on a switch?

- **It checks the source L2 address in the Ethernet header against the sender L2 address in the ARP body.**
- It disables all trunk ports.
- It displays the IP-to-MAC address associations for switch interfaces.
- It enables portfast on a specific switch interface.

157. What protocol or technology is a Cisco proprietary protocol that is automatically enabled on 2960 switches?

- **DTP**
- STP
- VTP
- EtherChannel

158. What address and prefix length is used when configuring an IPv6 default static route?

- **::/0**
- FF02::1/8
- 0.0.0.0/0
- ::1/128

159. What are two characteristics of Cisco Express Forwarding (CEF)? (Choose two.)

- When a packet arrives on a router interface, it is forwarded to the control plane where the CPU matches the destination address with a matching routing table entry.
- **This is the fastest forwarding mechanism on Cisco routers and multilayer switches.**
- With this switching method, flow information for a packet is stored in the fast-switching cache to forward future packets to the same destination without CPU intervention.
- **Packets are forwarded based on information in the FIB and an adjacency table.**
- When a packet arrives on a router interface, it is forwarded to the control plane where the CPU searches for a match in the fast-switching cache.

160. Which term describes the role of a Cisco switch in the 802.1X port-based access control?

- agent
- supplicant
- **authenticator**
- authentication server

161. Which Cisco solution helps prevent ARP spoofing and ARP poisoning attacks?

- **Dynamic ARP Inspection**
- IP Source Guard
- DHCP Snooping
- Port Security

162. What is an advantage of PVST+?

- PVST+ optimizes performance on the network through autoselection of the root bridge.
- PVST+ reduces bandwidth consumption compared to traditional implementations of STP that use CST.
- PVST+ requires fewer CPU cycles for all the switches in the network.
- **PVST+ optimizes performance on the network through load sharing.**

PVST+ results in optimum load balancing. However, this is accomplished by manually configuring switches to be elected as root bridges for different VLANs on the network. The root bridges are not automatically selected. Furthermore, having spanning-tree instances for each VLAN actually consumes more bandwidth and it increases the CPU cycles for all the switches in the network.

163. What protocol or technology uses a standby router to assume packet-forwarding responsibility if the active router fails?

- EtherChannel
- DTP
- **HSRP**
- VTP

164. What is the effect of entering the show ip dhcp snooping binding configuration command on a switch?

- It switches a trunk port to access mode.
- It checks the source L2 address in the Ethernet header against the sender L2 address in the ARP body.
- It restricts the number of discovery messages, per second, to be received on the interface.
- **It displays the IP-to-MAC address associations for switch interfaces.**

165. What action takes place when the source MAC address of a frame entering a switch is in the MAC address table?

- The switch forwards the frame out of the specified port.
- **The switch updates the refresh timer for the entry.**
- The switch replaces the old entry and uses the more current port.
- The switch adds a MAC address table entry for the destination MAC address and the egress port.

166. A small publishing company has a network design such that when a broadcast is sent on the LAN, 200 devices receive the transmitted broadcast. How can the network administrator reduce the number of devices that receive broadcast traffic?

- Add more switches so that fewer devices are on a particular switch.
- Replace the switches with switches that have more ports per switch. This will allow more devices on a particular switch.
- **Segment the LAN into smaller LANs and route between them.***
- Replace at least half of the switches with hubs to reduce the size of the broadcast domain.

Explain: By dividing the one big network into two smaller network, the network administrator has created two smaller broadcast domains. When a broadcast is sent on the network now, the broadcast will only be sent to the devices on the same Ethernet LAN. The other LAN will not receive the broadcast.

167. What defines a host route on a Cisco router?

- The link-local address is added automatically to the routing table as an IPv6 host route.
- **An IPv4 static host route configuration uses a destination IP address of a specific device and a /32 subnet mask.**
- A host route is designated with a C in the routing table.
- A static IPv6 host route must include the interface type and the interface number of the next hop router.

168. What else is required when configuring an IPv6 static route using a next-hop link-local address?

- administrative distance
- ip address of the neighbor router
- network number and subnet mask on the interface of the neighbor router
- **interface number and type**

169. A technician is configuring a wireless network for a small business using a SOHO wireless router. Which two authentication methods are used, if the router is configured with WPA2? (Choose two.)

- **personal**
- AES
- TKIP
- WEP
- **enterprise**

170. Which mitigation technique would prevent rogue servers from providing false IPv6 configuration parameters to clients?

- **enabling DHCPv6 Guard**
- enabling RA Guard
- implementing port security on edge ports
- disabling CDP on edge ports

Explanation: DHCPv6 Guard is a feature designed to ensure that rogue DHCPv6 servers are not able to hand out addresses to clients, redirect client traffic, or starve out the DHCPv6 server and cause a DoS attack. DHCPv6 Guard requires a policy to be configured in DHCP Guard configuration mode, and DHCPv6 Guard is enabled on an interface-by-interface basis.

171. A PC has sent an RS message to an IPv6 router attached to the same network. Which two pieces of information will the router send to the client? (Choose two.)

- **prefix length**
- subnet mask in dotted decimal notation
- domain name

- administrative distance
- **prefix**
- DNS server IP address

Explanation: Router is part of the IPv6 all-routers group and received the RS message. It generates an RA containing the local network prefix and prefix length (e.g., 2001:db8:acad:1::/64)

172. While attending a conference, participants are using laptops for network connectivity. When a guest speaker attempts to connect to the network, the laptop fails to display any available wireless networks. The access point must be operating in which mode?

- mixed
- passive
- **active**
- open

Explanation: Active is a mode used to configure an access point so that clients must know the SSID to connect to the access point. APs and wireless routers can operate in a mixed mode meaning that that multiple wireless standards are supported. Open is an authentication mode for an access point that has no impact on the listing of available wireless networks for a client. When an access point is configured in passive mode, the SSID is broadcast so that the name of wireless network will appear in the listing of available networks for clients.

173. Which three components are combined to form a bridge ID?

- **extended system ID**
- cost
- IP address
- **bridge priority**
- **MAC address**
- port ID

Explanation: The three components that are combined to form a bridge ID are bridge priority, extended system ID, and MAC address.