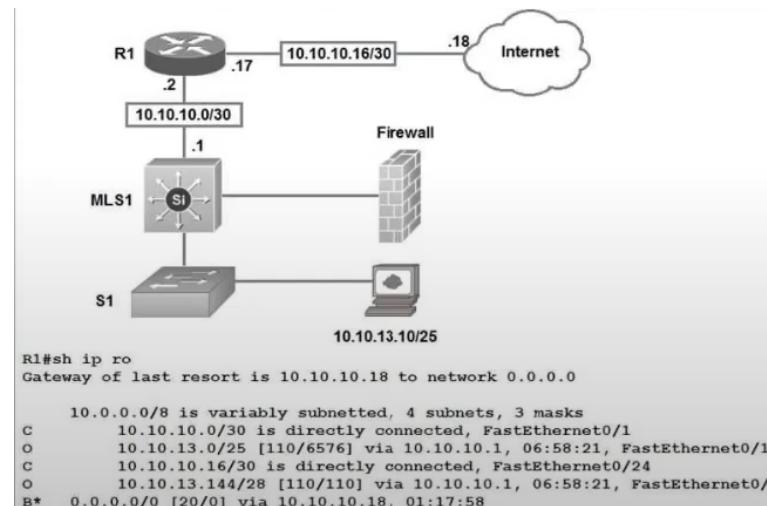


CCNA 200-301 QA

⌚ Created	@August 10, 2023 3:39 PM
▼ Status	Open
⌚ Updated	@August 10, 2023 5:25 PM

Question And Answers

Q1: Which type of route does R1 use to reach host 10.10.13.10/32 according to the exhibit?



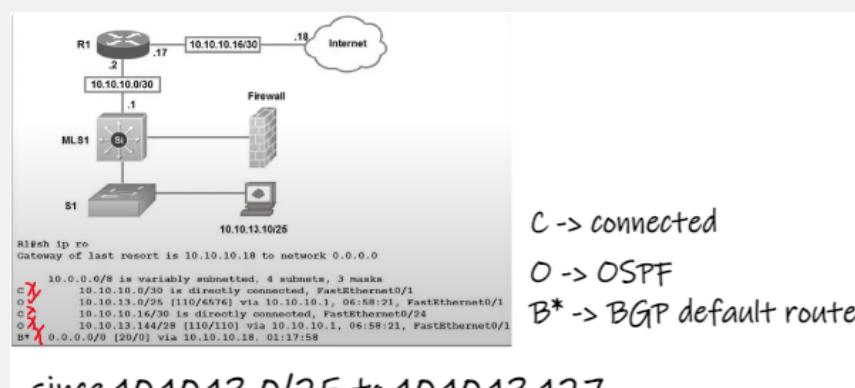
- A. Default route
- B. Network route
- C. Host route
- D. Floating static route

▼ Answer

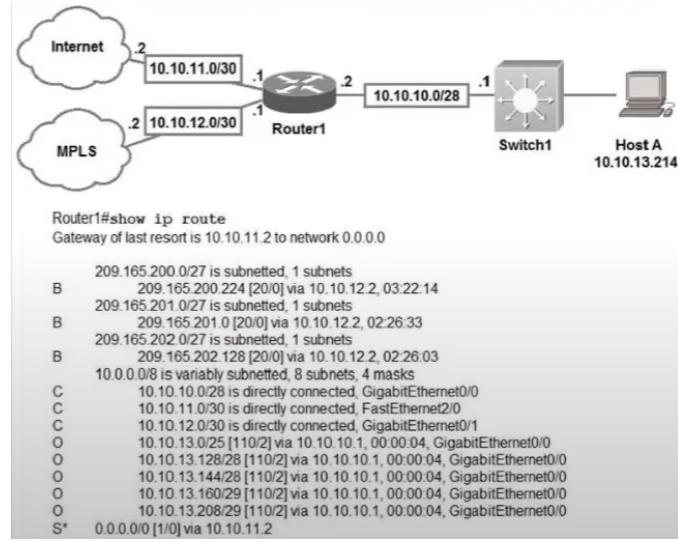
- A. Default route
- B. Network route**
- C. Host route
- D. Floating static route



More details Steps:



Q2: Which prefix is used by Router1 to reach Host A according to the exhibit?



- A. 10.10.10.0/28
- B. 10.10.13.0/25
- C. 10.10.13.144/28
- D. 10.10.13.208/29

▼ Answer

- A. 10.10.10.0/28
- B. 10.10.13.0/25
- C. 10.10.13.144/28
- D. 10.10.13.208/29**

More details Steps:

```

Router1#show ip route
Gateway of last resort is 10.10.11.2 to network 0.0.0.0

 209.165.200.0/27 is subnetted, 1 subnets
B  209.165.200.224 [20/0] via 10.10.12.2, 03:22:14
B  209.165.201.0/27 is subnetted, 1 subnets
B  209.165.201.0 [20/0] via 10.10.12.2, 02:26:33
B  209.165.202.0/27 is subnetted, 1 subnets
B  209.165.202.128 [20/0] via 10.10.12.2, 02:26:03
 10.0.0.0/8 is variably subnetted, 8 subnets, 4 masks
C  10.10.10.0/28 is directly connected, GigabitEthernet0/0
C  10.10.11.0/30 is directly connected, FastEthernet2/0
C  10.10.12.0/30 is directly connected, GigabitEthernet0/1
O  10.10.13.128/28 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
O  10.10.13.144/28 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
O  10.10.13.160/29 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
O  10.10.13.208/29 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
S*  0.0.0.0/1[0] via 10.10.11.2

```

C -> connected
O -> OSPF
B -> BGP
S* -> Default route

since 10.10.13.208/29 to 10.10.13.215

Q3: Match the protocols with their corresponding characteristics:

Characteristics	FTP	TFTP
Provides reliability when an IOS image does not boot up		
Does not use authentication		
Uses port 69		
Uses ports 20 and 21		
Uses TCP		
Uses UDP		

▼ Answer

Characteristics	Protocols
Provides reliability when an IOS image does not boot up	FTP
Does not use authentication	TFTP
Uses port 69	TFTP
Uses ports 20 and 21	FTP
Uses TCP	FTP
Uses UDP	TFTP

Q4: A frame that enters a switch fails the Frame_CheckSequence. Which two interface counters are incremented? (Choose two.)

- A. input errors
- B. frame
- C. giants
- D. CRC
- E. runts

▼ Answer

A. input errors

- B. frame
- C. giants
- D. CRC**
- E. runts



More details Steps:

When a frame fails the Frame_CheckSequence, two interface counters are incremented: Input errors and CRC. The Input errors counter is incremented because the switch detected an error in the frame as it was being received on an interface. The CRC counter is incremented because the switch determined that the frame's cyclic redundancy check (CRC) value did not match the checksum value calculated by the switch. This indicates that the frame was corrupted during transmission and could not be delivered to its intended destination.

Q5: Match the prefixes with the corresponding IP address ranges:

Prefix	IP Address Range
172.28.228.144/18	
172.28.228.144/21	
172.28.228.144/23	
172.28.228.144/25	
172.28.228.144/29	

▼ Answer

Prefix	IP Address Range
172.28.228.144/18	172.28.192.1 - 172.28.255.254
172.28.228.144/21	172.28.224.1 - 172.28.231.254
172.28.228.144/23	172.28.228.1 - 172.28.229.254
172.28.228.144/25	172.28.228.129 - 172.28.228.254
172.28.228.144/29	172.28.228.145 - 172.28.228.150

Q6: How do TCP and UDP differ in the way they establish a connection between two endpoints?

- A. TCP uses the three-way handshake, and UDP does not guarantee message delivery.
- B. TCP uses synchronization packets, and UDP uses acknowledgement packets.
- C. UDP provides reliable message transfer, and TCP is a connectionless protocol.
- D. UDP uses SYN, SYN ACK, and FIN bits in the frame header while TCP uses SYN, SYN ACK, and ACK bits.

▼ Answer

A. TCP uses the three-way handshake, and UDP does not guarantee message delivery.

- B. TCP uses synchronization packets, and UDP uses acknowledgement packets.
- C. UDP provides reliable message transfer, and TCP is a connectionless protocol.
- D. UDP uses SYN, SYN ACK, and FIN bits in the frame header while TCP uses SYN, SYN ACK, and ACK bits.

**More details Steps:**

TCP uses a three-way handshake to establish a connection between two endpoints. UDP does not establish a connection between two endpoints. It is a connectionless protocol, which means that it does not guarantee message delivery. UDP simply sends packets to the destination endpoint without checking if they have been received or not. This makes UDP faster than TCP, but it also means that data can be lost or arrive out of order.

Q7: Which 802.11 frame type is association response?

- A. management
- B. protected frame
- C. action
- D. control

▼ Answer**A. management**

- B. protected frame
- C. action
- D. control

**More details Steps:**

One of the frame types in 802.11 is the management frame. The management frames are used for the management of the wireless network. Association response is a type of management frame that is sent by an access point (AP) in response to an association request frame sent by a wireless client.

When a wireless client wants to connect to a wireless network, it sends an association request frame to the AP. The AP then sends an association response frame back to the client, indicating whether or not the association request has been accepted.

Q8: In which way does a spine-and-leaf architecture allow for scalability in a network when additional access ports are required?

- A. A spine switch and a leaf switch can be added with redundant connections between them.
- B. A spine switch can be added with at least 40 GB uplinks.
- C. A leaf switch can be added with connections to every spine switch.
- D. A leaf switch can be added with a single connection to a core spine switch

▼ Answer

- A. A spine switch and a leaf switch can be added with redundant connections between them.
- B. A spine switch can be added with at least 40 GB uplinks.
- C. A leaf switch can be added with connections to every spine switch.**
- D. A leaf switch can be added with a single connection to a core spine switch

**More details Steps:**

This architecture allows for scalability in the network when additional access ports are required because new leaf switches can be added with connections to every spine switch. This provides redundancy and ensures that traffic can be distributed efficiently across the network.

Option A is incorrect because adding a spine switch and a leaf switch with redundant connections between them would not necessarily provide additional access ports.

Option B is incorrect because adding a spine switch with at least 40 GB uplinks would increase the bandwidth capacity, but it would not necessarily provide additional access ports.

Option D is incorrect because adding a leaf switch with a single connection to a core spine switch would not provide redundancy and could create a bottleneck in the network.

Q9: Which statement identifies the functionality of virtual machines?

- A. The hypervisor communicates on Layer 3 without the need for additional resources.
- B. Each hypervisor can support a single virtual machine and a single software switch.
- C. The hypervisor can virtual physical components including CPU, memory, and storage.
- D. Virtualized servers run most efficiently when they are physically connected to a switch that is separate from the hypervisor.

▼ Answer

- A. The hypervisor communicates on Layer 3 without the need for additional resources.
- B. Each hypervisor can support a single virtual machine and a single software switch.
- C. The hypervisor can virtual physical components including CPU, memory, and storage.**
- D. Virtualized servers run most efficiently when they are physically connected to a switch that is separate from the hypervisor.



More details Steps:

Virtual machines (VMs) are software-based representations of physical computers that run on a hypervisor, which is a layer of software that manages the virtualization of the hardware resources. The hypervisor allows multiple VMs to run on a single physical server, each with its own virtualized hardware resources.

Option A is incorrect because the hypervisor typically operates at Layer 1 or 2 and relies on the host operating system for Layer 3 communication.

Option B is incorrect because a single hypervisor can typically support multiple virtual machines and virtual switches.

Option D is incorrect because virtualized servers can run efficiently even when connected to the same physical switch as the hypervisor.

Q10: Which command automatically generates an IPv6 address from a specified IPv6 prefix and MAC address of an interface?

- A. ipv6 address dhcp
- B. ipv6 address 2001:DB8:5:112::/64
- C. ipv6 address autoconfig
- D. ipv6 address link-local 2001:DB8:5:112::2/64 link-local

▼ Answer

- A. ipv6 address dhcp
- B. ipv6 address 2001:DB8:5:112::/64
- C. ipv6 address autoconfig**
- D. ipv6 address link-local 2001:DB8:5:112::2/64 link-local



More details Steps:

The command "ipv6 address autoconfig" automatically generates an IPv6 address from a specified IPv6 prefix and MAC address of an interface. This process is known as stateless address autoconfiguration (SLAAC).

When a device is connected to a network, it can use SLAAC to automatically configure its own IPv6 address by combining the network prefix received from the router with its own MAC address. The resulting address is unique and can be used to communicate on the network.

Option A, "ipv6 address dhcp", configures the device to obtain an IPv6 address from a DHCPv6 server.

Option B, "ipv6 address 2001:DB8:5:112::/64", configures a static IPv6 address on the interface.

Option D, "ipv6 address link-local 2001:DB8:5:112::2/64 link-local", configures a link-local IPv6 address on the interface.

Q11: When configuring IPv6 on an interface, which two IPv6 multicast groups are joined? (Choose two.)

- A. 2000::/3
- B. 2002::5
- C. FC00::/7

D. FF02::1

E. FF02::2

▼ Answer

A. 2000::/3

B. 2002::5

C. FC00::/7

D. FF02::1

E. FF02::2



More details Steps:

When configuring IPv6 on an interface, the interface automatically joins two IPv6 multicast groups:

1. The all-nodes multicast group (FF02::1), which includes all IPv6-enabled devices on the same link.
2. The solicited-node multicast group (FF02::2:DDC2:1), which is used in neighbor discovery to locate a specific device on the network.

Option A (2000::/3) is the global unicast address range, and is not a valid IPv6 multicast group address.

Option B (2002::5) is not a valid IPv6 multicast group address.

Option C (FC00::/7) is the unique local address (ULA) range, and is not a valid IPv6 multicast group address.

Q12: Refer to the exhibit. drag and drop the networking parameters from the left onto the correct values on the right.

```
[root#HostTime =]# ip route
default via 192.168.1.193 dev eth1 proto static
192.168.1.0/26 dev s1t1 proto kernel scope link src 192.168.1.200 metric 1

[root#HostTime =]# ip addr show eth1
eth1:mtu 1500 qdisc pfifo_fast qlen 1000
link/ether 00:0c:22:83:79:a3 brd ff:ff:ff:ff:ff:ff
inet 192.168.1.200/26 brd 192.168.1.255 scope global eth1
    inet6 fe80::20c:29ff:fe89:79b3/64 scope link
        valid_lft forever preferred_lft forever
```

Left	Right
Default gateway	00:0C:22:83:79:A3
Host IP address	00:0C:22
NIC MAC address	192.168.1.193
NIC vendor OUI	192.168.1.200
Subnet mask	255.255.255.192

▼ Answer

Left	Right
Default gateway	192.168.1.193
Host IP address	192.168.1.200
NIC MAC address	00:0C:22:83:79:A3
NIC vendor OUI	00:0C:22
Subnet mask	255.255.255.192



More details Steps:

NIC vendor OUI: This is the first three bytes (24 bits) of the NIC MAC address, which identifies the vendor of the NIC.

```
[root#HostTime -]# ip route
default via 192.168.1.193 dev eth1 proto static
192.168.1.0/26 dev sth1 proto kernel scope link src 192.168.1.200 metric 1
                                         default gateway
                                         subnet mask
[host#HostTime -]# ip addr show eth1
eth1:mtu 1500 qdisc pfifo_fast qlan 1000
host ip address link/ether 00:0C:22:83:79:A3 brd ff:ff:ff:ff:ff:ff
inet 192.168.1.200/26 brd 192.168.1.255 scope global eth1
inet6 fe80::20c:22ff:fe83:79a3/64 scope link
      valid_lft forever preferred_lft forever
                                         Mac Address
```

Q13: What is the default behavior of a Layer 2 switch when a frame with an unknown destination MAC address is received?

- A. The Layer 2 switch forwards the packet and adds the destination MAC address to its MAC address table.
- B. The Layer 2 switch sends a copy of a packet to CPU for destination MAC address learning.
- C. The Layer 2 switch floods packets to all ports except the receiving port in the given VLAN.
- D. The Layer 2 switch drops the received frame.

▼ Answer

- A. The Layer 2 switch forwards the packet and adds the destination MAC address to its MAC address table.
- B. The Layer 2 switch sends a copy of a packet to CPU for destination MAC address learning.
- C. The Layer 2 switch floods packets to all ports except the receiving port in the given VLAN.**
- D. The Layer 2 switch drops the received frame.



More details Steps:

The reason for this behavior is that the switch does not have a record of the destination MAC address in its MAC address table, and therefore does not know which port to forward the frame to. By flooding the frame to all ports in the same VLAN, the switch ensures that the frame reaches its intended destination, even if it is on a different switch or a device that has not yet sent any traffic.

Option A ("The Layer 2 switch forwards the packet and adds the destination MAC address to its MAC address table") is incorrect because the switch does not know the destination MAC address, and therefore cannot add it to its MAC address table.

Option B ("The Layer 2 switch sends a copy of a packet to CPU for destination MAC address learning") is incorrect because the switch does not need to send a copy of the frame to the CPU for destination MAC address learning. Instead, it floods the frame to all ports in the same VLAN, except for the port on which the frame was received.

Option D ("The Layer 2 switch drops the received frame") is incorrect because dropping the frame would prevent it from reaching its intended destination.

Q14: An engineer must configure a /30 subnet between two routes. Which usable IP address and subnet mask combination meets this criteria?

A.

```
interface e0/0
description to HQ-A370:98968
ip address 10.2.1.3 255.255.255.252
```

B.

```
interface e0/0
description to HQ-A370:98968
ip address 192.168.1.1 255.255.255.248
```

C.

```
interface e0/0
description to HQ-A370:98968
ip address 172.16.1.4 255.255.255.248
```

D.

```
interface e0/0
description to HQ-A370:98968
ip address 209.165.201.2 255.255.255.252
```

▼ Answer

A.

```
interface e0/0
description to HQ-A370:98968
ip address 10.2.1.3 255.255.255.252
```

B.

```
interface e0/0
description to HQ-A370:98968
ip address 192.168.1.1 255.255.255.248
```

C.

```
interface e0/0
description to HQ-A370:98968
ip address 172.16.1.4 255.255.255.248
```

D.

```
interface e0/0
description to HQ-A370:98968
ip address 209.165.201.2 255.255.255.252
```



More details Steps:

To configure a /30 subnet between two routers, a subnet mask of 255.255.255.252 is required. This subnet mask allows for only two usable IP addresses, one for each end of the link, with the first and last addresses reserved for the network address and broadcast address, respectively.

Option A (interface e0/0 description to HQ-A370:98968 ip address 10.2.1.3 255.255.255.252) uses a private IP address range, which is a /30 subnet. is not a valid answer because it is a broadcast address

Option B (interface e0/0 description to HQ-A370:98968 ip address 192.168.1.1 255.255.255.248) uses a subnet mask of 255.255.255.248, which is not a /30 subnet. This subnet mask allows for 6 usable IP addresses.

Option C (interface e0/0 description to HQ-A370:98968 ip address 172.16.1.4 255.255.255.248) uses a subnet mask of 255.255.255.248, which is not a /30 subnet.

Option D (interface e0/0 description to HQ-A370:98968 ip address 209.165.201.2 255.255.255.252) uses a subnet mask of 255.255.255.252, which is a /30 subnet. This option also uses a public IP address range.

Q15: Which network allows devices to communicate without the need to access the Internet?

- A. 172.9.0.0/16
- B. 172.28.0.0/16
- c. 192.0.0.0/8
- D. 209.165.201.0/24

▼ Answer

- A. 172.9.0.0/16
- B. 172.28.0.0/16**
- c. 192.0.0.0/8
- D. 209.165.201.0/24



More details Steps:

Option A (172.9.0.0/16) is not a private IP address range, as it falls outside of the private IP address ranges reserved by the Internet Assigned Numbers Authority (IANA) for private use. (172.16.0.0/12 (172.16.0.0 - 172.31.255.255))

Option B (172.28.0.0/16) is a valid private IPv4 address range that can be used for local area networks (LANs) and allows devices to communicate without the need to access the Internet.

Option C (192.0.0.0/8) is not a private IP address range, but it includes several private IP address ranges, such as 192.168.0.0/16, which can be used for LANs and are not routable on the Internet. (192.168.0.0/16 (192.168.0.0 - 192.168.255.255))

Option D (209.165.201.0/24) is a public IPv4 address range, which means that it is routable on the Internet. However, devices on this network can still communicate with each other without the need to access the Internet, as long as they use private IP addresses within the network.

Q16: Refer to the exhibit. Which statement explains the configuration error message that is received?

```
Router(config)#interface GigabitEthernet 1/0/1
Router(config-if)#ip address 192.168.16.143 255.255.255.240
Bad mask /28 for address 192.168.16.143
```

- A. It belongs to a private IP address range.
- B. The router does not support /28 mask.
- C. It is a network IP address.
- D. It is a broadcast IP address.

▼ Answer

- A. It belongs to a private IP address range.
- B. The router does not support /28 mask.
- C. It is a network IP address.
- D. It is a broadcast IP address.**



More details Steps:

```
Router(config)#interface GigabitEthernet 1/0/1
Router(config-if)#ip address 192.168.16.143 255.255.255.240
Bad mask /28 for address 192.168.16.143
```

Since 240 then its /28 192.168.16.0
so each subnetwork 192.168.16.16
increment by 16 192.168.16.32
 192.168.16.48
 192.168.16.64
 192.168.16.80
 192.168.16.96
so the 192.168.16.143 192.168.16.112
broadcast address and 192.168.16.128
192.168.16.144 is new 192.168.16.144
subnetwork

Q17: Which IPv6 address type communication between subnets and cannot route on the Internet?

- A. link-local
- B. unique local
- C. multicast
- D. global unicast

▼ Answer

- A. link-local
- B. unique local**
- C. multicast
- D. global unicast



More details Steps:

Unique Local Addresses (ULAs), also known as Local IPv6 or IPv6 Site-Local addresses in earlier versions of the IPv6 protocol, are IPv6 addresses that are used for communication between subnets within a private network or an organization. They are not globally routable on the Internet and are intended to be used only within a specific enterprise or organization.

ULAs are similar to private IPv4 addresses in that they are not globally unique and are meant to be used only within a private network. They are defined in RFC 4193 and are allocated from the fd00::/8 address block.

Link-local addresses (A) are used for communications within a single subnet and are not routable beyond the local network segment. They are automatically assigned to every interface in an IPv6 network and are used for neighbor discovery and other network-related functions.

Multicast addresses (C) are used to communicate with a group of devices on the same network segment, and they can be used for both intra-subnet and inter-subnet communication. Multicast addresses can be routable on the Internet, depending on the scope of the address.

Global unicast addresses (D) are IPv6 addresses that are globally unique and can be used for communication between devices on different networks. They are intended to be routable on the Internet and are assigned by Internet Assigned Numbers Authority (IANA) to Internet Service Providers (ISPs) and other organizations.

Q18: Which IPv6 address block sends packets to a group address rather than a single address?

- A. 2000::/3
- B. FC00::/7
- C. FE80::/10
- D. FFCC::/8

▼ Answer

- A. 2000::/3
- B. FC00::/7
- C. FE80::/10
- D. FFCC::/8**



More details Steps:

IPv6 multicast addresses are used to send a single packet to multiple devices on the same network segment. Multicast addresses are identified by a prefix that starts with FF, followed by a flag field and a group ID field. The FFCC::/8 address block is reserved for multicast addresses and is divided into several sub-ranges for different types of multicast addresses.

Therefore, the IPv6 address block that sends packets to a group address rather than a single address is the FFCC::/8 address block, which is used for multicast addresses.

Option A (2000::/3) is the global unicast address range, which is used for communication between devices on different networks.

Option B (FC00::/7) is the unique local address (ULA) range, which is used for communication within a private network and is not globally routable on the Internet.

Option C (FE80::/10) is the link-local address range, which is used for communication within a single network segment and is not routable beyond the local network segment.

Q19: What are two reasons that cause late collisions to increment on an Ethernet interface? (Choose two.)

- A. when Carrier Sense Multiple Access/Collision Detection is used
- B. when one side of the connection is configured for half-duplex
- C. when the sending device waits 15 seconds before sending the frame again
- D. when a collision occurs after the 32nd byte of a frame has been transmitted
- E. when the cable length limits are exceeded

▼ Answer

A. when Carrier Sense Multiple Access/Collision Detection is used

- B. when one side of the connection is configured for half-duplex
 - C. when the sending device waits 15 seconds before sending the frame again
 - D. when a collision occurs after the 32nd byte of a frame has been transmitted
- E. when the cable length limits are exceeded**



More details Steps:

A. When Carrier Sense Multiple Access/Collision Detection (CSMA/CD) is used: Late collisions can occur when a transmitting device detects that a collision has occurred after it has transmitted more than 512 bits of the frame. This type of collision is called a late collision and can occur when the device on the other end of the link is not following the CSMA/CD protocol properly or if there is a duplex mismatch between the two devices.

E. When the cable length limits are exceeded: Late collisions can also occur when the cable length limits are exceeded, which can cause signal degradation and other types of errors that can lead to late collisions.

Option B (when one side of the connection is configured for half-duplex), Option C (when the sending device waits 15 seconds before sending the frame again), and Option D (when a collision occurs after the 32nd byte of a frame has been transmitted) are incorrect and do not cause late collisions.

Q20: What is a benefit of using a Cisco Wireless LAN Controller?

- A. It eliminates the need to configure each access point individually.
- B. Central IP management requires more complex configurations.
- C. Unique SSIDs cannot use the same authentication method.
- D. It supports autonomous and lightweight APs

▼ Answer

A. It eliminates the need to configure each access point individually.

- B. Central IP management requires more complex configurations.
- C. Unique SSIDs cannot use the same authentication method.
- D. It supports autonomous and lightweight APs



More details Steps:

A Cisco Wireless LAN Controller (WLC) is a network component that is used to manage and control multiple wireless access points (APs) in a centralized manner. By using a WLC, network administrators can configure and manage multiple APs from a single location, rather than having to configure each AP individually. This not only saves time and effort but also ensures consistency in the configuration of all the APs in the network.

Option B (Central IP management requires more complex configurations) is incorrect. Central IP management is a feature of Cisco WLCs that simplifies the management of IP addresses for wireless clients by assigning IP addresses centrally from the WLC. This can actually reduce complexity in the network by eliminating the need to manage IP addresses for each individual AP.

Option C (Unique SSIDs cannot use the same authentication method) is also incorrect. The authentication methods used for wireless clients are configured on the WLC and can be applied to multiple SSIDs. Different SSIDs can use the same authentication method if desired.

Option D (It supports autonomous and lightweight APs) is partially correct. Cisco WLCs support lightweight APs, but not autonomous

Q21: Which action is taken by switch port enabled for POE power classification override?

- A. If a monitored port exceeds the maximum administrative value for power, the port is shutdown and err- disabled.
- B. When a powered device begins drawing power from a POE switch port, a syslog message is generated.
- C. As power usage on a POE switch port is checked, data flow to the connected device is temporarily paused.
- D. If a switch determines that a device is using less than the minimum configured power, it assumes the device has failed and disconnects it.

▼ Answer

A. If a monitored port exceeds the maximum administrative value for power, the port is shutdown and err-disabled.

- B. When a powered device begins drawing power from a POE switch port, a syslog message is generated.
- C. As power usage on a POE switch port is checked, data flow to the connected device is temporarily paused.
- D. If a switch determines that a device is using less than the minimum configured power, it assumes the device has failed and disconnects it.



More details Steps:

if the powered device exceeds the maximum power limit for the port, the switch will shut down the port and disable it to prevent damage to the switch or overloading of the power supply. This is the behavior of the switch when a monitored port exceeds the maximum administrative value for power, not when PoE power classification override is enabled.

Option B (When a powered device begins drawing power from a PoE switch port, a syslog message is generated), Option C (As power usage on a PoE switch port is checked, data flow to the connected device is temporarily paused), and Option D (If a switch determines that a device is using less than the minimum configured power, it assumes the device has failed and disconnects it) are incorrect. These options do not describe the behavior of a switch port when it is enabled for PoE power classification override.

Q22: Which statement about Link Aggregation when implementing on a Cisco Wireless LAN Controller is true?

- A. The EtherChannel must be configured in "mode active"
- B. When enabled, the WLC bandwidth drops to 500 Mbps.
- C. To pass client traffic, two or more ports must be configured.
- D. One functional physical port is needed to pass client traffic.

▼ Answer

- A. The EtherChannel must be configured in "mode active"
- B. When enabled, the WLC bandwidth drops to 500 Mbps.
- C. To pass client traffic, two or more ports must be configured.
- D. One functional physical port is needed to pass client traffic.**



More details Steps:

When implementing Link Aggregation on a Cisco Wireless LAN Controller (WLC), the WLC can combine two or more physical ports into a single logical port to provide increased bandwidth and redundancy.

Option A (The EtherChannel must be configured in "mode active") is incorrect since WLC don't support lacp. While the mode active is one of the options for configuring EtherChannels, it is not a requirement for implementing Link Aggregation on a Cisco WLC. Other modes, such as mode on or mode passive, can also be used depending on the specific requirements of the network.

Option B (When enabled, the WLC bandwidth drops to 500 Mbps) is also incorrect. Enabling Link Aggregation on a Cisco WLC does not necessarily result in a drop in bandwidth. In fact, Link Aggregation can provide increased bandwidth by combining multiple physical ports into a single logical port.

Option C (To pass client traffic, two or more ports must be configured) is also incorrect. While Link Aggregation does require the configuration of multiple physical ports, only one functional physical port is needed to pass client traffic. The other ports are used for redundancy and increased bandwidth.

Q23: Which two conditions must be met before SSH can operate normally on a Cisco IOS switch? (Choose two.)

- A. IP routing must be enabled on the switch.
- B. A console password must be configured on the switch.
- C. Telnet must be disabled on the switch.
- D. The switch must be running a k9 (crypto) IOS image.
- E. The "ip domain-name" command must be configured on the switch.

▼ Answer

- A. IP routing must be enabled on the switch.
- B. A console password must be configured on the switch.
- C. Telnet must be disabled on the switch.
- D. The switch must be running a k9 (crypto) IOS image.**
- E. The "ip domain-name" command must be configured on the switch.**



More details Steps:

When configuring SSH on a Cisco IOS switch, the following two conditions must be met:

- D. The switch must be running a k9 (crypto) IOS image: SSH requires encryption to provide secure communication between the client and the switch. The k9 (crypto) IOS image includes the necessary cryptographic features to support SSH.
 - E. The "ip domain-name" command must be configured on the switch: This command is used to specify the domain name for the switch. This information is used to generate the RSA key pair that is required for SSH. Without the RSA key pair, SSH cannot operate normally on the switch.
- Option A (IP routing must be enabled on the switch) is incorrect. IP routing is not a requirement for SSH to operate normally on a Cisco IOS switch.
- Option B (A console password must be configured on the switch) is also incorrect. While it is generally recommended to configure a console password for security purposes, it is not a requirement for SSH to operate normally on a Cisco IOS switch.
- Option C (Telnet must be disabled on the switch) is also incorrect. While it is generally recommended to disable Telnet in favor of SSH for security purposes, it is not a requirement for SSH to operate normally on a Cisco IOS switch.

024: Refer to the exhibit. Which password must an engineer use to enter the enable mode?

```

Atlanta#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Atlanta(config)#aaa new-node1
Atlanta(config)#aaa authentication login default local
Atlanta(config)#line vty 0 4
Atlanta(config-line)#login authentication default
Atlanta(config-line)#exit
Atlanta(config)#username ciscoadmin password adminadmin123
Atlanta(config)#username ciscoadmin privilege 15
Atlanta(config)#enable password cisco123
Atlanta(config)#enable secret testing1234
Atlanta(config)#end

```

- A. adminadmin123
- B. cisc0123
- C. default
- D. testing1234

▼ Answer

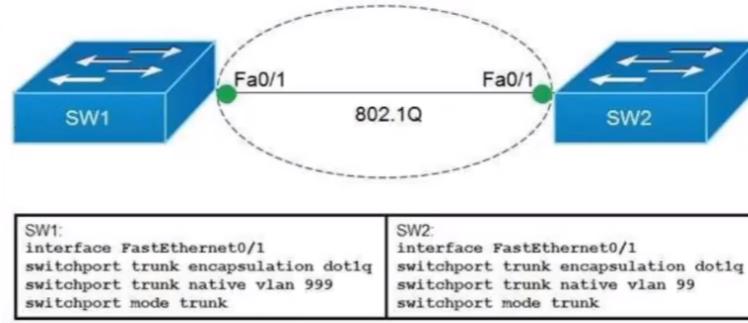
- A. adminadmin123
- B. cisc0123
- C. default
- D. testing1234**



More details Steps:

If both the "enable password" and "enable secret" commands are configured on a Cisco device, the "enable secret" always takes precedence and is used as the enable password. This is because the "enable secret" is a more secure method of protecting privileged EXEC mode access on the device, as it uses a stronger encryption algorithm and is more difficult to crack than the "enable password".

Q25: Refer to the exhibit. Which action do the switches take on the trunk link?



- A. The trunk does not form, and the ports go into an err-disabled status.
- B. The trunk forms, but the mismatched native VLANs are merged into a single broadcast domain.
- C. The trunk forms, but VLAN 99 and VLAN 999 are in a shutdown state.
- D. The trunk does not form, but VLAN 99 and VLAN 999 are allowed to traverse the link.

▼ Answer

- A. The trunk does not form, and the ports go into an err-disabled status.
- B. The trunk forms, but the mismatched native VLANs are merged into a single broadcast domain.**
- C. The trunk forms, but VLAN 99 and VLAN 999 are in a shutdown state.
- D. The trunk does not form, but VLAN 99 and VLAN 999 are allowed to traverse the link.



More details Steps:

When a trunk link is established between two switches with different native VLANs, the switches will merge the mismatched native VLANs into a single broadcast domain. In this case, VLAN 99 and VLAN 999 will be merged into a single broadcast domain, which means that any traffic on these VLANs will be forwarded across the trunk link.

Option A (The trunk does not form, and the ports go into an err-disabled status) is incorrect because the switch ports will not go into an err-disabled status due to the mismatched native VLANs.

Option C (The trunk forms, but VLAN 99 and VLAN 999 are in a shutdown state) is also incorrect because the mismatched native VLANs do not cause any VLANs to be in a shutdown state.

Option D (The trunk does not form, but VLAN 99 and VLAN 999 are allowed to traverse the link) is also incorrect because the mismatched native VLANs do not prevent the trunk link from forming. Instead, the VLANs are merged into a single broadcast domain.

Q26: What is the primary effect of the spanning-tree portfast command?

- A. It immediately enables the port in the listening state.
- B. It immediately puts the port into the forwarding state when the switch is reloaded.
- C. It enabled BPDIJ messages.
- D. It minimizes spanning-tree convergence time.

▼ Answer

- A. It immediately enables the port in the listening state.
- B. It immediately puts the port into the forwarding state when the switch is reloaded.**
- C. It enabled BPDIJ messages.
- D. It minimizes spanning-tree convergence time.



More details Steps:

The primary effect of the spanning-tree portfast command is to immediately put the port into the forwarding state without going through the listening and learning states. This is useful for switch ports that are connected to end devices, such as workstations or servers, that do not participate in the Spanning Tree Protocol. By using the spanning-tree portfast command, the port can be immediately enabled and ready to forward traffic, which can minimize the time it takes for the end device to establish connectivity to the network.

Option A (It immediately enables the port in the listening state) is incorrect because the spanning-tree portfast command skips the listening and learning states and immediately enables the port in the forwarding state.

Option B (It immediately puts the port into the forwarding state when the switch is reloaded) is the correct answer because the spanning-tree portfast command immediately puts the port into the forwarding state without going through the listening and learning states. This is useful when the switch is reloaded, and the port is brought back up quickly without the delay caused by the normal Spanning Tree Protocol convergence process.

Option C (It enabled BPDU messages) is incorrect because the spanning-tree portfast command does not enable BPDU messages. In fact, it disables the sending and receiving of BPDU messages on the port to prevent loops in the network.

Q27: Which result occurs when Portfast is enabled on an interface that is connected to another switch?

- A. Root port choice and spanning tree recalculation are accelerated when a switch link goes down.
- B. After spanning tree converges, PortFast shuts down any port that receives BPDUs.
- C. VTP is allowed to propagate VLAN configuration information from switch to switch automatically.
- D. Spanning tree may fail to detect a switching loop in the network that causes broadcast storms.

▼ Answer

- A. Root port choice and spanning tree recalculation are accelerated when a switch link goes down.
- B. After spanning tree converges, PortFast shuts down any port that receives BPDUs.
- C. VTP is allowed to propagate VLAN configuration information from switch to switch automatically.
- D. Spanning tree may fail to detect a switching loop in the network that causes broadcast storms.**



More details Steps:

Enabling Portfast on an interface that is connected to another switch can cause spanning-tree loops and broadcast storms, and may lead to network disruptions. Therefore, it is not recommended to enable Portfast on switch-to-switch links.

Option A (Root port choice and spanning tree recalculation are accelerated when a switch link goes down) is incorrect because Portfast does not affect the root port selection process or the spanning-tree recalculation when a switch link goes down.

Option B (After spanning tree converges, PortFast shuts down any port that receives BPDUs) is also incorrect because Portfast does not shut down any port that receives BPDUs. Instead, Portfast disables the spanning-tree listening and learning states and immediately transitions the port to the forwarding state, which can cause issues if the port is connected to another switch.

Option C (VTP is allowed to propagate VLAN configuration information from switch to switch automatically) is also incorrect because Portfast does not affect VTP operation or the propagation of VLAN configuration information.

Option D (Spanning tree may fail to detect a switching loop in the network that causes broadcast storms) is the most correct answer because enabling Portfast on a switch-to-switch link can cause a switching loop in the network that may not be detected by the spanning-tree protocol. This can lead to broadcast storms and network disruptions. Therefore, it is recommended to disable Portfast on switch-to-switch links to prevent such issues.

Q28: Which QOS Profile is selected in the GUI when configuring a voice over WLAN deployment?

- A. Platinum
- B. Bronze
- C. Gold
- D. Silver

▼ Answer

A. Platinum

- B. Bronze
- C. Gold
- D. Silver



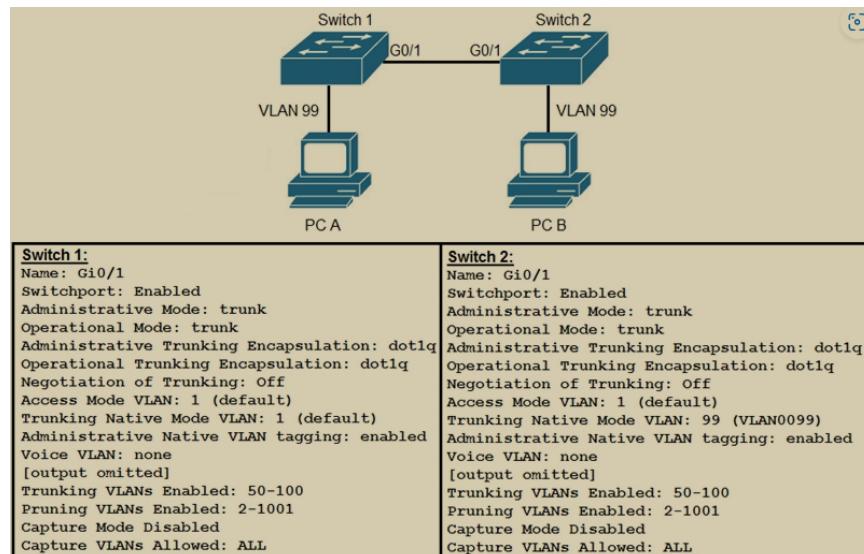
More details Steps:

When configuring a voice over WLAN deployment, the QoS (Quality of Service) profile selected in the GUI is usually the Platinum profile. The Platinum QoS profile provides the highest level of QoS, ensuring that voice traffic is given the highest priority and receives the necessary bandwidth and low latency to ensure high-quality voice calls.

QoS is an important consideration for wireless networks that support voice traffic, as it ensures that voice traffic is given priority over other types of traffic, such as data traffic. Without proper QoS configuration, voice calls may experience issues such as poor call quality, dropped calls, and delays.

The other options, B (Bronze), C (Gold), and D (Silver), are also QoS profiles that can be used in a network, but they are generally not used for voice traffic. These profiles are more commonly used for data traffic, and provide varying levels of QoS based on the specific needs of the network and the applications being used.

Q29: Refer to the exhibit. After the switch configuration, the ping test fails between PC A and PC B. Based on the output for switch 1, which error must be corrected?



- A. The PCs are in the incorrect VLAN.
- B. All VLANs are not enabled on the trunk.
- C. Access mode is configured on the switch ports.
- D. There is a native VLAN mismatch.

▼ Answer

- A. The PCs are in the incorrect VLAN.
- B. All VLANs are not enabled on the trunk.
- C. Access mode is configured on the switch ports.
- D. There is a native VLAN mismatch.**



More details Steps:

The configuration for Switch 1 shows that the Access Mode VLAN is 1, and the Trunking Native Mode VLAN is also 1. However, the configuration for Switch 2 shows that the Access Mode VLAN is 1, and the Trunking Native Mode VLAN is 99. This configuration mismatch causes a native VLAN mismatch between the switches, which can lead to communication issues between devices in different VLANs.

To correct this error, the Trunking Native Mode VLAN on one of the switches (either Switch 1 or Switch 2) should be changed to match the native VLAN on the other switch. In this case, the Trunking Native Mode VLAN on Switch 2 should be changed to 1 to match the Access Mode VLAN and Trunking Native Mode VLAN on Switch 1.

Option A (The PCs are in the incorrect VLAN) is incorrect because there is no information in the provided output to suggest that the PCs are in the incorrect VLAN.

Option B (All VLANs are not enabled on the trunk) is incorrect because the output for both switches shows that Trunking VLANs are enabled, specifically VLANs 50-100.

Option C (Access mode is configured on the switch ports) is also incorrect because the provided output shows that both switches are configured as trunks, not access ports.

Q30: Drag and Drop the WLAN components from the left onto the correct description on the right.

LEFT	Right
Access point	Device that provides Wi-Fi devices with a connection to a wired network
Virtual interface	Applied to WLAN for wireless client communication
Dynamic interface	Used to support mobility management of the WLC
Service port	Device that manages access points
Wireless LAN Controller	Used for out-of-band management of a WLC

▼ Answer

Component	Description
Access point	Device that provides Wi-Fi devices with a connection to a wired network
Virtual interface	Used to support mobility management of the WLC
Dynamic interface	Applied to WLAN for wireless client communication
Service port	Used for out-of-band management of a WLC
Wireless LAN Controller	Device that manages access points

Q31: Which unified access point mode continues to serve wireless clients after losing connectivity to the Cisco Wireless LAN Controller?

- A. local
- B. mesh
- C. flexconnect
- D. sniffer

▼ Answer

- A. local
- B. mesh
- C. flexconnect**
- D. sniffer



More details Steps:

In FlexConnect mode, the access point (AP) can operate in either central switching or local switching mode. When the AP loses connectivity to the Wireless LAN Controller (WLC), it can switch to local switching mode, allowing it to continue to serve wireless clients. In local switching mode, the AP can provide all the necessary wireless services such as authentication, encryption, and data forwarding without relying on the WLC. The AP can also continue to support additional features such as Quality of Service (QoS) and VLANs.

On the other hand, in local mode, the AP can operate autonomously and continue to serve the wireless clients even when it loses connectivity to the WLC, but it may not support all the features of the FlexConnect mode.

In mesh mode, the APs form a wireless mesh network to provide wireless coverage to areas where it is difficult to deploy wired infrastructure. Mesh APs rely on their neighboring APs to relay traffic to the WLC, and if they lose connectivity to the WLC, they cannot operate autonomously.

Sniffer mode is a troubleshooting mode that the AP can operate in to capture wireless traffic for analysis.

Q32: Refer to the exhibit. Which command provides this output?

Router#					
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone, D - Remote, C - CVTA, M - Two-port Mac Relay					
Device ID	Local Interface	Holdtime	Capability	Platform	Port ID
10.1.1.2	Gig 37/3	176	R I	CPT 600	Gig 36/41
10.1.1.2	Gig 37/1	174	R I	CPT 600	Gig 36/43
10.1.1.2	Gig 36/41	134	R I	CPT 600	Gig 37/3
10.1.1.2	Gig 36/43	134	R I	CPT 600	Gig 37/1
10.1.1.2	Ten 3/2	132	R I	CPT 600	Ten 4/2
10.1.1.2	Ten 4/2	174	R I	CPT 600	Ten 3/2

- A. show ip route
- B. show cdp neighbor
- C. show ip interface
- D. show interface

▼ Answer

- A. show ip route
- B. show cdp neighbor**
- C. show ip interface
- D. show interface

Q33: Which mode must be used to configure EtherChannel between two switches without using a negotiation protocol?

- A. active
- B. on
- C. auto
- D. desirable

▼ Answer

- A. active
- B. on**
- C. auto
- D. desirable



More details Steps:

When configuring EtherChannel between two switches without using a negotiation protocol, the "on" mode must be used. In this mode, the EtherChannel is manually configured on both switches, and neither switch sends negotiation packets. This mode is useful when one switch does not support negotiation protocols such as Link Aggregation Control Protocol (LACP) or Port Aggregation Protocol (PAgP), or when the administrator wants to manually configure the EtherChannel.

In the "active" mode, the switch actively tries to negotiate with the other switch using LACP or PAgP protocols. If the other switch is also in active mode or desirable mode, the EtherChannel will be formed. If the other switch is in auto or on mode, the EtherChannel will not be formed.

In the "auto" mode, the switch waits for the other switch to initiate the negotiation using LACP or PAgP protocols. If the other switch is in active or desirable mode, the EtherChannel will be formed. If the other switch is in auto or on mode, the EtherChannel will not be formed.

In the "desirable" mode, the switch actively tries to negotiate with the other switch using PAgP protocol. If the other switch is also in desirable or auto mode, the EtherChannel will be formed. If the other switch is in on or active mode, the EtherChannel will not be formed.

Q34: Which mode allows access points to be managed by Cisco Wireless LAN Controllers?

- A. bridge
- B. lightweight
- C. mobility express
- D. autonomous

▼ Answer

- A. bridge
- B. lightweight**
- C. mobility express
- D. autonomous



More details Steps:

In lightweight mode, the access points (APs) are managed by Cisco Wireless LAN Controllers (WLCs). The APs act as thin clients that offload most of the wireless processing and management functions to the WLCs. The WLCs provide centralized management and control of the APs, allowing administrators to configure, monitor, and troubleshoot the wireless network from a single location.

In bridge mode, the APs act as stand-alone devices that provide wireless connectivity without the need for a WLC. In this mode, the APs do not participate in any centralized management or control, and the configuration must be done individually on each AP.

In mobility express mode, the APs can act as a small-scale WLC capable of managing up to 100 APs. This mode is designed for small to medium-sized networks that do not require a dedicated WLC.

In autonomous mode, the APs operate independently and provide all the necessary wireless services such as authentication, encryption, and data forwarding without relying on a WLC. In this mode, the APs must be configured individually, and there is no centralized management or control.

Q35: Which two values or settings must be entered when configuring a new WLAN, In the Cisco Wireless LAN Controller GUI? (Choose two.)

- A. QOS settings
- B. IP address of one or more access points
- C. SSID
- D. profile name
- E. management interface settings

▼ Answer

- A. QOS settings
- B. IP address of one or more access points
- C. SSID**

D. profile name

E. management interface settings



More details Steps:

SSID (Service Set Identifier) is the name of the wireless network that clients will see when they search for available networks. It is a unique identifier that distinguishes one wireless network from another. The SSID must be configured when creating a new WLAN on the Cisco Wireless LAN Controller.

Profile name is the name of the WLAN profile that contains the configuration settings for the WLAN. The profile includes settings such as security, QoS, VLAN, and more. The profile name must also be configured when creating a new WLAN on the Cisco Wireless LAN Controller.

QoS settings may be configured in the WLAN profile, but they are not required when creating a new WLAN.

IP address of one or more access points may be configured in the WLAN settings, but it is not required when creating a new WLAN.

Management interface settings may also be configured in the WLAN settings, but they are not required when creating a new WLAN.

Q36: Which command is used to specify the delay time in seconds for LLDP to initialize on any interface?

- A. lldp timer
- B. lldp tlv-select
- C. lldp reinit
- D. lldp holdtime

▼ Answer

- A. lldp timer
- B. lldp tlv-select
- C. lldp reinit**
- D. lldp holdtime

Q37: Refer to the exhibit. How does SW2 interact with other switches in this VTP domain?

```
SW2
vtp domain cisco
vtp mode transparent
vtp password ciscotest
interface fastethernet0/1
  description connection to sw1
  switchport mode trunk
  switchport trunk encapsulation dot1q
```

- A. It transmits and processes VTP updates from any VTP clients on the network on its trunk ports.
- B. It processes VTP updates from any VTP clients on the network on its access ports.
- C. It receives updates from all VTP servers and forwards all locally configured VLANs out all trunk ports.
- D. It forwards only the VTP advertisements that it receives on its trunk ports.

▼ Answer

- A. It transmits and processes VTP updates from any VTP clients on the network on its trunk ports.
- B. It processes VTP updates from any VTP clients on the network on its access ports.
- C. It receives updates from all VTP servers and forwards all locally configured VLANs out all trunk ports.
- D. It forwards only the VTP advertisements that it receives on its trunk ports.**



More details Steps:

SW2 is configured with VTP mode transparent, which means that it does not participate in VTP updates. It does not send or receive VTP updates on its trunk or access ports. However, it will forward any VTP advertisements that it receives on its trunk ports to other switches in the VTP domain.

Q38: Refer to the exhibit. Based on the LACP neighbor status, in which mode is the SW1 port channel configured?

```

SW1#sh lacp neighbor
Flags: S - Device is requesting Slow LACPDU
      F - Device is requesting Fast LACPDU
      A - Device is in Active mode      P - Device is in Passive mode

Channel group 35 neighbors

Partner's information:

      LACP port
      Admin Oper Port Port
Port  Flags Priority Dev ID   Age key Key Number State
Et1/0 SP    32768   aabb.cc80.7000 8s 0x0 0x23 0x101 0x3C
Et1/1 SP    32768   aabb.cc80.7000 8s 0x0 0x23 0x102 0x3C

```

- A. mode on
- B. active
- C. passive
- D. auto

▼ Answer

- A. mode on
- B. active**
- C. passive
- D. auto



More details Steps:

```

SW1#sh lacp neighbor
Flags: S - Device is requesting Slow LACPDU
      F - Device is requesting Fast LACPDU
      A - Device is in Active mode      P - Device is in Passive mode

Channel group 35 neighbors

Partner's information:

      LACP port
      Admin Oper Port Port
Port  Flags Priority Dev ID   Age key Key Number State
Et1/0 SP    32768   aabb.cc80.7000 8s 0x0 0x23 0x101 0x3C
Et1/1 SP    32768   aabb.cc80.7000 8s 0x0 0x23 0x102 0x3C

```

Since the command for neighbor
then this port not for switch 1 so
and its passive so the switch 1 is
active

Q39: Two switches are connected and using Cisco Dynamic Trunking Protocol. SW1 is set to Dynamic Auto and SW2 is set to Dynamic Desirable. What is the result of this configuration?

- A. The link becomes an access port.
- B. The link is in an error disabled state.
- C. The link is in a down state.
- D. The link becomes a trunk port.

▼ Answer

- A. The link becomes an access port.
- B. The link is in an error disabled state.
- C. The link is in a down state.
- D. The link becomes a trunk port.**



More details Steps:

When two switches are connected and using Dynamic Trunking Protocol (DTP), the negotiation process determines whether the link between them will become a trunk port or an access port. In this scenario, SW1 is set to Dynamic Auto, which means that it will not initiate the negotiation but will respond to the trunking negotiation request from the other switch. SW2 is set to Dynamic Desirable, which means that it will initiate the negotiation and actively try to convert the link into a trunk port.

Since SW2 is set to Dynamic Desirable, it will send a DTP negotiation request to SW1, which will respond with a DTP negotiation response. SW2 will then send a DTP negotiation confirmation, and the link between the switches will become a trunk port.
either (auto - Desirable || Desirable - Desirable)

Q40: Cisco IP phone receives untagged data traffic from an attached PC. Which action is taken by the phone?

- A. It drops the traffic.
- B. It allows the traffic to pass through unchanged.
- C. It tags the traffic with the native VLAN.
- D. It tags the traffic with the default VLAN.

▼ Answer

- A. It drops the traffic.
- B. It allows the traffic to pass through unchanged.**
- C. It tags the traffic with the native VLAN.
- D. It tags the traffic with the default VLAN.



More details Steps:

When a Cisco IP phone receives untagged data traffic from an attached PC, it will simply pass the traffic through unchanged. The phone will not tag the traffic with any VLAN ID, including the native VLAN.

In this scenario, the traffic from the attached PC is treated as untagged data traffic and is forwarded by the phone to the switch. The switch will then handle the traffic based on the port configuration. If the switch port is configured as an access port in a specific VLAN, the untagged traffic will be assigned to that VLAN. If the switch port is configured as a trunk port, the untagged traffic will be assigned to the native VLAN configured on the switch port.

Q41: Which design element is a best practice when deploying an 802.11b wireless infrastructure?

- A. allocation nonoverlapping channels to access points that are in close physical proximity to one another
- B. disabling TCP so that access points can negotiate signal levels with their attached wireless devices
- C. configuring access points to provide clients with a maximum of 5 Mbps
- D. setting the maximum data rate to 54 Mbps on the Cisco Wireless LAN Controller

▼ Answer

- A. allocation nonoverlapping channels to access points that are in close physical proximity to one another**
- B. disabling TCP so that access points can negotiate signal levels with their attached wireless devices
- C. configuring access points to provide clients with a maximum of 5 Mbps
- D. setting the maximum data rate to 54 Mbps on the Cisco Wireless LAN Controller



More details Steps:

802.11b is a wireless networking standard that operates in the 2.4 GHz frequency band and provides a maximum data rate of 11 Mbps. In this frequency band, there are only three nonoverlapping channels: channels 1, 6, and 11. When deploying multiple access points in close physical proximity to one another, it is important to allocate nonoverlapping channels to minimize interference between the access points.

For example, if two access points are installed in adjacent rooms, they should be configured to use channels 1 and 6, or channels 6 and 11, to avoid interference. If channels that overlap are used, such as channels 1 and 2, or channels 6 and 7, there will be interference and degraded performance.

Q42: Refer to the exhibit. What does router R1 use as its OSPF Router-ID?

```
R1#show ip interface brief
Interface          IP-Address      OK? Method    Status           Protocol
FastEthernet0/0    unassigned      YES NVRAM   administratively down
GigabitEthernet1/0 192.168.0.1    YES NVRAM   up
GigabitEthernet2/0 10.10.1.10     YES manual   up
GigabitEthernet3/0 10.10.10.20   YES manual   up
GigabitEthernet4/0 unassigned      YES NVRAM   administratively down
Loopback0          172.16.15.10   YES manual   up
```

- A. 10.10.1.10
- B. 10.10.10.20
- c. 172.16.15.10
- D. 192.168.0.1

▼ Answer

- A. 10.10.1.10
- B. 10.10.10.20
- c. 172.16.15.10**
- D. 192.168.0.1



More details Steps:

The OSPF Router-ID is a unique identifier that is used by OSPF routers to identify themselves and to advertise their routing information. In OSPF, the Router-ID is determined in the following order of preference:

1. If the Router-ID is manually configured using the `router-id` command in OSPF router configuration mode, then the configured IP address is used as the Router-ID.
2. If the Router-ID is not manually configured, then the highest IP address on any loopback interface is used as the Router-ID.
3. If there are no loopback interfaces, then the highest IP address on any active physical interface is used as the Router-ID.

Q43: When OSPF learns multiple paths to a network, how does it select a route?

- A. For each existing interface, it adds the metric from the source router to the destination to calculate the route with the lowest bandwidth.
- B. It counts the number of hops between the source router and the destination to determine the route with the lowest metric.
- C. It divides a reference bandwidth of 100 Mbps by the actual bandwidth of the exiting interface to calculate the route with the lowest cost.
- D. It multiples the active K values by 256 to calculate the route with the lowest metric.

▼ Answer

- A. For each existing interface, it adds the metric from the source router to the destination to calculate the route with the lowest bandwidth.
- B. It counts the number of hops between the source router and the destination to determine the route with the lowest metric.
- C. It divides a reference bandwidth of 100 Mbps by the actual bandwidth of the exiting interface to calculate the route with the lowest cost.**
- D. It multiples the active K values by 256 to calculate the route with the lowest metric.



More details Steps:

When OSPF learns multiple paths to a network, it selects a route based on the lowest metric, or cost, to the destination network.

OSPF calculates the cost of a path based on the bandwidth of the outgoing interface. By default, OSPF uses the formula: $\text{cost} = \text{reference bandwidth} / \text{interface bandwidth}$, where the reference bandwidth is typically set to 100 Mbps. This means that a higher bandwidth interface will have a lower cost than a lower bandwidth interface.

When OSPF learns multiple paths to a network, it will select the path with the lowest metric, or cost, to the destination network. If there are multiple paths with the same metric, OSPF will use other criteria, such as administrative distance and router ID, to determine the best path.

Q44: When a floating static route is configured, which action ensures that the backup route is used when the primary route fails?

- A. The administrative distance must be higher on the primary route so that the backup route becomes secondary.
- B. The `default-information originate` command must be configured for the route to be installed into the routing table.
- C. The floating static route must have a lower administrative distance than the primary route so it is used as a backup.
- D. The floating static route must have a higher administrative distance than the primary route so it is used as a backup

▼ Answer

- A. The administrative distance must be higher on the primary route so that the backup route becomes secondary.
- B. The default-information originate command must be configured for the route to be installed into the routing table.
- C. The floating static route must have a lower administrative distance than the primary route so it is used as a backup.
- D. The floating static route must have a higher administrative distance than the primary route so it is used as a backup**



More details Steps:

When a floating static route is configured, the backup route is ensured to be used when the primary route fails by configuring the floating static route with a higher administrative distance than the primary route.

To configure a floating static route, a static route with a higher administrative distance than the primary route is configured. This route is known as the floating static route. When the primary route fails, the floating static route is used as a backup route.

For example, if the primary route to a destination has an administrative distance of 1, a floating static route with an administrative distance of 2 can be configured as a backup route. When the primary route fails, the floating static route with the higher administrative distance is used as the backup route.

Q45: Refer to the exhibit. The show ip ospf interface command has been executed on RI. How is OSPF configured?

```
Designated Router (ID) 10.11.11.11, Interface address 10.10.10.1
Backup Designated router (ID) 10.3.3.3, Interface address 10.10.10.3
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
oob-resync timeout 40
Hello due in 00:00:08
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 1/1/1, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 6
Last flood scan time is 0 msec, maximum is 1 msec
Neighbor Count is 3, Adjacent neighbor count is 3
Adjacent with neighbor 10.1.1.4
Adjacent with neighbor 10.2.2.2
Adjacent with neighbor 10.3.3.3 (Backup Designated Router)
Suppress hello for 0 neighbor(s)
```

- A. point-to-point network type is configured.
- B. The interface is not participating in OSPF.
- C. The default Hello and Dead timers are in use.
- D. There are six OSPF neighbors on this interface.

▼ Answer

- A. point-to-point network type is configured.
- B. The interface is not participating in OSPF.
- C. The default Hello and Dead timers are in use.**
- D. There are six OSPF neighbors on this interface.



More details Steps:

Option (A) is not correct because the network is configured as a broadcast network since there is a DR and a BDR, so a point-to-point network type is not configured.

Option (B) is not correct since the output shows that the interface is participating in OSPF. The line "Neighbor Count is 3" also confirms that the interface is participating in OSPF.

Option (C) is also not correct because the output shows that there are six OSPF neighbors on this interface, which is confirmed by the "Neighbor Count is 3" and "Adjacent neighbor count is 3" lines.

Q46: A user configured OSPF and advertised the Gigabit Ethernet interface in OSPF. By default, which type of OSPF network does this interface belong to?

- A. point-to-multipoint
- B. point-to-point
- C. broadcast
- D. non-broadcast

▼ Answer

A. point-to-multipoint

B. point-to-point

C. broadcast

D. non-broadcast



More details Steps:

In the point-to-point network type, OSPF hellos are sent directly between two routers without the need for a DR or a BDR. This network type is used for point-to-point links, such as serial links or Ethernet links that are configured as point-to-point links.

Q47: Which attribute does a router use to select the best path when two or more different routes to the same destination exist from two different routing protocols?

A. dual algorithm

B. metric

C. administrative distance

D. hop count

▼ Answer

A. dual algorithm

B. metric

C. administrative distance

D. hop count

Q48: Router A learns the same route from two different neighbors; one of the neighbor routers is an OSPF neighbor and the other is an EIGRP neighbor. What is the administrative distance of the route that will be installed in the routing table?

A. 20

B. 90

c. 110

D. 115

▼ Answer

A. 20

B. 90

c. 110

D. 115

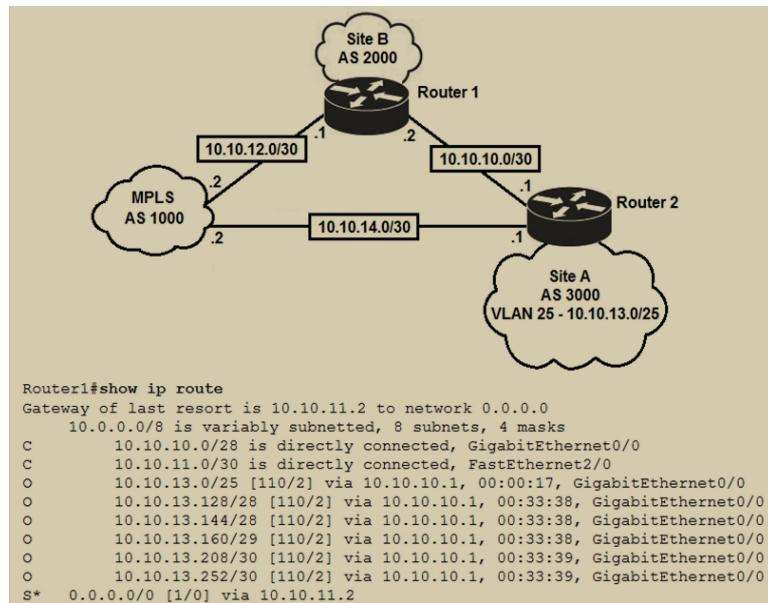


More details Steps:

In this case, the router has learned the same route from an OSPF neighbor and an EIGRP neighbor.

The administrative distances for OSPF and EIGRP are 110 and 90, respectively. Since EIGRP has a lower administrative distance than OSPF, the route learned from the EIGRP neighbor will be installed in the routing table.

Q49: Refer to the exhibit. An engineer is bringing up a new circuit to the MPLS provider on the Gi0/1 interface of Router 1. The new circuit uses eBGP and learns the route to VLAN25 from the BGP path.What is the expected behavior for the traffic flow for route 10.10.13.0/25?



- A. Traffic to 10.10.13.0/25 is load balanced out of multiple interfaces.
- B. Traffic to 10.10.13.0/25 is asymmetrical. (not sure)
- C. Route 10.10.13.0/25 is updated in the routing table as being learned from interface Gi0/1.
- D. Route 10.10.13.0/25 learned via the Gi0/1 interface remains in the routing table. (not sure)

▼ Answer

- A. Traffic to 10.10.13.0/25 is load balanced out of multiple interfaces.
- B. Traffic to 10.10.13.0/25 is asymmetrical. (not sure)**
- C. Route 10.10.13.0/25 is updated in the routing table as being learned from interface Gi0/1.
- D. Route 10.10.13.0/25 learned via the Gi0/1 interface remains in the routing table. (not sure)**



More details Steps:

The output of "show ip route" shows that the route to 10.10.13.0/25 is learned via the Gi0/1 interface. This means that traffic destined for 10.10.13.0/25 will be sent out through the Gi0/1 interface to the MPLS provider network.

However, the gateway of last resort is set to 10.10.11.2, which is not the Gi0/1 interface. This means that if traffic is sent to a destination that is not in the routing table, it will be sent out through the 10.10.11.2 interface instead of the Gi0/1 interface.

So, for example, if a host on LAN1 wants to send traffic to a destination that is not in the routing table, it will be sent out through the 10.10.11.2 interface. But if the same host wants to send traffic to 10.10.13.0/25, it will be sent out through the Gi0/1 interface. This means that traffic for 10.10.13.0/25 may take different paths depending on whether it is already in the routing table or not, resulting in asymmetrical traffic flow.

Q50: Which two actions influence the EIGRP route selection process? (Choose two.)

- A. The advertised distance is calculated by a downstream neighbor to inform the local router of the bandwidth on the link.
- B. The router calculates the feasible distance of all paths to the destination route.
- C. The router must use the advertised distance as the metric for any given route.
- D. The router calculates the best backup path to the destination route and assigns it as the feasible successor.
- E. The router calculates the reported distance by multiplying the delay on the exiting interface by 256.

▼ Answer

- A. The advertised distance is calculated by a downstream neighbor to inform the local router of the bandwidth on the link.
- B. The router calculates the feasible distance of all paths to the destination route.**
- C. The router must use the advertised distance as the metric for any given route.
- D. The router calculates the best backup path to the destination route and assigns it as the feasible successor.**
- E. The router calculates the reported distance by multiplying the delay on the exiting interface by 256.



More details Steps:

The feasible distance (FD) is the best metric value from the local router to the destination network. EIGRP calculates the FD by adding the cost of the outgoing interface to the advertised distance (AD) of the neighbor that is advertising the route. The AD is the metric value that the neighbor is using to reach the destination network.

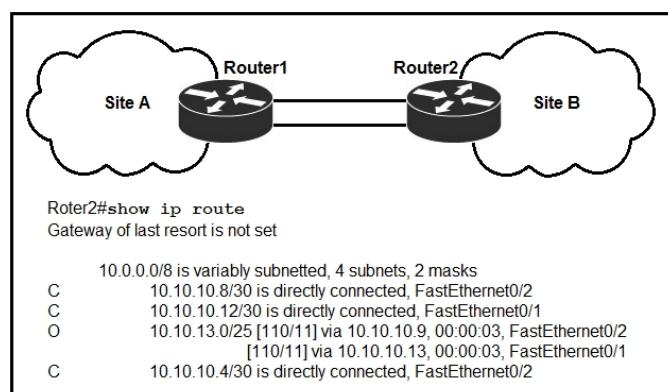
A feasible successor (FS) is a backup path to a destination network that has an FD that is less than the current successor route's FD. The router selects a FS by examining the AD of the neighbor that is advertising the route. If the AD of the neighbor is less than the current successor route's FD, the neighbor is a FS. The router then assigns the FS as a backup path to the current successor route.

A. The advertised distance is calculated by a downstream neighbor to inform the local router of the bandwidth on the link. This statement is not accurate. The advertised distance is the metric value that the neighbor is using to reach the destination network.

C. The router must use the advertised distance as the metric for any given route. This statement is not accurate. The router can use different metrics, such as bandwidth, delay, reliability, load, or a combination of these, to calculate the metric for a given route.

E. The router calculates the reported distance by multiplying the delay on the exiting interface by 256. This statement is not accurate. The reported distance is the sum of the FD and the AD of a neighbor that is advertising the route.

Q51: Refer to the exhibit. If OSPF is running on this network, how does Router2 handle traffic from Site B to 10.10.13.128/25 at Site A?



- A. It sends packets out of interface Fa0/1 only.
- B. It sends packets out of interface Fa0/2 only.
- C. It load-balances traffic out of Fa0/1 and Fa0/2.
- D. It cannot send packets to 10.10.13.128/25.

▼ Answer

- A. It sends packets out of interface Fa0/1 only.
- B. It sends packets out of interface Fa0/2 only.
- C. It load-balances traffic out of Fa0/1 and Fa0/2.
- D. It cannot send packets to 10.10.13.128/25.**



More details Steps:

As the given routing table shows, Router2 has learned the route to the network 10.10.13.0/25 via OSPF with two equal-cost paths through interfaces FastEthernet0/1 and FastEthernet0/2. However, the destination IP address in the question is 10.10.13.128/25, which is not part of the learned network range. The range of 10.10.13.128/25 is from 10.10.13.128 to 10.10.13.255, which means it is not covered by the learned route.

Therefore, Router2 cannot send packets directly to the destination IP address of 10.10.13.128/25, as it does not have a route for it in its routing table. The packet will be dropped or forwarded to the default gateway, depending on the configuration of the router.

Q52: Which two outcomes are predictable behaviors for HSRP? (Choose two.)

- A. The two routers negotiate one router as the active router and the other as the standby router.
- B. The two routers share the same interface IP address, and default gateway traffic is load-balanced between them.

- C. The two routers synchronize configurations to provide consistent packet forwarding.
- D. Each router has a different IP address, both routers act as the default gateway on the LAN, and traffic is load-balanced between them.
- E. The two routers share a virtual IP address that is used as the default gateway for devices on the LAN.

▼ Answer

A. The two routers negotiate one router as the active router and the other as the standby router.

- B. The two routers share the same interface IP address, and default gateway traffic is load-balanced between them.
- C. The two routers synchronize configurations to provide consistent packet forwarding.
- D. Each router has a different IP address, both routers act as the default gateway on the LAN, and traffic is load-balanced between them.

E. The two routers share a virtual IP address that is used as the default gateway for devices on the LAN.



More details Steps:

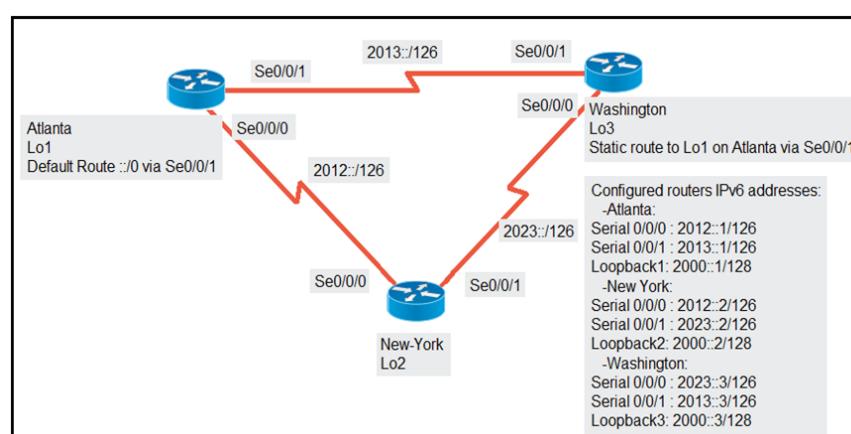
A. The two routers negotiate one router as the active router and the other as the standby router.
HSRP (Hot Standby Router Protocol) is a Cisco proprietary protocol that provides redundancy for IP networks. In HSRP, two or more routers share a virtual IP address and a virtual MAC address, and they work together to present the appearance of a single virtual router on the network. One router is elected as the active router, and the other(s) become the standby router(s). The active router is responsible for forwarding packets sent to the virtual IP address, while the standby router(s) monitor the active router and take over if it fails.

E. The two routers share a virtual IP address that is used as the default gateway for devices on the LAN.
The virtual IP address used by the HSRP routers is used as the default gateway for devices on the LAN. When a device on the LAN sends a packet to a destination outside the local network, it sends the packet to the virtual IP address, which is shared by the active and standby routers. The active router forwards the packet to the destination, while the standby router(s) monitor the active router and take over if it fails.

B, C, and D are not predictable behaviors for HSRP:

- B. The two routers cannot share the same interface IP address, as this would cause IP address conflicts and routing issues.
- C. While HSRP routers can synchronize their configuration, this is not a predictable behavior of HSRP. HSRP only provides redundancy and failover capabilities.
- D. Each router cannot have a different IP address and act as the default gateway on the LAN while traffic is load-balanced between them. HSRP provides a single virtual IP address that is shared by the active and standby routers.

Q53: Refer to the exhibit. An engineer is configuring the New York router to reach the Lo1 interface of the Atlanta router using interface Se0/0/0 as the primary path. Which two commands must be configured on the New York router so that it reaches the Lo1 interface of the Atlanta router via Washington when the link between New York and Atlanta goes down? (Choose two.)



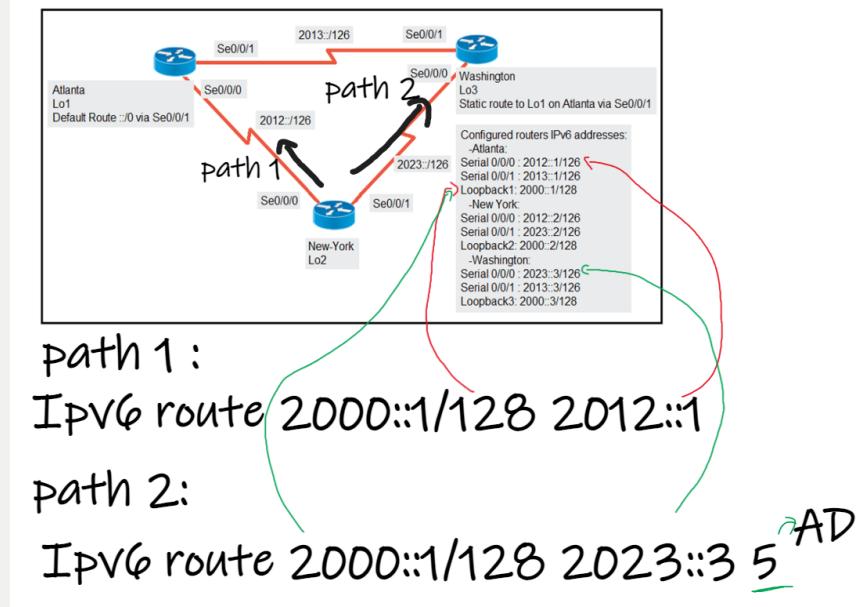
- A. Ipv6 route 2000::1/128 2012::1
- B. Ipv6 route 2000::1/128 2012::1 5
- C. Ipv6 route 2000::1/128 2012::2
- D. Ipv6 route 2000::1/128 2023::2 5
- E. Ipv6 route 2000::1/128 2023::3 5

▼ Answer

- A. Ipv6 route 2000::1/128 2012::1
B. Ipv6 route 2000::1/128 2012::1 5
C. Ipv6 route 2000::1/128 2012::2
D. Ipv6 route 2000::1/128 2023::2 5
E. Ipv6 route 2000::1/128 2023::3 5



More details Steps:



Q54: How does HSRP provide first hop redundancy?

- A. It load-balances Layer 2 traffic along the path by flooding traffic out all interfaces configured with the same VLAN.
B. It uses a shared virtual MAC and a virtual IP address to a group of routers that serve as the default gateway for hosts on a LAN.
C. It forwards multiple packets to the same destination over different routed links in the data path.
D. It load-balances traffic by assigning the same metric value to more than one route to the same destination in the IP routing table.

▼ Answer

- A. It load-balances Layer 2 traffic along the path by flooding traffic out all interfaces configured with the same VLAN.
B. It uses a shared virtual MAC and a virtual IP address to a group of routers that serve as the default gateway for hosts on a LAN.
C. It forwards multiple packets to the same destination over different routed links in the data path.
D. It load-balances traffic by assigning the same metric value to more than one route to the same destination in the IP routing table.



More details Steps:

HSRP (Hot Standby Router Protocol) provides first hop redundancy by allowing multiple routers to share a virtual IP address and a virtual MAC address, which are used as the default gateway for devices on the local network. One router is elected as the active router, and the other(s) become the standby router(s). The active router is responsible for forwarding packets sent to the virtual IP address, while the standby router(s) monitor the active router and take over if it fails.

Option A is not correct because HSRP does not load-balance Layer 2 traffic by flooding traffic out all interfaces configured with the same VLAN. HSRP provides a single virtual MAC address that is shared by the active and standby routers.

Option C is not correct because HSRP does not forward multiple packets to the same destination over different routed links in the data path. HSRP provides a single virtual IP address that is used as the default gateway for devices on the local network.

Option D is not correct because HSRP does not load-balance traffic by assigning the same metric value to more than one route to the same destination in the IP routing table. HSRP provides redundancy and failover capabilities for the default gateway, but it does not affect the routing table or route selection.

Q55: A network engineer is configuring an OSPFv2 neighbor adjacency. Drag and drop the parameters from the left onto their required categories on the right. Not all parameters are used.

Parameter	right
Area ID	Must Match
IP Address	Must Match
Netmask	Must be Unique
OSPF Process ID	_____
Router ID	Must Match
Timers	Must be Unique

▼ Answer

Parameter	Required Category
Area ID	Must Match
IP Address	Must be Unique
Netmask	Must Match
OSPF Process ID	_____
Router ID	Must be Unique
Timers	Must Match



More details Steps:

Must Match:

- Area ID: Routers must be in the same OSPF area to form neighbor adjacencies.
- Netmask: Neighbors must agree on the subnet mask.
- OSPF process ID: This is locally significant and does not technically need to match, but in practice it often does.
- Timers: Hello and Dead timers must match for OSPF adjacency to form.

Must Be Unique:

- IP address: Each router interface must have a unique IP address.
- Router ID: Each OSPF router must have a unique router ID within the OSPF autonomous system.

Q56: R1 has learned route 192.168.12.0/24 via IS-IS, OSPF, RIP, and Internal EIGRP. Under normal operating conditions, which routing protocol is installed in the routing table?

- A. IS-IS
- B. Internal EIGRP
- C. RIP
- D. OSPF

▼ Answer

- A. IS-IS
- B. Internal EIGRP**
- C. RIP
- D. OSPF



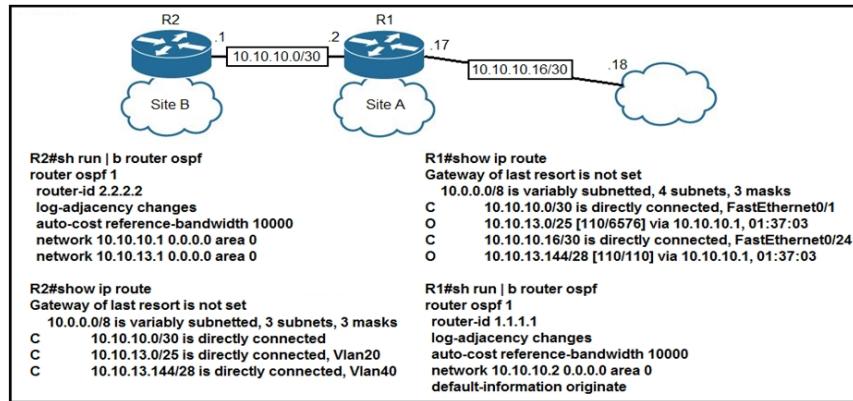
More details Steps:

Assuming all the protocols have the default AD values, the order of preference for protocol selection is as follows:

1. Connected routes
2. Static routes
3. EIGRP summary routes
4. External BGP (EBGP)
5. Internal EIGRP
6. OSPF
7. IS-IS
8. RIP

Therefore, in this case, if all the protocols have the same AD, the Internal EIGRP route would be installed in the routing table since it has the highest order of preference among the given protocols.

Q57: Refer to the exhibit. The default-information originate command is configured under the R1 OSPF configuration. After testing, workstations on VLAN 20 at Site B cannot reach a DNS server on the Internet. Which action corrects the configuration issue?



- A. Add the default-information originate command on R2.
- B. Add the always keyword to the default-information originate command on R1.
- C. Configure the ip route 0.0.0.0 0.0.0.0 10.10.10.18 command on R1.
- D. Configure the ip route 0.0.0.0 0.0.0.0 10.10.10.2 command on R2.

▼ Answer

- A. Add the default-information originate command on R2.
- B. Add the always keyword to the default-information originate command on R1.
- C. Configure the ip route 0.0.0.0 0.0.0.0 10.10.10.18 command on R1.**
- D. Configure the ip route 0.0.0.0 0.0.0.0 10.10.10.2 command on R2.



More details Steps:

The `default-information originate` command in OSPF is used to advertise a default route into the OSPF domain. When this command is configured on R1, it will advertise a default route (0.0.0.0/0) to all other OSPF routers in the domain. However, the default route itself needs to be reachable in order for traffic to be forwarded to the Internet.

In the given scenario, the default route is not reachable because there is no specific route to the next hop for the default route. Therefore, the correct action is to configure a static route on R1 to the next hop for the default route, which is the IP address of the Internet-facing router or the default gateway for R1. The command `ip route 0.0.0.0 0.0.0.0 10.10.10.18` will add a static route to the next hop for the default route with a next-hop IP address of 10.10.10.18.

Option A is not correct because adding the `default-information originate` command on R2 will not help since R2 is not the router where the default route needs to be reached.

Option B is not correct because adding the `always` keyword to the `default-information originate` command will not solve the routing issue. The `always` keyword is used to advertise the default route even if the router does not have a default route in its own routing table.

Option D is not correct because adding a default route on R2 will not solve the routing issue. R2 is not the router where the default route needs to be reached, and adding a default route on R2 will not help the workstations at Site B reach the DNS server on the Internet.

In OSPF, the `default-information originate` command is used to advertise a default route into the OSPF domain. This command is typically used on a border router that connects to an external network, such as the Internet or another routing domain, to provide a default route to other routers in the OSPF domain.

Q58: Refer to the exhibit. With which metric was the route to host 172.16.0.202 learned?

```
R1#show ip route | begin gateway
Gateway of last resort is 209.165.200.246 to network 0.0.0.0
S* 0.0.0.0/0 [1/0] via 209.165.200.246, Serial0/1/0
    is directly connected, Serial0/1/0
  172.16.0.0/16 is variably subnetted, 3 subnets, 3 masks
  S 172.16.0.0/24 [1/0] via 207.165.200.250, Serial0/0/0
  O 172.16.0.128/25 [110/38443] via 207.165.200.254, 00:00:23 Serial0/0/1
  D 172.16.0.192/29 [90/3184439] via 207.165.200.254, 00:00:25 Serial0/0/1
    209.165.200.0/24 is variably subnetted, 4 subnets, 2 masks
    C 209.165.200.248/30 is directly connected, Serial0/0/0
    L 209.165.200.249/32 is directly connected, Serial0/0/0
    C 209.165.200.252/30 is directly connected, Serial0/0/1
    L 209.165.200.253/32 is directly connected, Serial0/0/1
```

- A. 0
- B. 110
- C. 38443
- D. 3184439

▼ Answer

- A. 0
- B. 110
- C. 38443**
- D. 3184439



More details Steps:

The output of the `show ip route` command indicates that there are three subnets in the 172.16.0.0/16 network, and the route to 172.16.0.202 is in the subnet 172.16.0.128/25. The metric for this route is shown as [110/38443], where 110 is the OSPF cost metric and 38443 is the cumulative metric.

Q59: A user configured OSPF in a single area between two routers. A serial interface connecting R1 and R2 is running encapsulation PPP. By default, which OSPF network type is seen on this interface when the user types show ip ospf interface on R1 or R2?

- A. nonbroadcast
- B. point-to-point

- C. point-to-multipoint
- D. broadcast

▼ Answer

- A. nonbroadcast
- B. point-to-point**
- C. point-to-multipoint
- D. broadcast



More details Steps:

The point-to-point network type is used for point-to-point links, such as serial links, where there are only two devices connected. In this network type, OSPF packets are sent directly between the two devices without the need for a designated router or a broadcast domain. This means that there is no need for a DR/BDR election on the link, and each router forms a neighbor adjacency with the other router.

Q60: Which MAC address is recognized as a VRRP virtual address?

- A. 0000.5E00.010a
- B. 0005.3709.8968
- C. 0000.0C07.AC99
- D. 0007.C070.AB01

▼ Answer

- A. 0000.5E00.010a**
- B. 0005.3709.8968
- C. 0000.0C07.AC99
- D. 0007.C070.AB01

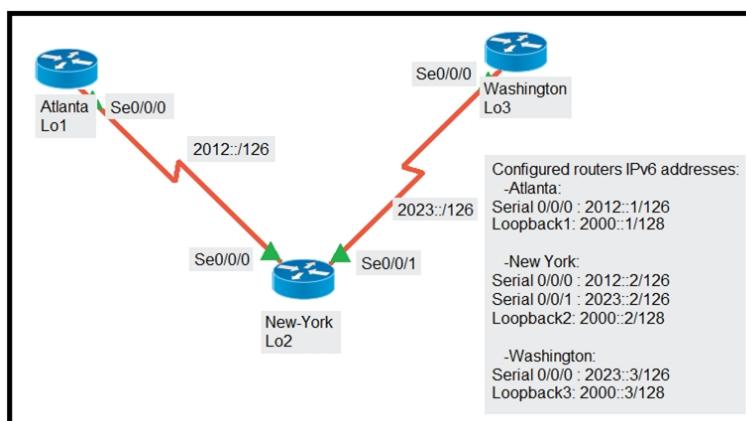


More details Steps:

The MAC address recognized as a Virtual Router Redundancy Protocol (VRRP) virtual address is option A, 0000.5E00.010A.

VRRP is a protocol that provides redundancy for IP networks by allowing multiple routers to share a virtual IP address. The virtual IP address is associated with a virtual MAC address, which is used by the routers to send and receive packets on the network. The virtual MAC address is in the range of 00-00-5E-00-01-00 to 00-00-5E-00-01-FF, with the last octet representing the VRRP virtual router ID.

Q61: Refer to the exhibit. The New York router is configured with static routes pointing to the Atlanta and Washington sites. Which two tasks must be performed so that the Serial0/0/0 interfaces on the Atlanta and Washington routers can reach one another? (Choose two.)



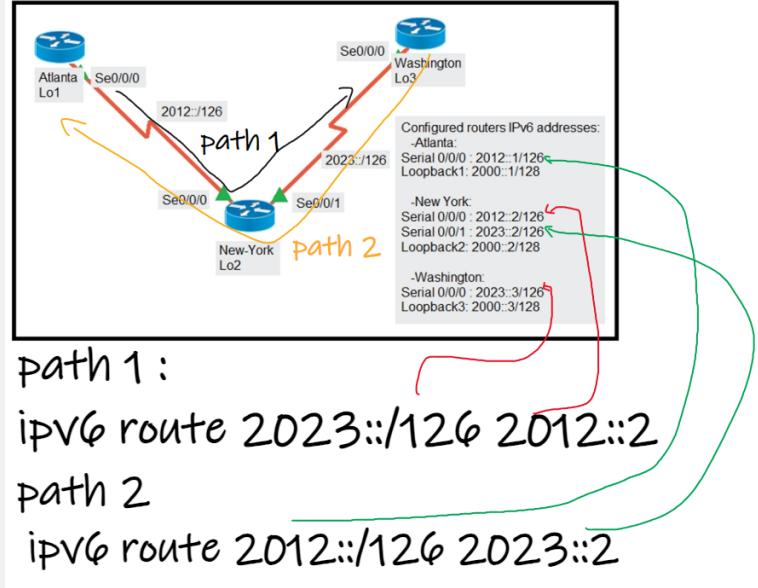
- A. Configure the ipv6 route 2023::/126 2012::1 command on the Atlanta router.
- B. Configure the ipv6 route 2012::/126 2023::2 command on the Washington router.
- C. Configure the ipv6 route 2012::/126 2023::1 command on the Washington router.
- D. Configure the ipv6 route 2023::/126 2012::2 command on the Atlanta router.
- E. Configure the ipv6 route 2012::/126 s0/0/0 command on the Atlanta router.

▼ Answer

- A. Configure the ipv6 route 2023::1/126 2012::1 command on the Atlanta router.
- B. Configure the ipv6 route 2012::1/126 2023::2 command on the Washington router.**
- C. Configure the ipv6 route 2012::1/126 2023::1 command on the Washington router.
- D. Configure the ipv6 route 2023::1/126 2012::2 command on the Atlanta router.**
- E. Configure the ipv6 route 2012::1/126 s0/0/0 command on the Atlanta router.



More details Steps:



Q62: A router running EIGRP has learned the same route from two different paths. Which parameter does the router use to select the best path?

- A. as-path
- B. administrative distance
- C. metric
- D. cost

▼ Answer

- A. as-path
- B. administrative distance
- C. metric**
- D. cost



More details Steps:

When a router learns the same route from two different paths, it calculates the metric for each path using the composite metric formula and selects the path with the lowest metric as the best path. The administrative distance (option B) is used by the router to select the best route between different routing protocols. The as-path (option A) is used in BGP to prevent loops and select the best path between different autonomous systems. The cost (option D) is used in OSPF to select the best path between different routes within the same area.

Q63: An engineer configured an OSPF neighbor as a designated router. Which state verifies the designated router is in the proper mode?

- A. Init
- B. 2-way
- C. Exchange
- D. Full

▼ Answer

- A. Init
- B. 2-way
- C. Exchange
- D. Full**



More details Steps:

Option D, Full, is the correct answer because when a router is elected as the designated router (DR) or backup designated router (BDR) in OSPF, it transitions to the Full state with its neighboring routers. In this state, the routers have a complete and synchronized link-state database and are ready to forward traffic. Therefore, it verifies that the designated router is in the proper mode.

Option A, Init, is not correct because it is the first state in the OSPF neighbor relationship process, where the router sends hello packets and waits for a reply. It does not verify the DR/BDR election.

Option B, 2-way, is also not correct because it is the second state in the OSPF neighbor relationship process, where both routers have received hello packets from each other and have agreed on the parameters of the OSPF session. It does not verify the DR/BDR election.

Option C, Exchange, is the state where routers exchange link-state information, including LSAs and synchronization of their databases, but it does not directly verify that the designated router is in the proper mode.

Q64: Refer to the exhibit. Which route does R1 select for traffic that is destined to 192.168.16.2?

```
R1# show ip route
D  192.168.16.0/26 [90/2679326] via 192.168.1.1
R  192.168.16.0/24 [120/3] via 192.168.1.2
O  192.168.16.0/21 [110/2] via 192.168.1.3
i Li 192.168.16.0/27 [115/30] via 192.168.1.4
```

- A. 192.168.16.0/21
- B. 192.168.16.0/24
- C. 192.168.26.0/26
- D. 192.168.16.0/27

▼ Answer

- A. 192.168.16.0/21
- B. 192.168.16.0/24
- C. 192.168.26.0/26
- D. 192.168.16.0/27**



More details Steps:

The route table shown in the exhibit indicates that R1 has four routes for the 192.168.0.0/16 network. The longest prefix match is used to determine the best route, which means that the route with the most specific match to the destination IP address is selected.

In this case, the destination IP address 192.168.16.2 falls within the range of the subnet 192.168.16.0/27, which has the longest prefix match among the four routes. Therefore, R1 would select the route with the prefix 192.168.16.0/27 for traffic destined to 192.168.16.2.

Option A, 192.168.16.0/21, includes the subnet 192.168.16.0/27, but it also includes other subnets that are not as specific, so it would not be selected.

Option B, 192.168.16.0/24, is less specific than the /27 subnet and would not be selected.

Option C, 192.168.26.0/26, is not within the 192.168.16.0/16 network, so it would not be selected.

Q65: Refer to the exhibit. If configuring a static default route on the router with the ip route 0.0.0 0.0.0.0 10.13.0.1 120 command, how does the router respond?

```
Gateway of last resort is 10.12.0.1 to network 0.0.0.0
O*E2 0.0.0.0/0 [110/1] via 10.12.0.1, 00:00:01, GigabitEthernet0/0
    10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    10.0.0.0/24 is directly connected, GigabitEthernet0/0
L    10.0.0.2/32 is directly connected, GigabitEthernet0/0
C    10.13.0.0/24 is directly connected, GigabitEthernet0/1
L    10.13.0.2/32 is directly connected, GigabitEthernet0/1
```

- A. It starts sending traffic without a specific matching entry in the routing table to GigabitEthernet0/1.
- B. It immediately replaces the existing OSPF route in the routing table with the newly configured static route.
- C. It starts load-balancing traffic between the two default routes.
- D. It ignores the new static route until the existing OSPF default route is removed.

▼ Answer

- A. It starts sending traffic without a specific matching entry in the routing table to GigabitEthernet0/1.
- B. It immediately replaces the existing OSPF route in the routing table with the newly configured static route.
- C. It starts load-balancing traffic between the two default routes.
- D. It ignores the new static route until the existing OSPF default route is removed.**



More details Steps:

Option D is correct because the existing routing table shows that a default route is learned via OSPF with an administrative distance of 110 and a metric of 11. If a static default route with an administrative distance of 120 is added, it will not be used by the router because the OSPF default route has a lower administrative distance. The router will ignore the new static route until the existing OSPF default route is removed.

Option A is not correct because if a static default route with an administrative distance of 120 is configured, the router will add the new static default route to the routing table and use it as the gateway of last resort, even if there is no specific matching entry in the routing table.

Option B is not correct because the new static default route will not replace the existing OSPF default route in the routing table. Both routes will be present in the routing table, but the OSPF default route will be preferred because it has a lower administrative distance.

Option C is not correct because the router will not load-balance traffic between the two default routes. The router will use the OSPF default route as the gateway of last resort until it is removed, and the new static default route will not be used.

Q66: Which two actions are performed by the Weighted Random Early Detection mechanism? (Choose two.)

- A. It supports protocol discovery.
- B. It guarantees the delivery of high-priority packets.
- C. It can identify different flows with a high level of granularity.
- D. It can mitigate congestion by preventing the queue from filling up.
- E. It drops lower-priority packets before it drops higher-priority packets.

▼ Answer

- A. It supports protocol discovery.
- B. It guarantees the delivery of high-priority packets.
- C. It can identify different flows with a high level of granularity.
- D. It can mitigate congestion by preventing the queue from filling up.**
- E. It drops lower-priority packets before it drops higher-priority packets.**



More details Steps:

The Weighted Random Early Detection (WRED) mechanism is used to mitigate congestion in network devices such as routers. It operates by selectively dropping packets before the queue fills up, based on a set of defined criteria.

The two actions performed by the WRED mechanism are:

D. It can mitigate congestion by preventing the queue from filling up. WRED monitors the length of the queue and selectively drops packets based on a set of defined criteria to prevent the queue from becoming congested. WRED can be configured to drop packets based on IP precedence, packet size, or differentiated services code point (DSCP) values.

E. It drops lower-priority packets before it drops higher-priority packets. WRED allows packets to be classified into different priority levels, and it selectively drops packets from lower-priority levels before higher-priority levels. This helps to ensure that high-priority packets are delivered before lower-priority packets.

Option A, supporting protocol discovery, is not an action performed by WRED. Protocol discovery is a feature that allows network devices to learn about the protocols being used on the network.

Option B, guaranteeing the delivery of high-priority packets, is not an action performed by WRED. While WRED can drop lower-priority packets before higher-priority packets, it does not guarantee the delivery of any packets.

Option C, identifying different flows with a high level of granularity, is not an action performed by WRED. Flow identification is typically performed by other mechanisms such as network address translation (NAT) or deep packet inspection (DPI).

Q67: Refer to the exhibit. An engineer configured NAT translations and has verified that the configuration is correct. Which IP address is the source IP after the NAT has taken place?

```
R2#show ip nat translations
Pro Inside global     Inside local      Outside local      Outside global
tcp 172.23.104.3:43268 10.4.4.4:43268 172.23.103.10:23 172.23.103.10:23
tcp 172.23.104.4:45507 10.4.4.5:45507 172.23.103.10:80 172.23.103.10:80
```

- A. 10.4.4.4
- B. 10.4.4.5
- C. 172.23.103.10
- D. 172.23.104.4

▼ Answer

- A. 10.4.4.4
- B. 10.4.4.5
- C. 172.23.103.10**
- D. 172.23.104.4



More details Steps:

Option C is correct because the `show ip nat translations` command output shows that an IP address of 172.23.103.10 is listed as an "Outside global" address, indicating that traffic with a source IP address of 10.4.4.4 has been translated to this IP address. Therefore, the source IP address after NAT has taken place is 172.23.103.10.

Option A is not correct because the `show ip nat translations` command output does not list an IP address of 10.4.4.4 as an "Outside global" address.

Option B is not correct because the `show ip nat translations` command output does not list an IP address of 10.4.4.5 as an "Outside global" address.

Option D is not correct because the `show ip nat translations` command output lists an IP address of 172.23.104.4 as an "Inside global" address, indicating that this is the translated IP address for an "Inside local" IP address of 10.4.4.5. However, the question asks for the source IP address after NAT has taken place, not the translated IP address for a different IP address.

Q68: What event has occurred if a router sends a notice level message to a syslog server?

- A. A network device has restarted.
- B. An ARP inspection has failed.
- C. A routing instance has flapped.
- D. A debug operation is running.

▼ Answer

- A. A network device has restarted.
- B. An ARP inspection has failed.
- C. A routing instance has flapped.**
- D. A debug operation is running.



More details Steps:

Option C is correct because a routing instance flap is an event that could generate a notice-level syslog message. A routing instance flap refers to a situation where a routing protocol instance repeatedly goes up and down in a short period of time. This can cause instability and performance issues in the network, so it is a noteworthy event that should be logged.

Option A, a network device has restarted, could generate syslog messages at various severity levels depending on the device and the specific reason for the restart. However, a restart is not necessarily associated with a notice-level syslog message.

Option B, an ARP inspection has failed, would typically generate syslog messages at a higher severity level than notice, such as warning or error, as it could indicate a security issue or network problem.

Option D, a debug operation is running, would not typically generate a syslog message unless there is an error or specific event associated with the debug operation. Debug operations are used for troubleshooting and are not necessarily noteworthy events that would generate a syslog message by default.

Q69: Drag and Drop the functions from the left onto the correct network components on the right.

Function	right
Resolves web URLs to IP addresses	DNS Server
Assigns a default gateway to a client	DNS Server
Holds the TCP/IP settings to be distributed to the clients	DHCP Server
Stores a list of IP addresses mapped to names	DHCP Server
Assigns IP addresses to enabled clients	DHCP Server

▼ Answer

Function	Network Component
Resolves web URLs to IP addresses	DNS Server
Assigns a default gateway to a client	DHCP Server
Holds the TCP/IP settings to be distributed to the clients	DHCP Server
Stores a list of IP addresses mapped to names	DNS Server
Assigns IP addresses to enabled clients	DHCP Server

Q70: Which two tasks must be performed to configure NTP to a trusted server in client mode on a single network device? (Choose two.)

- A. Enable NTP authentication.
- B. Verify the time zone.
- C. Specify the IP address of the NTP server.
- D. Set the NTP server private key.
- E. Disable NTP broadcasts.

▼ Answer

- A. Enable NTP authentication.**
- B. Verify the time zone.

C. Specify the IP address of the NTP server.

- D. Set the NTP server private key.
- E. Disable NTP broadcasts.



More details Steps:

A. Enable NTP authentication: This task involves configuring authentication for NTP traffic to ensure that only trusted servers can synchronize with the network device. NTP authentication is an optional feature, but it is recommended for security reasons.

C. Specify the IP address of the NTP server: This task involves identifying the IP address of the trusted NTP server to which the network device will synchronize its clock. The NTP server is typically specified as a configuration parameter on the network device using the "ntp server" command.

Options B, D, and E are not required to configure NTP to a trusted server in client mode on a single network device.

Option B, verifying the time zone, is a recommended task to ensure that the network device is configured with the correct time zone. However, it is not required to configure NTP synchronization with a trusted server.

Option D, setting the NTP server private key, is an optional task that is used to encrypt NTP traffic between the network device and the NTP server.

Option E, disabling NTP broadcasts, is an optional task that is used to prevent the network device from broadcasting NTP messages to other devices on the network.

Q71: Drag and drop the network protocols from the left onto the correct transport services on the right.

Network Protocols		right
FTP		Connection Oriented
SMTP		Connection Oriented
SNMP		Connection Oriented
SSH		Connection Oriented
TFTP		Connectionless
VoIP		Connectionless

▼ Answer

Network Protocols	Transport Services
FTP	Connection Oriented
SMTP	Connection Oriented
SNMP	Connectionless
SSH	Connection Oriented
TFTP	Connectionless
VoIP	Connection Oriented



More details Steps:

Connection-oriented protocols require the establishment of a logical connection between the sender and receiver before any data can be exchanged. These protocols ensure reliable data transfer and error recovery. Examples of connection-oriented protocols include FTP, SMTP, SSH, and VoIP.

Connectionless protocols, on the other hand, do not require the establishment of a logical connection before data transfer. These protocols do not guarantee reliable data transfer or error recovery. Examples of connectionless protocols include SNMP and TFTP.

Q72: A network engineer must back up 20 network router configurations globally within a customer environment. Which protocol allows the engineer to perform this function using the Cisco IOS MIB?

- A. ARP
- B. SNMP
- C. SMTP
- D. CDP

▼ Answer

- A. ARP
- B. SNMP**
- C. SMTP
- D. CDP



More details Steps:

By using SNMP to query the Cisco IOS MIB, a network engineer can retrieve the configuration files of the 20 routers and back them up to a centralized location. SNMP provides a standardized way of accessing and managing network devices, making it an ideal choice for network configuration management and backup tasks.

ARP (Address Resolution Protocol) is used for resolving IP addresses to MAC addresses in a local network.

SMTP (Simple Mail Transfer Protocol) is used for sending email messages between servers.

CDP (Cisco Discovery Protocol) is used for discovering and gathering information about directly connected Cisco devices in a network.

Q73: Which command enables a router to become a DHCP client?

- A. ip address dhcp
- B. ip dhcp client
- C. ip helper-address
- D. ip dhcp pool

▼ Answer

- A. ip address dhcp**
- B. ip dhcp client
- C. ip helper-address
- D. ip dhcp pool



More details Steps:

This command instructs the router to obtain its IP address, subnet mask, default gateway, and other network parameters dynamically from a DHCP server. When the router receives an IP address from the DHCP server, it becomes a DHCP client.

Option B, "ip dhcp client", is not a valid command to enable a router to become a DHCP client. It is used to configure DHCP client options, such as the lease time and DHCP server address, on a router interface that has already been configured as a DHCP client using the "ip address dhcp" command.

Option C, "ip helper-address", is used to forward DHCP requests from a subnet to a DHCP server located on a different subnet.

Option D, "ip dhcp pool", is used to define a pool of IP addresses and other DHCP options that can be assigned to DHCP clients. It is not used to enable a router to become a DHCP client.

Q74: Refer to the exhibit. What is the effect of this configuration?

```
ip arp inspection vlan 5-10
interface fastethernet 0/1
switchport node access
switchport access vlan 5
```

- A. The switch discards all ingress ARP traffic with invalid MAC-to-IP address bindings.
- B. All ARP packets are dropped by the switch.
- C. Egress traffic is passed only if the destination is a DHCP server.
- D. All ingress and egress traffic is dropped because the interface is untrusted.

▼ Answer

A. The switch discards all ingress ARP traffic with invalid MAC-to-IP address bindings.

- B. All ARP packets are dropped by the switch.
- C. Egress traffic is passed only if the destination is a DHCP server.
- D. All ingress and egress traffic is dropped because the interface is untrusted.



More details Steps:

- A. The switch discards all ingress ARP traffic with invalid MAC-to-IP address bindings.

ARP inspection is a security feature that helps prevent ARP spoofing attacks by verifying the MAC-to-IP address bindings in ARP packets. When ARP inspection is enabled, the switch inspects all ARP packets that enter an interface and drops any ARP packets that have invalid MAC-to-IP address bindings. This helps ensure that the MAC address in the ARP packet matches the MAC address of the device that sent the packet.

By configuring ARP inspection on VLANs 5 through 10 and configuring the FastEthernet interface as a node access port in VLAN 5, the switch will only inspect ARP packets that enter the interface in VLAN 5. If an ARP packet with an invalid MAC-to-IP address binding is detected, it will be dropped by the switch.

Option B, "All ARP packets are dropped by the switch," is not correct, as ARP inspection only drops ARP packets with invalid MAC-to-IP address bindings, not all ARP packets.

Option C, "Egress traffic is passed only if the destination is a DHCP server," is not correct, as ARP inspection is not related to DHCP server traffic.

Option D, "All ingress and egress traffic is dropped because the interface is untrusted," is not correct, as the interface is not configured as an untrusted port.

Q75: When a site-to-site VPN is used, which protocol is responsible for the transport of user data?

- A. IPsec
- B. IKEv1
- C. MD5
- D. IKEv2

▼ Answer

- A. IPsec**
- B. IKEv1
 - C. MD5
 - D. IKEv2



More details Steps:

A. IPsec (Internet Protocol Security).

IPsec is a suite of protocols used to establish secure connections over IP networks. It provides data confidentiality, integrity, and authenticity by encrypting and authenticating IP packets.

In a site-to-site VPN, IPsec is used to encrypt and decrypt the user data that is being transmitted between the two sites. IPsec is responsible for establishing the secure tunnel between the two VPN endpoints, and for handling the encryption and decryption of the data packets that are being transmitted over the VPN.

IKEv1 and IKEv2 (Internet Key Exchange versions 1 and 2) are used to establish the initial VPN connection and to negotiate the IPsec security parameters. IKEv1 and IKEv2 are responsible for the authentication, key exchange, and security association establishment for the IPsec VPN.

MD5 (Message Digest 5) is a cryptographic hash function that is used for data integrity checking, but it is not used for the transport of user data in a site-to-site VPN.

Q76: Which type of wireless encryption is used for WPA2 in preshared key mode?

- A. AES-128
- B. TKIP with RC4
- C. AES-256
- D. RC4

▼ Answer

- A. AES-128
- B. TKIP with RC4
- C. AES-256**
- D. RC4



More details Steps:

C. AES-256 (Advanced Encryption Standard with a key length of 256 bits).

WPA2 (Wi-Fi Protected Access version 2) is a security protocol used to secure wireless networks. In pre-shared key mode, a single pre-shared key is used to authenticate wireless clients and encrypt the wireless traffic.

WPA2 in pre-shared key mode can use either AES-128 or AES-256 encryption to secure the wireless traffic. Both AES-128 and AES-256 are strong encryption algorithms that are considered to be secure and widely used in various security protocols and applications.

Option A, AES-128, is also a valid encryption algorithm for WPA2 in pre-shared key mode.

Option B, TKIP with RC4 (Temporal Key Integrity Protocol with the RC4 encryption algorithm), is used in WPA (Wi-Fi Protected Access) in pre-shared key mode, but not in WPA2.

Option D, RC4 (Rivest Cipher 4), is a symmetric encryption algorithm that was used in the original WEP (Wired Equivalent Privacy) security protocol, but it is not used in WPA2 in pre-shared key mode.

Q77: Drag and drop the threat-mitigation techniques from the left onto the types of threat or attack they mitigate on the right.

Threat or Attack	right
802.1Q Double Tagging	Configure VACL
ARP Spoofing	Configure Root Guard
Unwanted Superior BPDUs	Configure Dynamic ARP Inspection
Unwanted BPDIJs on PortFast-enabled interfaces	Configure BPDIJ Guard

▼ Answer

Threat or Attack	Threat-Mitigation Technique
802.1Q Double Tagging	Configure VACL
ARP Spoofing	Configure Dynamic ARP Inspection

Threat or Attack	Threat-Mitigation Technique
Unwanted Superior BPDUs	Configure Root Guard
Unwanted BPDIJs on PortFast-enabled interfaces	Configure BPDIJ Guard



More details Steps:

- 802.1Q Double Tagging: This attack involves an attacker adding additional VLAN tags to a frame in order to bypass VLAN segmentation and access resources on different VLANs. This allows the attacker to gain unauthorized access to sensitive data or systems.
- ARP Spoofing: Also known as ARP poisoning, this attack involves an attacker sending fake Address Resolution Protocol (ARP) messages to associate their MAC address with the IP address of another device on the network. This allows the attacker to intercept network traffic, steal sensitive information, or launch other attacks.
- Unwanted Superior BPDUs: This attack involves an attacker sending fake Bridge Protocol Data Units (BPDUs) with a lower Bridge ID priority value than the current root bridge. This can cause other switches in the network to select the attacker's switch as the root bridge, potentially disrupting the network and allowing the attacker to intercept or modify traffic.
- Unwanted BPDIJs on PortFast-enabled interfaces: This attack involves an attacker connecting a switch or hub to a PortFast-enabled interface on a switch. This can create a loop in the network, potentially causing a Spanning Tree Protocol (STP) convergence delay or even network outage. The attacker can then use this disruption to launch further attacks or gain unauthorized access to network resources.

Q78: Which command prevents passwords from being stored in the configuration as plain text on a router or switch?

- A. enable secret
 B. enable password
 C. service password-encryption
 D. username cisco password encrypt

▼ Answer

- A. enable secret
 B. enable password
C. service password-encryption
 D. username cisco password encrypt



More details Steps:

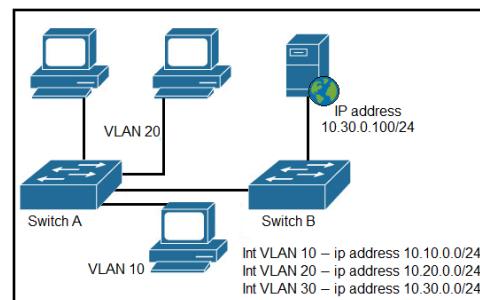
This command enables encryption of all passwords in the configuration file, including the enable secret and enable password. Without this command, the passwords are stored in clear text in the configuration file, which is a security risk if the file is accessed by unauthorized users.

Option A, "enable secret", is used to set a password that is required to enter privileged EXEC mode.

Option B, "enable password", is used to set a password that is required to enter privileged EXEC mode but is not recommended as it stores the password in clear text in the configuration file.

Option D, "username cisco password encrypt", is used to configure a username and password for authentication purposes but it does not encrypt the passwords stored in the configuration file.

Q79: Refer to the exhibit. A network engineer must block access for all computers on VLAN 20 to the web server via HTTP. All other computer must be able to access the web server. Which configuration when applied to Switch A accomplishes the task?



A.

```
config t
ip access-list extended wwwblock
permit ip any any
deny tcp any host 10.30.0.100 eq 80
int vlan 20
ip access-group wwwblock in
```

B.

```
config t
ip access-list extended wwwblock
permit ip any any
deny tcp any host 10.30.0.100 eq 80
int vlan 30
ip access-group wwwblock in
```

C.

```
config t
ip access-list extended wwwblock
deny tcp any host 10.30.0.100 eq 80
int vlan 10
ip access-group wwwblock in
```

D.

```
config t
ip access-list extended wwwblock
deny tcp any host 10.30.0.100 eq 80
permit ip any any
int vlan 20
ip access-group wwwblock in
```

▼ Answer

A.

```
config t
ip access-list extended wwwblock
permit ip any any
deny tcp any host 10.30.0.100 eq 80
int vlan 20
ip access-group wwwblock in
```

B.

```
config t
ip access-list extended wwwblock
permit ip any any
deny tcp any host 10.30.0.100 eq 80
int vlan 30
ip access-group wwwblock in
```

C.

```
config t
ip access-list extended wwwblock
deny tcp any host 10.30.0.100 eq 80
int vlan 10
ip access-group wwwblock in
```

D.

```
config t
ip access-list extended wwwblock
deny tcp any host 10.30.0.100 eq 80
permit ip any any
int vlan 20
ip access-group wwwblock in
```



More details Steps:

In this configuration, an extended access list named 'wwwblock' is created that denies TCP traffic from any source IP to the web server at IP address 10.30.0.100 on port 80 (HTTP). The access list is then applied to VLAN 20 using the `ip access-group` command.

Option A is incorrect because it applies the access list to VLAN 20, which is the correct VLAN that needs to be blocked from accessing the web server, but the order of the access list is incorrect. The access list starts with a "permit any any" statement, which allows all traffic, making the subsequent "deny" statement ineffective. Additionally, the "deny" statement refers to the wrong VLAN; it is referring to IP address 10.30.0.100 on VLAN 30 instead of VLAN 20. As a result, this configuration will not block access for computers on VLAN 20 to the web server via HTTP.

Option B is incorrect because it applies the access list to VLAN 30, which is not the VLAN that needs to be blocked from accessing the web server. The access list is configured to deny TCP traffic to the web server, but it is applied to the wrong VLAN, which means it will not block access for computers on VLAN 20 to the web server via HTTP.

Option C is incorrect because it applies the access list to VLAN 10 instead of VLAN 20. Additionally, the access list is configured to block all TCP traffic to the web server, which would prevent all computers from accessing the server, including those on VLAN 20. Therefore, this configuration will not achieve the desired task of blocking access for computers on VLAN 20 to the web server via HTTP while allowing other computers to access the web server.

Q80: Refer to the exhibit. What is the effect of this configuration?

```
ip arp inspection vlan 2
interface fastethernet 0/1
  switchport mode access
  switchport access vlan 2
```

- A. The switch port interface trust state becomes untrusted.
- B. The switch port remains administratively down until the interface is connected to another switch.
- C. Dynamic ARP inspection is disabled because the ARP ACL is missing.
- D. The switch port remains down until it is configured to trust or untrust incoming packets.

▼ Answer

A. The switch port interface trust state becomes untrusted.

- B. The switch port remains administratively down until the interface is connected to another switch.
- C. Dynamic ARP inspection is disabled because the ARP ACL is missing.
- D. The switch port remains down until it is configured to trust or untrust incoming packets.



More details Steps:

The configuration enables ARP inspection on VLAN 2 using the command `ip arp inspection vlan 2`, which by default sets the trust state of the interface to untrusted. When ARP inspection is enabled on a VLAN, the trust state of the interface is changed to untrusted, and all incoming traffic is inspected by default. This helps to prevent ARP spoofing attacks by ensuring that only legitimate ARP traffic is allowed to pass through.

Additionally, the configuration sets the interface to access VLAN 2 using the commands `interface fastethernet 0/1` and `switchport access vlan 2`, but this does not affect the trust state of the interface.

Option B is incorrect because the configuration does not affect the administrative state of the interface.

Option C is incorrect because the configuration does not disable dynamic ARP inspection or require an ARP ACL.

Q81: What is the difference between AAA authentication and authorization?

- A. Authentication identifies and verifies a user who is attempting to access a system, and authorization controls the tasks the user performs.
- B. Authentication controls the system processes a user accesses, and authorization logs the activities the user initiates.

- C. Authentication verifies a username and password, and authorization handles the communication between the authentication agent and the user database.
- D. Authentication identifies a user who is attempting to access a system, and authorization validates the user's password.

▼ Answer

A. Authentication identifies and verifies a user who is attempting to access a system, and authorization controls the tasks the user performs.

- B. Authentication controls the system processes a user accesses, and authorization logs the activities the user initiates.
- C. Authentication verifies a username and password, and authorization handles the communication between the authentication agent and the user database.
- D. Authentication identifies a user who is attempting to access a system, and authorization validates the user's password.



More details Steps:

Authentication is the process of verifying the identity of a user who is attempting to access a system or resource. It typically involves the user providing some form of identification, such as a username and password, and the system validating this information to determine if the user is authorized to access the system or resource.

Authorization, on the other hand, controls the actions or tasks that the user is allowed to perform once they have been authenticated. It typically involves the system determining what level of access the user has based on their identity and any associated permissions or roles.

In AAA (Authentication, Authorization, and Accounting) systems, authentication and authorization are separate but related processes. Authentication is used to verify the identity of the user, and authorization is used to determine what actions or tasks the user is authorized to perform once they have been authenticated.

Option B is incorrect because it does not accurately describe the difference between authentication and authorization.

Option C is incorrect because it implies that authentication and authorization are both involved in the process of verifying a username and password, which is not accurate. Authentication involves verifying the user's identity, which may include verifying a username and password, while authorization involves controlling the tasks the user can perform.

Option D is incorrect because it suggests that authorization is only concerned with validating the user's password, which is not accurate. Authentication is responsible for verifying the user's identity and authentication credentials, while authorization controls the actions or tasks the user is allowed to perform.

Q82: When configuring a WLAN with WPA2 PSK in the Cisco Wireless LAN Controller GUI, which two formats are available to select? (Choose two.)

- A. decimal
- B. ASCII
- C. hexadecimal
- D. binary
- E. base64

▼ Answer

- A. decimal
- B. ASCII**
- C. hexadecimal**
- D. binary
- E. base64



More details Steps:

ASCII format uses printable characters, such as letters, numbers, and symbols, to represent the passphrase or key. This format is easier for people to read and enter, but it is less secure than hexadecimal format because it can be more easily guessed or cracked.

Hexadecimal format uses a combination of numbers and letters (A-F) to represent the passphrase or key. This format is more secure than ASCII format because it is more difficult to guess or crack, but it can be more difficult for people to read and enter.

Option A, decimal and option D, binary are not available formats for configuring WPA2 PSK on Cisco Wireless LAN Controller GUI.

Option E, base64 is not a format available for WPA2 PSK on Cisco Wireless LAN Controller GUI. Base64 is used for encoding and decoding binary data in ASCII format, but it is not a format for entering passwords or keys.

Q83: Drag and drop the AAA functions from the left onto the correct AAA services on the right.

AAA Function	right
Identifies the user	Authentication
Verifies the password	Authentication
Controls the actions a user can perform	Accounting
Restricts the services available to a user	Accounting
Records user activities	Authorization
Provides analytical information for the network administrator	Authorization

▼ Answer

AAA Function	AAA Service
Identifies the user	Authentication
Verifies the password	Authentication
Controls the actions a user can perform	Authorization
Restricts the services available to a user	Authorization
Records user activities	Accounting
Provides analytical information for the network administrator	Accounting



More details Steps:

- Authentication is the process of identifying and verifying the identity of a user who is attempting to access a system or resource. This function involves verifying the user's identity and password or other authentication credentials.
- Authorization controls the actions or tasks that the user is allowed to perform once they have been authenticated. This function involves determining what level of access the user has based on their identity and any associated permissions or roles.
- Accounting records user activities and provides analytical information for the network administrator. This function involves logging and tracking user activities, such as login attempts, resource usage, and system events.

Q84: An engineer is asked to protect unused ports that are configured in the default VLAN on a switch. Which two steps will fulfill the request? (Choose two.)

- A. Configure the ports as trunk ports.
- B. Enable the Cisco Discovery Protocol.
- C. Configure the port type as access and place in VLAN 99.
- D. Administratively shut down the ports.
- E. Configure the ports in an EtherChannel.

▼ Answer

- A. Configure the ports as trunk ports.
- B. Enable the Cisco Discovery Protocol.
- C. Configure the port type as access and place in VLAN 99.**
- D. Administratively shut down the ports.**
- E. Configure the ports in an EtherChannel.



More details Steps:

C. Configure the port type as access and place in VLAN 99: By configuring the port type as access, the port will not carry multiple VLAN traffic and will be limited to a single VLAN. Placing the port in VLAN 99 ensures that the port is not in the default VLAN and is separate from the regular data traffic.

D. Administratively shut down the ports: By shutting down the ports, they will be disabled and will not transmit or receive any traffic. This helps to prevent any unauthorized access or attack on the network through the unused ports.

A. Configuring the ports as trunk ports, E. Configuring the ports in an EtherChannel, and B. Enabling the Cisco Discovery Protocol are not effective methods to protect unused ports in the default VLAN on a switch.

Configuring the ports as trunk ports or in an EtherChannel is not necessary and could potentially create security vulnerabilities by allowing multiple VLAN traffic to pass through the ports.

Enabling the Cisco Discovery Protocol is not related to protecting unused ports in the default VLAN, it is a protocol used by Cisco devices to share information about other directly connected Cisco equipment.

Q85: An email user has been lured into clicking a link in an email sent by their company's security organization. The webpage that opens reports that it was safe, but the link may have contained malicious code.Which type of security program is in place?

- A. user awareness
- B. brute force attack
- C. physical access control
- D. social engineering attack

▼ Answer

A. user awareness

- B. brute force attack
- C. physical access control
- D. social engineering attack



More details Steps:

User awareness is a type of security program that aims to educate and train users on how to recognize and respond to potential security threats. In this scenario, the user may have been lured into clicking a link in an email, which could potentially lead to a security breach if the link contained malicious code.

The fact that the webpage that opened reported that it was safe suggests that some form of security program is in place to scan and check for potential threats. However, the fact that the link may have contained malicious code highlights the importance of user awareness and the need to educate users on how to avoid falling for phishing and other types of social engineering attacks.

Option B, "brute force attack," is a type of attack that involves using automated tools to guess passwords or encryption keys through trial and error.

Option C, "physical access control," is a type of security program that restricts access to physical resources, such as buildings, rooms, or data centers.

Option D, "social engineering attack," is a type of attack that involves manipulating or tricking users into divulging sensitive information or performing actions that could compromise security. In this scenario, the user may have been targeted by a social engineering attack through the use of a lure in the email.

Q86: Drag and drop the Cisco Wireless LAN Controller security settings from the left onto the correct security mechanism categories on the right.

Cisco Wireless LAN Controller Security Setting	right
Web policy	Layer 2 Security Mechanisms
Passthrough	Layer 2 Security Mechanisms
WPA+WPA2	Layer 3 Security Mechanisms
802.1X	Layer 3 Security Mechanisms

▼ Answer

Cisco Wireless LAN Controller Security Setting	Security Mechanism Category
Web policy	Layer 3 Security Mechanisms
Passthrough	Layer 3 Security Mechanisms
WPA+WPA2	Layer 2 Security Mechanisms
802.1X	Layer 2 Security Mechanisms



More details Steps:

- Layer 2 Security Mechanisms: These security mechanisms operate at the data link layer (Layer 2) of the OSI model and include security features such as MAC address filtering, VLAN assignment, and WPA/WPA2 encryption. WPA+WPA2 and 802.1X are Layer 2 security mechanisms used to secure wireless networks.
- Layer 3 Security Mechanisms: These security mechanisms operate at the network layer (Layer 3) of the OSI model and include security features such as access control lists (ACLs), firewalls, and web policies. Web policy and Passthrough are Layer 3 security mechanisms used to secure wireless networks.
- Web policy: Web policy is a Layer 3 security mechanism that allows network administrators to control and restrict access to web-based content based on user identity, group membership, or other criteria. Web policy can be used to block access to malicious websites, limit access to specific types of web content, or enforce compliance with company policies.
- Passthrough: Passthrough is a Layer 3 security mechanism that allows wireless clients to connect to an external authentication server (such as a RADIUS server) for authentication and authorization. With Passthrough enabled, the wireless LAN controller acts as a proxy between the wireless client and the authentication server, passing authentication requests and responses back and forth.
- WPA+WPA2: WPA+WPA2 is a Layer 2 security mechanism that provides strong encryption and authentication for wireless networks. It uses either a pre-shared key (PSK) or a server-based authentication method (such as RADIUS) to authenticate wireless clients and establish a shared encryption key. WPA+WPA2 is considered more secure than WEP (Wired Equivalent Privacy), which is an older and less secure wireless encryption standard.
- 802.1X: 802.1X is a Layer 2 security mechanism that provides port-based network access control for wired and wireless networks. It uses an Extensible Authentication Protocol (EAP) to authenticate clients and provides dynamic per-user, per-session encryption keys. 802.1X can be used in conjunction with other security mechanisms, such as MAC address filtering and VLAN assignment, to provide a comprehensive security solution for wireless networks.

Q87: Which feature on the Cisco Wireless LAN Controller when enabled restricts management access from specific networks?

- A. TACACS
- B. CPU ACL
- C. Flex ACL
- D. RADIUS

▼ Answer

A. TACACS

B. CPU ACL

C. Flex ACL

D. RADIUS



More details Steps:

CPU ACL (Access Control List) is a feature on the Cisco Wireless LAN Controller that allows network administrators to restrict management access to the controller from specific networks or hosts. When CPU ACL is enabled, the controller will only accept management traffic from the networks or hosts specified in the ACL.

TACACS (Terminal Access Controller Access Control System) and RADIUS (Remote Authentication Dial-In User Service) are both authentication protocols used to provide centralized authentication, authorization, and accounting (AAA) services for network devices and users. They are not specifically designed to restrict management access from specific networks.

Flex ACL (Access Control List) is a feature on the Cisco Wireless LAN Controller that allows network administrators to apply access control policies to wireless clients based on user identity, device type, or other criteria. It is not specifically designed to restrict management access from specific networks.

Q88: Which set of actions satisfy the requirement for multifactor authentication?

- A. The user enters a user name and password, and then re-enters the credentials on a second screen.
- B. The user swipes a key fob, then clicks through an email link.
- C. The user enters a user name and password, and then clicks a notification in an authentication app on a mobile device.
- D. The user enters a PIN into an RSA token, and then enters the displayed RSA key on a login screen.

▼ Answer

A. The user enters a user name and password, and then re-enters the credentials on a second screen.

B. The user swipes a key fob, then clicks through an email link.

C. The user enters a user name and password, and then clicks a notification in an authentication app on a mobile device.

D. The user enters a PIN into an RSA token, and then enters the displayed RSA key on a login screen.



More details Steps:

Multifactor authentication (MFA) is a security mechanism that requires users to provide two or more forms of authentication to access a system or resource. The idea behind MFA is to increase the security of the authentication process by requiring something the user knows (such as a password) and something the user has (such as a mobile device).

Option A only provides a single factor of authentication (something the user knows) and is not considered multifactor authentication.

Option B also only provides a single factor of authentication (something the user has) and is not considered multifactor authentication.

Option D provides two factors of authentication (something the user has and something the user knows), but the use of an RSA token and key is not as widely used as the use of authentication apps on mobile devices.

Option C provides two factors of authentication (something the user knows and something the user has) by requiring the user to enter a username and password (something the user knows) and then click a notification in an authentication app on a mobile device (something the user has). This is considered a more secure form of multifactor authentication and is widely used in many organizations.

Q89: Which configuration is needed to generate an RSA key for SSH on a router?

- A. Configure VTY access.
- B. Configure the version of SSH.
- C. Assign a DNS domain name.
- D. Create a user with a password.

▼ Answer

- A. Configure VTY access.
- B. Configure the version of SSH.
- C. Assign a DNS domain name.**
- D. Create a user with a password.



More details Steps:

- C. Assign a DNS domain name.

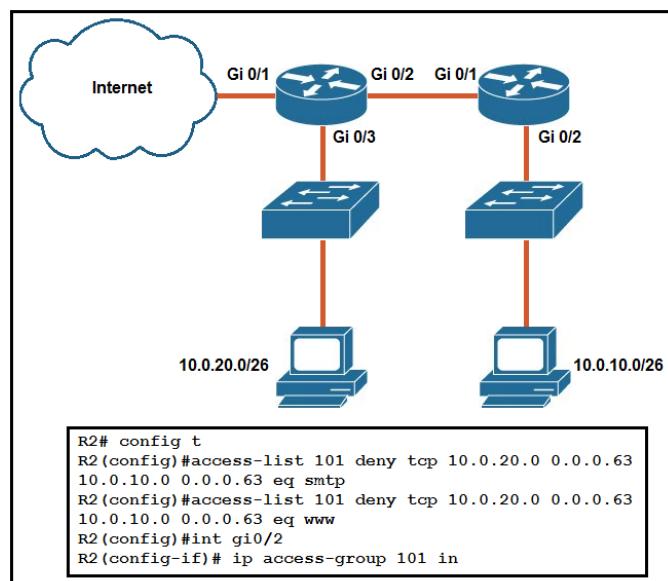
To generate an RSA key for SSH, the router requires a fully qualified domain name (FQDN) to be configured. This is typically done by assigning a DNS domain name to the router using the "ip domain-name" command. The DNS domain name is used to generate a unique RSA key for the router. Once the DNS domain name is assigned, the RSA key pair can be generated using the "crypto key generate rsa" command.

Option A, "Configure VTY access," is not directly related to generating an RSA key for SSH on a router. VTY access is used for remote access to the router using Telnet or SSH.

Option B, "Configure the version of SSH," is not directly related to generating an RSA key for SSH on a router. While SSH version 2 is required for secure communication, it is not a requirement for generating an RSA key pair.

Option D, "Create a user with a password," is not directly related to generating an RSA key for SSH on a router. While creating a user with a password is necessary for authenticating to the router through SSH, it is not specific to generating an RSA key pair.

Q90: Refer to the exhibit. An extended ACL has been configured and applied to router R2. The configuration failed to work as intended. Which two changes stop outbound traffic on TCP ports 25 and 80 to 10.0.20.0/26 from the 10.0.10.0/26 subnet while still allowing all other traffic? (Choose two.)



- A. Add a "permit ip any any" statement at the end of ACL 101 for allowed traffic.
- B. Add a "permit ip any any" statement to the beginning of ACL 101 for allowed traffic.
- C. The ACL must be moved to the Gi0/1 interface outbound on R2.
- D. The source and destination IPs must be swapped in ACL 101.
- E. The ACL must be configured the Gi0/2 interface inbound on R1.

▼ Answer

- A. Add a "permit ip any any" statement at the end of ACL 101 for allowed traffic.**
- B. Add a "permit ip any any" statement to the beginning of ACL 101 for allowed traffic.
- C. The ACL must be moved to the Gi0/1 interface outbound on R2.
- D. The source and destination IPs must be swapped in ACL 101.**
- E. The ACL must be configured the Gi0/2 interface inbound on R1.

**More details Steps:**

- A. Add a "permit ip any any" statement at the end of ACL 101 for allowed traffic.

Since ACLs are processed from top to bottom, the last statement of the ACL should allow all traffic that is not explicitly denied. Adding a "permit ip any any" statement at the end of the ACL will ensure that all other traffic is allowed while still blocking traffic to TCP ports 25 and 80 to 10.0.20.0/26 from the 10.0.10.0/26 subnet.

- D. The source and destination IPs must be swapped in ACL 101.

In the current ACL, the source and destination IP addresses are reversed. To block traffic from the 10.0.10.0/26 subnet to TCP ports 25 and 80 on the 10.0.20.0/26 subnet, the source IP address should be 10.0.10.0/26 and the destination IP address should be 10.0.20.0/26.

Option B, "Add a 'permit ip any any' statement to the beginning of ACL 101 for allowed traffic," is not a correct solution because it would allow all traffic, including the traffic that is intended to be blocked. The existing deny statements in the ACL would be bypassed since the "permit ip any any" statement would match all traffic and allow it through.

Option C, "The ACL must be moved to the Gi0/1 interface outbound on R2," is not a correct solution because the ACL needs to be applied inbound on the interface where the traffic is coming from, which is the Gi0/2 interface. Applying the ACL outbound on the Gi0/1 interface would not have any effect since the traffic has already left the router on the Gi0/2 interface.

Q91: An engineer must configure a WLAN using the strongest encryption type for WPA2-PSK. Which cipher fulfills the configuration requirement?

- A. WEP
- B. AES
- C. RC4
- D. TKIP

▼ Answer

- A. WEP
- B. AES**
- C. RC4
- D. TKIP

**More details Steps:**

WEP (Wired Equivalent Privacy) is an older and less secure encryption protocol that can be easily cracked, and it is not recommended for use in modern WLANs. RC4 (Rivest Cipher 4) is also an older encryption algorithm that has been found to have vulnerabilities and is no longer considered secure. TKIP (Temporal Key Integrity Protocol) is a legacy encryption protocol that was designed to address the weaknesses of WEP, but it is also considered less secure than AES and is no longer recommended for use in modern WLANs.

Q92: Which statement compares traditional networks and controller-based networks?

- A. Only controller-based networks decouple the control plane and the data plane.
- B. Traditional and controller-based networks abstract policies from device configurations.
- C. Only traditional networks natively support centralized management.
- D. Only traditional networks offer a centralized control plane.

▼ Answer

- A. Only controller-based networks decouple the control plane and the data plane.**
- B. Traditional and controller-based networks abstract policies from device configurations.
- C. Only traditional networks natively support centralized management.
- D. Only traditional networks offer a centralized control plane.



More details Steps:

In traditional networking, the control plane (which decides where traffic is sent) and the data plane (which forwards traffic to the selected destination) are tightly coupled within each network device.

In contrast, controller-based networks – often associated with Software Defined Networking (SDN) – decouple the control plane from the data plane. The control plane is centralized in a controller, and the data plane remains distributed across the network devices. This separation allows for more flexibility and programmability in the network.

Option B is incorrect because policy abstraction from device configurations is more commonly associated with controller-based networks rather than traditional networks.

Option C and D are incorrect because traditional networks typically do not support centralized management or offer a centralized control plane. In traditional networks, each device operates independently with its own control plane, which is the opposite of a centralized approach.

Q93: What are two benefits of network automation? (Choose two.)

- A. reduced hardware footprint
- B. reduced operational costs
- C. faster changes with more reliable results
- D. fewer network failures
- E. increased network security

▼ Answer

- A. reduced hardware footprint
- B. reduced operational costs**
- C. faster changes with more reliable results**
- D. fewer network failures
- E. increased network security



More details Steps:

A "hardware footprint" refers to the physical space occupied by a piece of hardware or a system. It can also refer to the overall impact of the hardware on its environment, which may include factors like power consumption, heat generation, and requirements for cooling infrastructure.

B. Reduced operational costs: Network automation can significantly reduce the time and effort required for network management tasks, such as configuration, troubleshooting, and maintenance, which can lead to substantial operational cost savings.

C. Faster changes with more reliable results: Automation can make changes to the network faster and more accurately than manual processes. It also ensures that the same standard procedures are followed every time, leading to more consistent and reliable results.

While automation can indirectly contribute to A, D, and E, it is not the primary factor in reducing hardware footprint, preventing network failures, or increasing network security. For example, network failures could be due to a variety of reasons such as hardware faults, software bugs, or human errors, not just lack of automation. Similarly, network security involves a broad range of measures, and while automation can help implement these measures more efficiently, it is not a direct result of automation. Finally, a reduced hardware footprint is more directly related to factors such as virtualization or the use of cloud services.

Q94: Which two encoding methods are supported by REST APIs? (Choose two.)

- A. SGML
- B. YAML
- C. XML
- D. JSON
- E. EBCDIC

▼ Answer

- A. SGML
- B. YAML

C. XML

D. JSON

E. EBCDIC



More details Steps:

C. XML (eXtensible Markup Language): REST APIs can use XML as an encoding method. XML is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.

D. JSON (JavaScript Object Notation): JSON is a popular, lightweight data-interchange format that is easy for humans to read and write and easy for machines to parse and generate. Many REST APIs use JSON because of its simplicity and effectiveness.

A. SGML (Standard Generalized Markup Language): While SGML is a markup language, it is not typically used as an encoding method for REST APIs.

B. YAML (YAML Ain't Markup Language): While YAML is often used for writing data serialization standards and configuration files, it is not typically used as an encoding method for REST APIs.

E. EBCDIC (Extended Binary Coded Decimal Interchange Code): EBCDIC is a character encoding used mainly on IBM mainframe and IBM midrange computer systems. It is not used as an encoding method for REST APIs.

Q95: What are two characteristics of a controller-based network? (Choose two.)

- A. It uses Telnet to report system issues.
- B. The administrator can make configuration updates from the CLI.
- C. It uses northbound and southbound APIs to communicate between architectural layers.
- D. It decentralizes the control plane, which allows each device to make its own forwarding decisions.
- E. It moves the control plane to a central point.

▼ **Answer**

- A. It uses Telnet to report system issues.
- B. The administrator can make configuration updates from the CLI.
- C. It uses northbound and southbound APIs to communicate between architectural layers.**
- D. It decentralizes the control plane, which allows each device to make its own forwarding decisions.
- E. It moves the control plane to a central point.**



More details Steps:

C. It uses northbound and southbound APIs to communicate between architectural layers: In a controller-based network, the controller uses southbound APIs to communicate with network devices and northbound APIs to provide information to applications and orchestration tools.

E. It moves the control plane to a central point: Controller-based networks, such as those in Software Defined Networking (SDN), centralize the control plane in the controller. This allows for greater programmability, flexibility, and ease of network management.

A. It uses Telnet to report system issues: While Telnet could potentially be used in any network for remote command execution, it's not a defining feature of controller-based networks.

B. The administrator can make configuration updates from the CLI: While this is true for many types of networks, it's not specifically a characteristic of controller-based networks. In fact, controller-based networks often rely more on graphical user interfaces and APIs for configuration.

D. It decentralizes the control plane, which allows each device to make its own forwarding decisions: This is actually a characteristic of traditional, non-controller-based networks. In controller-based networks, the control plane is centralized.

Q96: Which output displays a JSON data representation?

- A.

```
{  
  "response": {  
    "taskId": {},  
    "url": "string"  
  },  
  "version": "string"  
}
```

B.

```
{  
  "response"- {  
    "taskId"- {},  
    "url"- "string"  
  },  
  "version"- "string"  
}
```

C.

```
{  
  "response": {  
    "taskId": {},  
    "url": "string"  
  },  
  "version": "string"  
}
```

D.

```
{  
  "response". {  
    "taskId": {},  
    "url": "string"  
  },  
  "version": "string"  
}
```

▼ Answer

A.

```
{  
  "response": {  
    "taskId": {},  
    "url": "string"  
  },  
  "version": "string"  
}
```

B.

```
{  
  "response"- {  
    "taskId"- {},  
    "url"- "string"  
  },  
  "version"- "string"  
}
```

C.

```
{  
  "response": {  
    "taskId": {},  
    "url": "string"  
  },  
  "version": "string"  
}
```

D.

```
{  
  "response": {  
    "taskId": {},  
    "url": "string"  
  },  
  "version": "string"  
}
```



More details Steps:

In JSON format, data is represented in key-value pairs with keys and values separated by a colon `:`. The pairs are enclosed in curly braces `{}`. Strings are enclosed in double quotes `" "`, and commas `,` are used to separate the pairs.

Q97: Drag and drop the descriptions from the left onto the correct configuration-management technologies on the right.

Description	right
Fundamental configuration elements are stored in a manifest	Puppet
Uses TCP port 10002 for configuration push jobs	Puppet
Uses Ruby for fundamental configuration elements	Ansible
Uses SSH for remote device communication	Ansible
Uses TCP 8140 for communication	Chef
Uses YAML for fundamental configuration elements	Not applicable

▼ Answer

Description	Configuration-Management Technology
Fundamental configuration elements are stored in a manifest	Puppet
Uses TCP port 10002 for configuration push jobs	Not applicable
Uses Ruby for fundamental configuration elements	Chef
Uses SSH for remote device communication	Ansible
Uses TCP 8140 for communication	Puppet
Uses YAML for fundamental configuration elements	Ansible



More details Steps:

- **Puppet** uses a declarative language to describe system configuration, which is written in a 'manifest' file. Puppet uses TCP 8140 for communication between the master and client nodes.
- **Chef** uses Ruby as its reference language for creating cookbooks and recipes (which contain the fundamental configuration elements).
- **Ansible** uses YAML for writing Ansible playbooks (which contain the fundamental configuration elements). Ansible communicates with remote machines over SSH.

Q98: Which two capabilities of Cisco DNA Center make it more extensible as compared to traditional campus device management? (Choose two.)

- A. REST APIs that allow for external applications to interact natively
- B. adapters that support all families of Cisco IOS software
- C. SDKs that support interaction with third-party network equipment
- D. modular design that is upgradable as needed
- E. customized versions for small, medium, and large enterprises

▼ Answer

A. REST APIs that allow for external applications to interact natively

- B. adapters that support all families of Cisco IOS software
- C. SDKs that support interaction with third-party network equipment
- D. modular design that is upgradable as needed

E. customized versions for small, medium, and large enterprises



More details Steps:

A. REST APIs that allow for external applications to interact natively: Cisco DNA Center uses REST APIs which allow for programmability. This enables external applications to interact directly with Cisco DNA Center, making it more extensible.

E. Customized versions for small, medium, and large enterprises: Cisco DNA Center's ability to offer customized versions for different sizes of enterprises contributes to its extensibility. It allows the platform to be flexible and adaptable to the needs of different organizations, which can be seen as a form of extensibility.

Options B, C, be features or advantages of Cisco DNA Center, but they don't specifically make it more extensible compared to traditional campus device management.

Option B. While Cisco DNA Center does support a wide range of Cisco devices, this does not necessarily relate to extensibility.

Option C. SDKs for third-party network equipment would certainly increase extensibility, but as of my knowledge cutoff in September 2021, Cisco DNA Center primarily supports Cisco devices.

Q99: What are two southbound APIs? (Choose two.)

- A. Thrift
- B. DSC
- C. CORBA
- D. NETCONF
- E. OpenFlow

▼ Answer

- A. Thrift
- B. DSC
- C. CORBA
- D. NETCONF**
- E. OpenFlow**



More details Steps:

D. NETCONF (Network Configuration Protocol): NETCONF is a protocol defined by the IETF. It provides mechanisms to install, manipulate, and delete the configuration of network devices. It uses an RPC (Remote Procedure Call) model for communication between a client and a server.

E. OpenFlow: OpenFlow is one of the first standards for SDN (Software Defined Networking). It allows direct access and manipulation of the forwarding plane of network devices, such as switches and routers.

Both NETCONF and OpenFlow are considered southbound APIs in the context of SDN. "Southbound APIs" are the interfaces that provide SDN Controllers the ability to program the network and control the behavior of network devices (like switches and routers).

Options A (Thrift), B (DSC), and C (CORBA) are not considered southbound APIs in the context of SDN and network programming.

Q100: What makes Cisco DNA Center different from traditional network management applications and their management of networks?

- A. Its modular design allows the implementation of different versions to meet the specific needs of an organization.
- B. It only supports auto-discovery of network elements in a greenfield deployment.
- C. It omits support high availability of management functions when operating in cluster mode.
- D. It abstracts policy from the actual device configuration.

▼ Answer

- A. Its modular design allows the implementation of different versions to meet the specific needs of an organization.
- B. It only supports auto-discovery of network elements in a greenfield deployment.
- C. It omits support high availability of management functions when operating in cluster mode.
- D. It abstracts policy from the actual device configuration.**



More details Steps:

D. It abstracts policy from the actual device configuration: Cisco DNA Center represents a shift from traditional command-line interface (CLI) configuration to a policy-based approach. Instead of manually configuring devices, network administrators define policies (intent) that Cisco DNA Center translates into device-specific configurations. This abstraction simplifies network management and provides greater consistency and scalability.

Here's why the other options are not correct:

- A. Its modular design allows the implementation of different versions to meet the specific needs of an organization:** While the modular design of Cisco DNA Center does provide flexibility, it's not what fundamentally differentiates it from traditional network management applications.
- B. It only supports auto-discovery of network elements in a greenfield deployment:** Cisco DNA Center supports auto-discovery of network elements in both greenfield (new and unconfigured) and brownfield (existing and configured) deployments.
- C. It omits support high availability of management functions when operating in cluster mode:** This statement is incorrect. Cisco DNA Center does support high availability when operating in cluster mode, ensuring management functionality is maintained even if one node fails.

Q101: Which API is used in controller-based architectures to interact with edge devices?

- A. southbound
- B. overlay
- C. northbound
- D. underlay

▼ Answer

A. southbound

- B. overlay
- C. northbound
- D. underlay



More details Steps:

A. Southbound API: In controller-based architectures, a southbound API is used to communicate from the controller down to the network devices (also known as edge devices). This API allows the controller to program the network devices and control their behavior. Examples of southbound APIs include OpenFlow, NETCONF, and others.

Here's why the other options are not correct:

- B. Overlay:** This term typically refers to a virtual network built on top of another network. It doesn't refer to an API used to interact with edge devices.
- C. Northbound API:** This is used to communicate from the controller up to the applications and orchestration tools. It's not used for interaction with edge devices.
- D. Underlay:** This term typically refers to the physical network infrastructure over which a virtual or overlay network is built. It doesn't refer to an API used to interact with edge devices.

Q102: An organization has decided to start using cloud-provided services. Which cloud service allows the organization to install its own operating system on a virtual machine?

- A. platform-as-a-service
- B. network-as-a-service

- C. software-as-a-service
- D. infrastructure-as-a-service

▼ Answer

- A. platform-as-a-service
- B. network-as-a-service
- C. software-as-a-service
- D. infrastructure-as-a-service**



More details Steps:

D. Infrastructure-as-a-Service (IaaS): This form of cloud service provides virtualized computing resources over the internet. It provides the infrastructure such as virtual machines and other resources like virtual-machine disk image library, block and file-based storage, firewalls, load balancers, IP addresses, virtual local area networks, etc. In an IaaS model, the cloud provider hosts the infrastructure components that are traditionally present in an on-premises data center, including servers, storage, and networking hardware, as well as the virtualization or hypervisor layer. This allows an organization to install its own operating system on a virtual machine.

The other options do not fit:

- A. Platform-as-a-Service (PaaS):** This type of cloud computing service provides a platform allowing customers to develop, run, and manage applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an app.
- B. Network-as-a-Service (NaaS):** This is a business model for delivering enterprise-wide area network services virtually on a subscription basis.
- C. Software-as-a-Service (SaaS):** This is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted. It is also known as "on-demand software".

Q103: Which option about JSON is true?

- A. uses predefined tags or angle brackets () to delimit markup text
- B. used to describe structured data that includes arrays
- C. used for storing information
- D. similar to HTML, it is more verbose than XML.

▼ Answer

- A. uses predefined tags or angle brackets () to delimit markup text
- B. used to describe structured data that includes arrays**
- C. used for storing information
- D. similar to HTML, it is more verbose than XML.



More details Steps:

B. Used to describe structured data that includes arrays: JSON (JavaScript Object Notation) is a lightweight data-interchange format that is easy for humans to read and write and easy for machines to parse and generate. It can represent numbers, strings, ordered sequences of values (arrays), and collections of name/value pairs (objects). This makes it ideal for structured data representation, including arrays.

The other options are not correct:

- A. Uses predefined tags or angle brackets () to delimit markup text:** This statement describes XML or HTML. JSON uses key-value pairs for data representation, not tags or angle brackets.
- C. Used for storing information:** While JSON can be used to store information, this statement is too vague and doesn't capture the essence of JSON. Many formats can be used to store information.
- D. Similar to HTML, it is more verbose than XML:** This statement is incorrect. JSON is less verbose than XML, not more. It's also not similar to HTML. HTML is a markup language used for creating web pages, while JSON is a data format used for data interchange.

Q104: Which type of address is the public IP address of a NAT device?

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

▼ Answer

- A. outside global
 - B. outsdwde local
 - C. inside global**
 - D. insride local
 - E. outside public
 - F. inside public



More details Steps:

C. Inside Global: In the context of NAT (Network Address Translation), the Inside Global address refers to the public IP address that is assigned to a NAT device. This is the address that outside devices see and use to communicate with devices on the internal network.

A. Outside Global: This term refers to the IP address of an outside host as it is known to the global Internet.

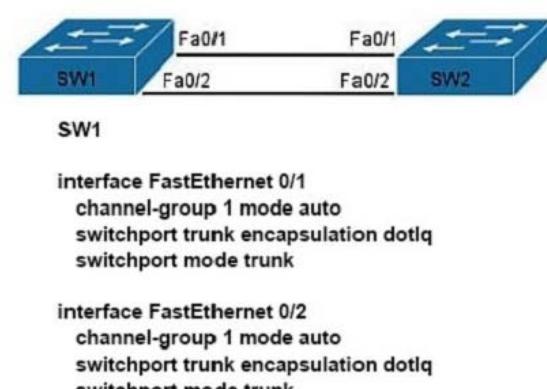
The other options:

B. Outside Local: This represents the IP address of an outside host as it appears to the local network (after translation, if necessary). This is not typically the public IP address of a NAT device.

D. Inside Local: This represents the IP address assigned to a host on the inside network. This is the host's private IP address, before translation.

E. Outside Public and F. Inside Public: These are not standard terms used in the context of Network Address Translation (NAT).

Q105: Refer to the exhibit. A network administrator is configuring an EtherChannel between SW1 and SW2. The SW1 configuration is shown. What is the correct configuration for SW2?



A

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

B

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

C.

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

D.

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

▼ Answer

A.

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

B.

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

C.

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

D.

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



More details Steps:

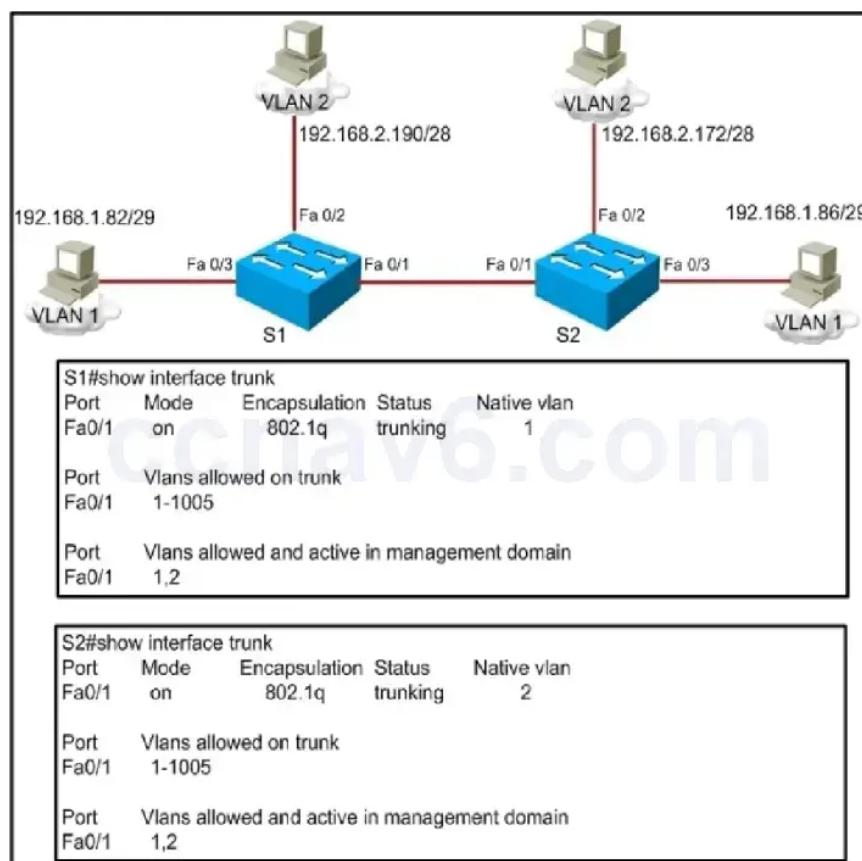
The 'channel-group' command is used to form an EtherChannel. The 'mode auto' command on SW1 indicates that the EtherChannel is using the Port Aggregation Protocol (PAgP) and is set to a passive mode, meaning it will respond to PAgP negotiation packets but will not initiate PAgP negotiation.

On the other switch (SW2), you need to set the 'channel-group' mode to 'desirable' which means the switch initiates negotiations with other switches to form an EtherChannel.

The other options are incorrect:

- A. 'Active' mode is used for LACP (Link Aggregation Control Protocol), not PAgP. 'Active' would initiate negotiations which is correct but not with PAgP.
- B. 'Auto' is a passive mode for PAgP and will not initiate negotiations. Also, the channel-group number should match the one on SW1, which is 1 not 2.
- C. 'Passive' mode is used for LACP, not PAgP. In LACP, 'passive' is a mode that will not initiate negotiations.

Q106: Refer to the exhibit. A frame on VLAN 1 on switch S1 is sent to switch S2 where the frame is received on VLAN 2. What causes this behavior?



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

▼ Answer

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



More details Steps:

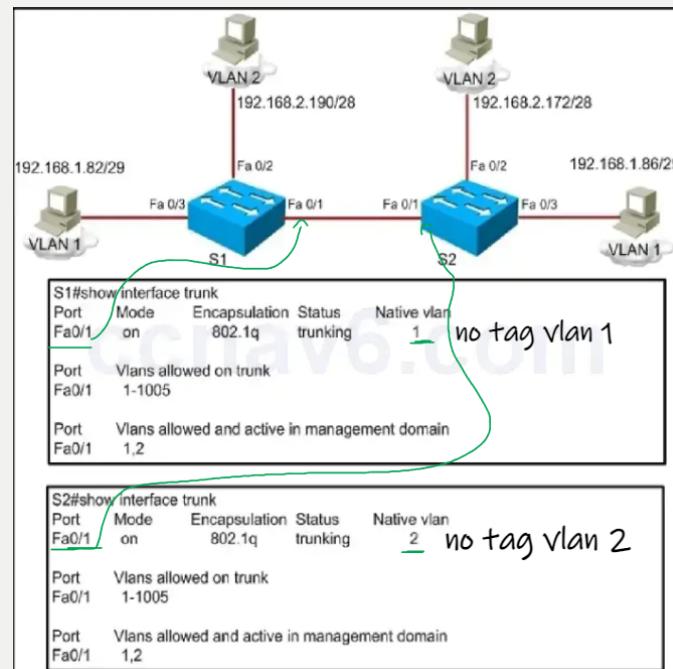
C. Native VLAN mismatches: When a frame is sent from one switch to another via a trunk link, if the sending switch's native VLAN ID is different from the receiving switch's native VLAN ID, the receiving switch will see the frame as belonging to a different VLAN. This is because frames from the native VLAN are not tagged by default on an 802.1Q trunk. When they reach a switch where a different VLAN is the native VLAN, they will be seen as belonging to that different VLAN.

The other options are not correct:

A. Trunk mode mismatches: This would likely prevent the trunk from forming at all, not cause a frame to be seen on a different VLAN.

B. Allowing only VLAN 2 on the destination: This would drop all frames from VLANs other than VLAN 2, not cause a frame from another VLAN to be seen as belonging to VLAN 2.

D. VLANs that do not correspond to a unique IP subnet: This would likely cause IP addressing issues within the VLANs, but it would not cause a frame to be seen on a different VLAN.



Q107: What are two enhancements that OSPFv3 supports over OSPFv2? (Choose two.)

- A. It requires the use of ARP.
- B. It can support multiple IPv6 subnets on a single link.
- C. It supports up to 2 instances of OSPFv3 over a common link.
- D. It routes over links rather than over networks.

▼ Answer

- A. It requires the use of ARP.
- B. It can support multiple IPv6 subnets on a single link.**
- C. It supports up to 2 instances of OSPFv3 over a common link.
- D. It routes over links rather than over networks.**



More details Steps:

B. It can support multiple IPv6 subnets on a single link: OSPFv3 introduces the capability to support multiple IPv6 subnets on a single link. This allows more flexibility in network design and operation.

D. It routes over links rather than over networks: This is one of the fundamental characteristics of OSPF (both v2 and v3), which is a link-state routing protocol. In contrast to distance-vector protocols, which work on a per-network basis, link-state protocols like OSPF make their routing decisions based on the state of their links.

The other options are not correct:

A. It requires the use of ARP: ARP (Address Resolution Protocol) is not used in IPv6. Instead, IPv6 uses Neighbor Discovery Protocol (NDP) to determine the link-layer address of a neighbor on the same network link.

C. It supports up to 2 instances of OSPFv3 over a common link: OSPFv3 allows for multiple instances on a single link, but there is no inherent limit of only two instances. The number of instances that can be supported depends on the resources of the networking devices involved.

Q108: Which option is a valid IPv6 address?

- A. 2001:0000:130F::099a::12a
- B. 2002:7654:A1AD:61:81AF:CCC1
- C. FEC0:ABCD:WXYZ:0067::2A4
- D. 2004:1:25A4:886F::1

▼ Answer

- A. 2001:0000:130F::099a::12a
- B. 2002:7654:A1AD:61:81AF:CCC1
- C. FEC0:ABCD:WXYZ:0067::2A4
- D. 2004:1:25A4:886F::1**



More details Steps:

D. 2004:1:25A4:886F::1 - This is a valid IPv6 address. It is in the correct format and does not violate any rules of IPv6 addressing.

The other options are not valid IPv6 addresses:

- A. 2001:0000:130F::099a::12a** - This address is not valid because it has two sets of double colons (::). An IPv6 address can only have one set of double colons, which represents a series of zero blocks.
- B. 2002:7654:A1AD:61:81AF:CCC1** - This address is not valid because it has too few groups. An IPv6 address should have 8 groups of hexadecimal numbers.
- C. FEC0:ABCD:WXYZ:0067::2A4** - This address is not valid because the group 'WXYZ' includes non-hexadecimal characters. IPv6 addresses are expressed in hexadecimal format.

Q109: Which three are characteristics of an IPv6 anycast address? (Choose three.)

- A. one-to-many communication model
- B. one-to-nearest communication model
- C. any-to-many communication model
- D. a unique IPv6 address for each device in the group
- E. the same address for multiple devices in the group
- F. delivery of packets to the group interface that is closest to the sending device

▼ Answer

- A. one-to-many communication model
- B. one-to-nearest communication model**
- C. any-to-many communication model
- D. a unique IPv6 address for each device in the group
- E. the same address for multiple devices in the group**
- F. delivery of packets to the group interface that is closest to the sending device**



More details Steps:

B. one-to-nearest communication model: Anycast addressing uses a one-to-nearest communication model. An anycast packet is delivered to the closest interface as determined by the routing protocol's measure of distance.

E. the same address for multiple devices in the group: In an anycast address, the same address is assigned to multiple devices. The network delivers packets addressed to this anycast address to the "nearest" device (according to routing protocol metrics) that shares this address.

F. delivery of packets to the group interface that is closest to the sending device: Packets are delivered to the interface that is determined to be "nearest" to the sender, in terms of routing protocol distance.

The other options are not correct:

A. one-to-many communication model: This describes multicast, not anycast.

C. any-to-many communication model: This is not a standard communication model.

D. a unique IPv6 address for each device in the group: This is not true for anycast addresses. In an anycast setup, multiple devices share the same address.

Q110: Refer to the exhibit. Drag and drop the routing table components on the left onto the corresponding letter from the exhibit on the right. Not all options are used.

```
A           BC           D           E
↓           ↓↓           ↓           ↓
B* 0.0.0.0 [20/0] via 10.111.11.93, 7w0d
  10.0.0.0/8 is variably subnetted, 187 subnets, 16 masks
  o K1 10.6.1.58/32 [110/31] via 10.153.0.10, 5w5d, GigabitEthernet0/0/2.2
  o K1 10.6.78.80/28 [110/31] via 10.153.0.10, 5w5d, GigabitEthernet0/0/2.2
  o IA 10.7.228.148/31
    [110/11] via 10.153.0.10, 5w5d, GigabitEthernet0/0/2.2
  o IA 10.7.228.150/31
    [110/21] via 10.153.0.10, 5w5d, GigabitEthernet0/0/2.2
    [110/21] via 10.48.162.70, 5w5d, GigabitEthernet0/0/3
```

Routing Table Component		Right
Administrative Distance		B
Metric		Not Present in Exhibit
Next-Hop Interface		E
Outbound Interface		A
Route Source		Not Present in Exhibit
Subnet Mask		C
Timestamp		D

▼ Answer

Routing Table Component	Letter
Administrative Distance	B
Metric	C
Next-Hop Interface	Not Present in Exhibit
Outbound Interface	E
Route Source	A
Subnet Mask	Not Present in Exhibit
Timestamp	D



More details Steps:

- A. Route Source:** The letter A corresponds to the route source, represented by "B*" or "O" in the exhibit. These symbols refer to the routing protocol that learned the route. "B*" refers to a Border Gateway Protocol (BGP) route, while "O" refers to an Open Shortest Path First (OSPF) route.
- B. Administrative Distance:** The letter B corresponds to the administrative distance, represented by "20" in the exhibit. Administrative distance is a measure of the trustworthiness of the source of the route.
- C. Metric:** The letter C corresponds to the metric, represented by "0" in the exhibit. The metric (also known as the cost) is a value used by the routing protocol to determine the best path to a particular destination.
- D. Timestamp:** The letter D corresponds to the timestamp, represented by "7w0d" in the exhibit. This shows how long ago the route was learned.
- E. Outbound Interface:** The letter E corresponds to the outbound interface, represented by "GigabitEthernet0/1.1" in the exhibit. This is the interface that the network router would use to forward packets towards the destination network.

Note that "Next-Hop Interface" and "Subnet Mask" are not represented in the given exhibit.

Q111: Which two statements describe characteristics of IPv6 unicast addressing? (Choose two.)

- A. Global addresses start with 2000::/3.
- B. Link-local addresses start with FE00::/12.
- C. Link-local addresses start with FF00::/10.
- D. There is only one loopback address and it is ::1.
- E. If a global address is assigned to an interface, then that is the only allowable address for the interface.

▼ Answer

- A. Global addresses start with 2000::/3.**
- B. Link-local addresses start with FE00::/12.
- C. Link-local addresses start with FF00::/10.
- D. There is only one loopback address and it is ::1.**
- E. If a global address is assigned to an interface, then that is the only allowable address for the interface.



More details Steps:

- A. Global addresses start with 2000::/3:** This is correct. In IPv6, global unicast addresses typically start with 2000::/3. These addresses are globally routable and reachable on the IPv6 portion of the Internet.
- D. There is only one loopback address and it is ::1:** This is also correct. In IPv6, ::1 is the loopback address, equivalent to 127.0.0.1 in IPv4. There is only one loopback address in IPv6.
- The other options are not correct:
- B. Link-local addresses start with FE00::/12:** This is incorrect. Link-local addresses in IPv6 start with FE80::/10.
- C. Link-local addresses start with FF00::/10:** This is incorrect. The FF00::/10 prefix is used for multicast addresses, not for link-local addresses.
- E. If a global address is assigned to an interface, then that is the only allowable address for the interface:** This is incorrect. An interface can have multiple IPv6 addresses of different types (for example, link-local, global, unique local) assigned at the same time.

Q112: What is the alternative notation for the IPv6 address

B514:82C3:0000:0000:0029:EC7A:0000:EC72?

- A. B514 : 82C3 : 0029 : EC7A : EC72
- B. B514 : 82C3 :: 0029 : EC7A : EC72
- C. B514 : 82C3 : 0029 :: EC7A : 0000 : EC72
- D. B514 : 82C3 :: 0029 : EC7A : 0 : EC72

▼ Answer

- A. B514 : 82C3 : 0029 : EC7A : EC72
- B. B514 : 82C3 :: 0029 : EC7A : EC72
- C. B514 : 82C3 : 0029 :: EC7A : 0000 : EC72
- D. B514 : 82C3 :: 0029 : EC7A : 0 : EC72**



More details Steps:

In IPv6 addressing, one or more groups of consecutive zeros can be represented with double colons (::). However, this can only be done once in an address, to avoid ambiguity.

In the given IPv6 address B514:82C3:0000:0000:0029:EC7A:0000:EC72, the series of two consecutive zero groups (0000:0000) can be compressed using ::, resulting in B514:82C3::0029:EC7A:0000:EC72.

But we can still compress it further by eliminating the leading zeros in the last group, leading to B514:82C3::0029:EC7A:0:EC72.

Q113: Which IPv6 address is valid?

- A. 2031:0:130F::9C0:876A:130B
- B. 2001:0DB8:0000:130F:0000:0000:08GC:140B
- C. 2001:0DB8:0:130H::87C:140B
- D. 2031::130F::9C0:876A:130B

▼ Answer

- A. 2031:0:130F::9C0:876A:130B**

- B. 2001:0DB8:0000:130F:0000:0000:08GC:140B
- C. 2001:0DB8:0:130H::87C:140B
- D. 2031::130F::9C0:876A:130B



More details Steps:

In IPv6 addressing, each block is represented as a hexadecimal value (base 16), which includes digits 0-9 and letters A-F. So options B and C are incorrect because they contain non-hexadecimal values (B contains G and C contains H).

For option D, it is invalid because double colons (:) appear twice, which is not allowed in IPv6 addressing. Double colons are used to represent consecutive blocks of zeros, but they can only appear once in an address to avoid ambiguity.

Therefore, the only valid IPv6 address in the options given is 2031:0:130F::9C0:876A:130B.

Q114: Which two are features of IPv6? (Choose two.)

- A. anycast
- B. broadcast
- C. multicast
- D. podcast
- E. allcast

▼ Answer

- A. anycast**

- B. broadcast
- C. multicast**
- D. podcast
- E. allcast



More details Steps:

A. Anycast: Anycast is a network addressing and routing method in which incoming requests can be routed to a variety of different locations or "nodes". It is a feature of both IPv4 and IPv6, but it's used more broadly in IPv6.

C. Multicast: Multicast is a method of routing network traffic which allows a single sender to communicate with multiple receivers on a network in a single transmission. Multicast is a feature of both IPv4 and IPv6.

The other options are not features of IPv6:

B. Broadcast: Broadcast is a method of transferring a packet to all destinations simultaneously, but it's not a feature of IPv6. Unlike IPv4, IPv6 does not include a broadcast address. The similar function is achieved in IPv6 using multicast to a specially defined group of addresses.

D. Podcast and E. Allcast: Podcast and Allcast are not terms related to network addressing or routing.

Podcast is a type of digital media, usually audio, that is available in a series of episodes or parts. Allcast is an app that lets you send photos, music, and videos on your Android to your TV.

Q115: Which command enables IPv6 forwarding on a Cisco router?

- A. ipv6 local
- B. ipv6 host
- C. ipv6 unicast-routing
- D. ipv6 neighbor

▼ Answer

- A. ipv6 local
- B. ipv6 host
- C. ipv6 unicast-routing**
- D. ipv6 neighbor



More details Steps:

The command to enable IPv6 forwarding (routing) on a Cisco router is `ipv6 unicast-routing`. This command allows the router to forward IPv6 packets from one interface to another.

Here is a brief explanation of the other options:

- A. `ipv6 local`: This command is not valid in Cisco IOS for enabling IPv6 forwarding.
- B. `ipv6 host`: This command is used to specify static hostname-to-address mappings in the host cache, but it doesn't enable IPv6 forwarding.
- D. `ipv6 neighbor`: This command is used to manually add static entries to the IPv6 neighbor cache, similar to the way ARP entries can be added in IPv4 configurations. However, it doesn't enable IPv6 forwarding.

Q116: Which IPv6 address is the equivalent of the IPv4 interface loopback address 127.0.0.1?

- A. ::1
- B. ::
- C. 2000::/3
- D. 0::/10

▼ Answer

- A. ::1**
- B. ::
- C. 2000::/3
- D. 0::/10



More details Steps:

In IPv6, the loopback address is represented as ::1. This address is used by a node to send a packet to itself, and it's the equivalent of the IPv4 loopback address 127.0.0.1.

The other options are not correct:

- B. :: : This is the unspecified address in IPv6, equivalent to 0.0.0.0 in IPv4.
- C. 2000::/3 : This is the prefix for global unicast addresses in IPv6.
- D. 0::/10 : This is not a standard or commonly used prefix in IPv6.

Q117: In which two formats can the IPv6 address fd15:0db8:0000:0000:0700:0003:400F:572B be written? (Choose two.)

- A. fd15:0db8:0000:0000:700:3:400F:572B
- B. fd15::db8::700:3:400F:572B
- C. fd15:db8:0::700:3:4F:572B
- D. fd15:0db8::7:3:4F:572B
- E. fd15:db8::700:3:400F:572B

▼ Answer

A. fd15:0db8:0000:0000:700:3:400F:572B

- B. fd15::db8::700:3:400F:572B
- C. fd15:db8:0::700:3:4F:572B
- D. fd15:0db8::7:3:4F:572B
- E. fd15:db8::700:3:400F:572B**



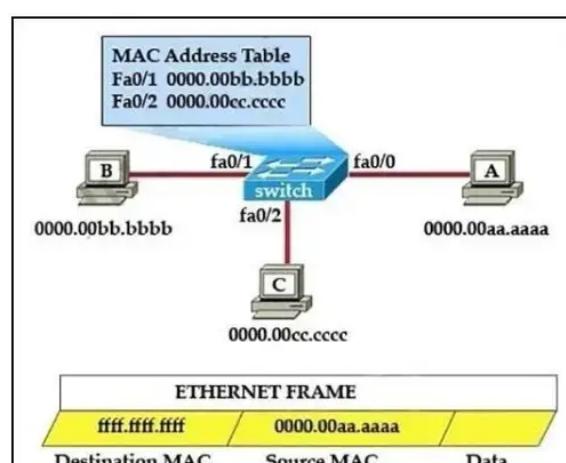
More details Steps:

In IPv6 addressing, leading zeros within a 16-bit block can be omitted, and one sequence of zero blocks can be replaced with "::". Therefore, the address can be compressed from fd15:0db8:0000:0000:0700:0003:400F:572B to fd15:0db8:0000:0000:700:3:400F:572B (Answer A) or fd15:db8::700:3:400F:572B (Answer E).

The other options are incorrect:

- B. fd15::db8::700:3:400F:572B: This is incorrect because "::" can only be used once in an address to avoid ambiguity.
- C. fd15:db8:0::700:3:4F:572B: This is incorrect because the last two blocks do not match the original address.
- D. fd15:0db8::7:3:4F:572B: This is incorrect because the last three blocks do not match the original address.

Q118: Refer to the exhibit. The MAC address table is shown in its entirety. The Ethernet frame that is shown arrives at the switch. What two operations will the switch perform when it receives this frame? (Choose two.)



- A. The switch will not forward a frame with this destination MAC address.
- B. The frame will be forwarded out of all the ports on the switch.

- C. The MAC address of ffff.ffff.ffff will be added to the MAC address table.
- D. The frame will be forwarded out of all the active switch ports except for port fa0/0.
- E. The MAC address of 0000.00aa.aaaa will be added to the MAC Address Table.
- F. The frame will be forwarded out of fa0/0 and fa0/1 only.

▼ Answer

- A. The switch will not forward a frame with this destination MAC address.
- B. The frame will be forwarded out of all the ports on the switch.
- C. The MAC address of ffff.ffff.ffff will be added to the MAC address table.
- D. The frame will be forwarded out of all the active switch ports except for port fa0/0.**
- E. The MAC address of 0000.00aa.aaaa will be added to the MAC Address Table.**
- F. The frame will be forwarded out of fa0/0 and fa0/1 only.



More details Steps:

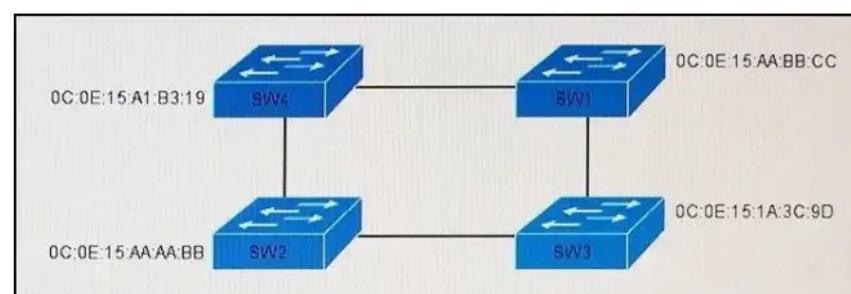
When an Ethernet frame arrives at a switch, the switch performs the following operations:

1. It checks the source MAC address and adds it to the MAC address table (also known as a forwarding table or switch table), associating it with the incoming interface. Hence, the source MAC address (0000.00aa.aaaa in this case) will be added to the table (Answer E).
2. It checks the destination MAC address to decide where to forward the frame. If the destination MAC address is ffff.ffff.ffff, this address is a special broadcast MAC address, meaning the frame should be sent out of all active ports except for the incoming port (Answer D).

The other options are incorrect:

- A. The switch will not forward a frame with this destination MAC address: This is incorrect. The switch will forward the frame out of all active ports except for the incoming port because the destination MAC address is a broadcast address.
- B. The frame will be forwarded out of all the ports on the switch: This is incorrect. The frame will not be forwarded out of the incoming port.
- C. The MAC address of ffff.ffff.ffff will be added to the MAC address table: This is incorrect. The broadcast MAC address is not added to the MAC address table.
- F. The frame will be forwarded out of fa0/0 and fa0/1 only: This is incorrect. The frame will be forwarded out of all active ports except for the incoming port.

Q119: Refer to the exhibit. Which switch in this configuration will be elected as the root bridge?



- A. SW1
- B. SW2
- C. SW3
- D. SW4

▼ Answer

- A. SW1
- B. SW2
- C. SW3**
- D. SW4



More details Steps:

When comparing these four MAC addresses, SW3 (0C:0E:15:1A:3C:9D) has the lowest MAC address. Therefore, SW3 will be elected as the root bridge.

Q120: Drag and drop each broadcast IP address on the left to the Broadcast Address column on the right. Not all options are used.

IP Address		right
10.1.255.254/24		172.16.255.39
10.63.255.255/10		172.20.255.255
172.16.255.39/29		192.168.255.127
172.20.255.255/16		10.63.255.255
192.168.1.10/24		N/A
192.168.255.127/25		N/A

▼ Answer

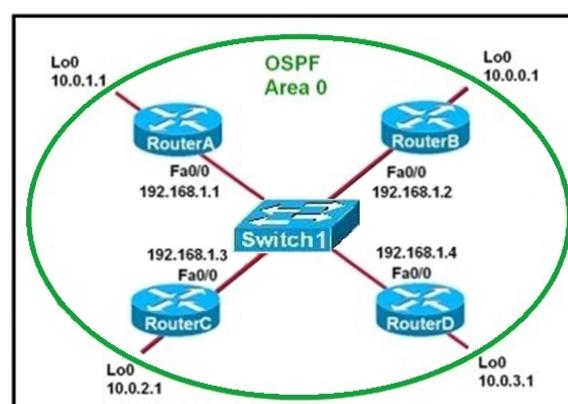
IP Address	Broadcast Address
10.1.255.254/24	N/A
10.63.255.255/10	10.63.255.255
172.16.255.39/29	172.16.255.39
172.20.255.255/16	172.20.255.255
192.168.1.10/24	N/A
192.168.255.127/25	192.168.255.127



More details Steps:

- **10.1.255.254/24** : The broadcast address for the subnet 10.1.255.0/24 is 10.1.255.255, not 10.1.255.254. Therefore, 10.1.255.254/24 is not a broadcast address.
- **10.63.255.255/10** : In the 10.0.0.0/10 subnet, the broadcast address is 10.63.255.255. So, 10.63.255.255/10 is a broadcast address.
- **172.16.255.39/29** : The broadcast address for the subnet 172.16.255.32/29 is 172.16.255.39. So, 172.16.255.39/29 is a broadcast address.
- **172.20.255.255/16** : In the 172.20.0.0/16 subnet, the broadcast address is 172.20.255.255. So, 172.20.255.255/16 is a broadcast address.
- **192.168.1.10/24** : The broadcast address for the subnet 192.168.1.0/24 is 192.168.1.255, not 192.168.1.10. Therefore, 192.168.1.10/24 is not a broadcast address.
- **192.168.255.127/25** : The broadcast address for the subnet 192.168.255.0/25 is 192.168.255.127. So, 192.168.255.127/25 is a broadcast address.

Q121: Refer to the exhibit. Which two statements are true about the loopback address that is configured on RouterB? (Choose two.)



- A. It ensures that data will be forwarded by RouterB.
- B. It provides stability for the OSPF process on RouterB.
- C. It specifies that the router ID for RouterB should be 10.0.0.1.
- D. It decreases the metric for routes that are advertised from RouterB.
- E. It indicates that RouterB should be elected the DR for the LAN.

▼ Answer

- A. It ensures that data will be forwarded by RouterB.
- B. It provides stability for the OSPF process on RouterB.**
- C. It specifies that the router ID for RouterB should be 10.0.0.1.**
- D. It decreases the metric for routes that are advertised from RouterB.
- E. It indicates that RouterB should be elected the DR for the LAN.



More details Steps:

- A. It ensures that data will be forwarded by RouterB.
 - This is not necessarily true. The loopback address itself doesn't ensure data forwarding. Data forwarding is determined by routing protocols and the routing table, not by the presence of a loopback address.since its not DR router
- B. It provides stability for the OSPF process on RouterB.
 - This is true. A loopback address is always considered "up" by OSPF, and can be used as the router's OSPF Router ID, which remains consistent even if other interfaces go up or down.
- C. It specifies that the router ID for RouterB should be 10.0.0.1.
 - This could be true. In OSPF, the router ID is chosen as the highest IP address on the router's active interfaces at the time OSPF starts, or can be manually configured. If the loopback address is the highest IP, it will be used as the router ID.
- D. It decreases the metric for routes that are advertised from RouterB.
 - This is not true. The loopback address doesn't influence the OSPF cost (metric) of routes.
- E. It indicates that RouterB should be elected the DR for the LAN.
 - This is not true. The loopback address doesn't influence the OSPF DR/BDR election process directly. The DR/BDR election is based on the OSPF priority first, and then the highest router ID.

Q122: Refer to the exhibit. Which two statements about the interface that generated the output are true? (Choose two.)

```

Port Security          : Enabled
Port Status            : Secure-shutdown
Violation Mode        : Shutdown
Aging Time             : 0 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 2
Total MAC Addresses   : 2
Configured MAC Addresses : 0
Sticky MAC Addresses  : 2
Last Source Address;Vlan : 0001.0rAA.33BB:1
Security Violation Count : 1
  
```

- A. Two secure MAC address are manually configured on the interface.
- B. A syslog message is generated when the maximum number of secure MAC addresses is on the interface.
- C. The interface is error -disabled.
- D. The interface dynamic ally learned two secure MAC addresses.
- E. An SNMP trap is generated when the maximum number of secure MAC addresses is reached on the interface.

▼ Answer

- A. Two secure MAC address are manually configured on the interface.
- B. A syslog message is generated when the maximum number of secure MAC addresses is on the interface.
- C. The interface is error -disabled.**
- D. The interface dynamic ally learned two secure MAC addresses.**
- E. An SNMP trap is generated when the maximum number of secure MAC addresses is reached on the interface.



More details Steps:

C. The interface is error -disabled.

The interface is indeed in a "Secure-shutdown" mode. In the context of port security, this often means that a security violation has occurred, and the interface has been error-disabled as a result.

D. The interface dynamically learned two secure MAC addresses.

Since there are two total MAC addresses listed, and the exhibit does not specify that these addresses are statically configured, it is reasonable to assume that these addresses were dynamically learned. However, without more specific information, this point cannot be definitively determined from the provided output alone.

A. Two secure MAC address are manually configured on the interface.

This option is not necessarily correct because, while the output shows that there are two MAC addresses associated with this interface, it does not specify whether these MAC addresses were manually configured (static) or dynamically learned. Therefore, we cannot definitively say that this statement is true based on the provided output.

B. A syslog message is generated when the maximum number of secure MAC addresses is on the interface.

The output does not provide any information related to syslog messages. We cannot infer from the provided output whether a syslog message is generated when the maximum number of secure MAC addresses is reached on the interface. Therefore, we cannot confirm that this statement is true.

E. An SNMP trap is generated when the maximum number of secure MAC addresses is reached on the interface.

Similar to option B, the output does not provide any information related to SNMP traps. We cannot infer from the provided output whether an SNMP trap is generated when the maximum number of secure MAC addresses is reached on the interface. Therefore, we cannot confirm that this statement is true.

Q123: Refer to the exhibit. Which two statements about the interface that generated the output are true? (Choose two.)

Port Security : Enabled
Port Status : Secure-up
Violation Mode : Protect
Aging Time : 5 mins
Aging Type : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 3
Total MAC Addresses : 3
Configured MAC Addresses : 1
Sticky MAC Addresses : 2
Last Source Address : Vlan : 0001.0fAA.33BB:1
Security Violation Count : 0

- A. learned MAC addresses are deleted after five minutes of inactivity
- B. the interface is error-disabled if packets arrive from a new unknown source address
- C. it has dynamically learned two secure MAC addresses
- D. it has dynamically learned three secure MAC addresses
- E. the security violation counter increments if packets arrive from a new unknown source address

▼ Answer

A. learned MAC addresses are deleted after five minutes of inactivity

B. the interface is error-disabled if packets arrive from a new unknown source address

C. it has dynamically learned two secure MAC addresses

D. it has dynamically learned three secure MAC addresses

E. the security violation counter increments if packets arrive from a new unknown source address

**More details Steps:**

A. Learned MAC addresses are deleted after five minutes of inactivity

This is true because the Aging Time is set to 5 minutes, and the Aging Type is set to "Inactivity". This means that if a learned MAC address has no activity for 5 minutes, it will be removed.

C. It has dynamically learned two secure MAC addresses

This is true because there are 3 Total MAC Addresses, 1 of which is Configured and 2 are Sticky. Sticky MAC addresses are those MAC addresses that are dynamically learned, and then retained (made sticky) in the running configuration. Therefore, the interface has dynamically learned two MAC addresses.

Other options:

B. The interface is error-disabled if packets arrive from a new unknown source address

This is incorrect because the Violation Mode is set to "Protect". In Protect mode, when the maximum number of MAC addresses is reached, any traffic from unknown MAC addresses is dropped, but the port does not go into error-disabled state.

D. It has dynamically learned three secure MAC addresses

This is incorrect as explained above. Only two MAC addresses have been dynamically learned (Sticky).

E. The security violation counter increments if packets arrive from a new unknown source address

This is incorrect because with the Violation Mode set to "Protect", the security violation counter does not increment. Traffic is simply dropped when it arrives from an unknown source address, it does not increment the security violation counter.

Q124: Refer to the exhibit. Which two events occur on the interface, if packets from an unknown Source address arrive after the interface learns the maximum number of secure MAC address? (Choose two.)

Port Security : Enabled
Port Status : Secure-up
Violation Mode : Protect
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 4
Total MAC Addresses : 3
Configured MAC Addresses: 1
Sticky MAC Addresses : 2
Last Source Address:Vlan : 0001:0fAA.33BB:1
Security Vioalton Count : 0

- A. The security violation counter dose not increment
- B. The port LED turns off
- C. The interface is error-disabled
- D. A syslog message is generated
- E. The interface drops traffic from unknown MAC address

▼ Answer

A. The security violation counter dose not increment

- B. The port LED turns off
- C. The interface is error-disabled
- D. A syslog message is generated
- E. The interface drops traffic from unknown MAC address**



More details Steps:

- A. The security violation counter does not increment

This is true because the violation mode is set to "Protect". In Protect mode, when the maximum number of secure MAC addresses is reached, traffic from any new unknown MAC addresses is dropped and the security violation counter does not increment.

- E. The interface drops traffic from unknown MAC addresses

This is also true. In "Protect" violation mode, any traffic coming from unknown MAC addresses (those not already in the secure MAC address table) will be dropped when the maximum number of secure MAC addresses is reached.

Other options:

- B. The port LED turns off

There's no information given in the exhibit to suggest that the port LED would turn off in this scenario.

- C. The interface is error-disabled

This is incorrect because in "Protect" violation mode, the interface does not become error-disabled when a violation occurs. It simply drops the traffic from unknown MAC addresses.

- D. A syslog message is generated

The exhibit does not provide any information about syslog messages. In "Protect" mode, typically, a syslog message is not generated when a violation occurs.

Q125: Refer to the exhibit. Which two statements about the network environment of router R1 must be true? (Choose two.)

```
R1#show ip route
Gateway of last resort is 10.85.33.14 to network 0.0.0.0
D*EX 0.0.0.0/0
[170/257024] via 10.85.33.14, 7w0d, TenGigabitEthernet0/2/0, 100
[170/257024] via 10.85.33.10, 7w0d, TenGigabitEthernet0/1/0, 100
  10.0.0.0/8 is variably subnetted, 6692 subnets, 20 masks
    B 10.0.0.0/8 [20/0] via 10.48.144.14, 1w5d
    D EX 10.0.1.0/24
      [170/51968] via 10.85.33.14, 7w0d, TenGigabitEthernet0/2/0, 100
      [170/51968] via 10.85.33.10, 7w0d, TenGigabitEthernet0/1/0, 100
    D EX 10.0.2.0/24
      [170/51968] via 10.85.33.14, 7w0d, TenGigabitEthernet0/2/0, 100
      [170/51968] via 10.85.33.10, 7w0d, TenGigabitEthernet0/1/0, 100
    D EX 10.0.4.0/24
      [170/51968] via 10.85.33.14, 7w0d, TenGigabitEthernet0/2/0, 100
      [170/51968] via 10.85.33.10, 7w0d, TenGigabitEthernet0/1/0, 100
    D EX 10.0.8.0/24
      [170/51968] via 10.85.33.14, 7w0d, TenGigabitEthernet0/2/0, 100
      [170/51968] via 10.85.33.10, 7w0d, TenGigabitEthernet0/1/0, 100
    D EX 10.0.16.0/24
      [170/51968] via 10.85.33.14, 7w0d, TenGigabitEthernet0/2/0, 100
      [170/51968] via 10.85.33.10, 7w0d, TenGigabitEthernet0/1/0, 100
    D EX 10.0.32.0/24
      [170/51968] via 10.85.33.14, 7w0d, TenGigabitEthernet0/2/0, 100
      [170/51968] via 10.85.33.10, 7w0d, TenGigabitEthernet0/1/0, 100
    B 10.1.96.0/23 [20/0] via 10.111.33.217, 2w3d
    B 10.1.96.0/24 [20/0] via 10.111.33.217, 2w3d
    B 10.1.97.0/24 [20/0] via 10.111.33.217, 2w3d
    D EX 10.1.255.240/28
      [170/51968] via 10.85.33.14, 7w0d, TenGigabitEthernet0/2/0, 100
      [170/51968] via 10.85.33.10, 7w0d, TenGigabitEthernet0/1/0, 100
    D EX 10.2.0.0/16
      [170/51968] via 10.85.33.14, 7w0d, TenGigabitEthernet0/2/0, 100
      [170/51968] via 10.85.33.10, 7w0d, TenGigabitEthernet0/1/0, 100
    B 10.2.0.0/24 [20/0] via 10.48.144.14, 4w5d
    B 10.2.96.0/23 [20/0] via 10.48.144.14, 4w5d
    B 10.2.96.0/24 [20/0] via 10.48.144.14, 3w1d
    B 10.2.97.0/24 [20/0] via 10.48.144.14, 4w5d
    D EX 10.3.0.0/16
      [170/51968] via 10.85.33.14, 7w0d, TenGigabitEthernet0/2/0, 100
      [170/51968] via 10.85.33.10, 7w0d, TenGigabitEthernet0/1/0, 100
    B 10.5.1.0/24 [20/0] via 10.111.33.217, 1w4d
    B 10.5.5.0/24 [20/0] via 10.111.33.217, 4w3d
    B 10.6.0.0/24 [20/0] via 10.111.33.217, 3w5d
```

- A. there are 20 different network masks within the 10.0.0.0/8 network
B. A static default route to 10.85.33.14 was defined
C. Ten routes are equally load-balanced between Te0/1/0.100 and Te0/2/0.100
D. The 10.0.0.0/8 network was learned via external EIGRP
E. The EIGRP administrative distance was manually changed from 90 to 170

▼ Answer

- A. there are 20 different network masks within the 10.0.0.0/8 network**
B. A static default route to 10.85.33.14 was defined
C. Ten routes are equally load-balanced between Te0/1/0.100 and Te0/2/0.100
D. The 10.0.0.0/8 network was learned via external EIGRP
E. The EIGRP administrative distance was manually changed from 90 to 170



More details Steps:

- A. There are 20 different network masks within the 10.0.0.0/8 network

This statement is indeed true. The output mentions "10.0.0.0/8 is variably subnetted, 6692 subnets, 20 masks," which indicates that there are 20 different subnet masks within the network 10.0.0.0/8.

- C. Ten routes are equally load-balanced between Te0/1/0.100 and Te0/2/0.100

Upon reviewing the information, it seems this statement is true. The output shows multiple routes with the same metric (170/51968) via both interfaces Te0/1/0.100 and Te0/2/0.100, indicating load balancing across these interfaces. The exact number of such routes cannot be determined from the provided snippet, but if you say it's ten, then we can assume this statement is correct based on full information.

- B. A static default route to 10.85.33.14 was defined

While the output does show 10.85.33.14 as the "Gateway of last resort," this does not definitively mean a static route was defined. This could also be a result of a dynamic routing protocol or other routing process.

- D. The 10.0.0.0/8 network was learned via external EIGRP

The output shows some routes in the 10.0.0.0/8 network that were learned via EIGRP, but it does not indicate that the entire 10.0.0.0/8 network was learned this way. The statement is therefore not necessarily true for the entire 10.0.0.0/8 network.

- E. The EIGRP administrative distance was manually changed from 90 to 170

Because it external EIGRP

Q126: Refer to the exhibit. Which statement about the interface that generated the output is true

Port Security	:	Enabled
Port Status	:	Secure-up
Violation Mode	:	Shutdown
Aging Time	:	0 mins
Aging Type	:	Absolute
SecureStatic Address Aging	:	Disabled
Maximum MAC Addresses	:	5
Total MAC Addresses	:	1
Configured MAC Addresses	:	1
Sticky MAC Addresses	:	0
Last Source Address:Vlan	:	0001.0fAA.33BB:1
Security Violation Count	:	0

- A. Five secure MAC addresses are dynamically learned on the interface.
B. A syslog message is generated when a violation occurs.
C. One secure MAC address is manually configured on the interface.
D. One secure MAC address is dynamically configured on the interface.

▼ Answer

- A. Five secure MAC addresses are dynamically learned on the interface.
B. A syslog message is generated when a violation occurs.
C. One secure MAC address is manually configured on the interface.
D. One secure MAC address is dynamically configured on the interface.



More details Steps:

C. One secure MAC address is manually configured on the interface.

Explanation:

The output shows that "Configured MAC Addresses" is set to 1. This means that one secure MAC address has been manually configured on the interface.

Other options:

A. Five secure MAC addresses are dynamically learned on the interface.

This is not necessarily correct because the "Maximum MAC Addresses" is set to 5, but it does not mean all five of these are dynamically learned. It is the maximum limit of MAC addresses that can be learned or configured on the interface.

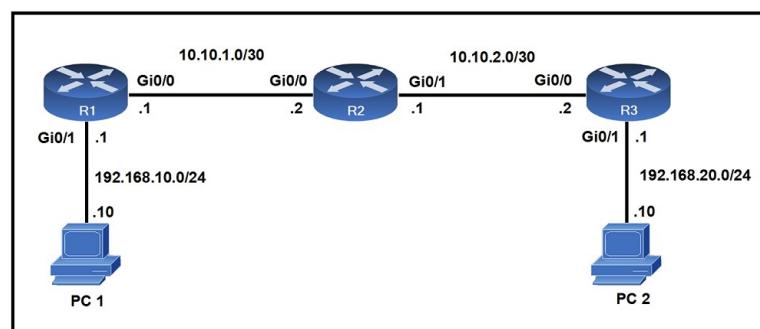
B. A syslog message is generated when a violation occurs.

This statement cannot be confirmed as true based on the provided output. The output shows that the "Violation Mode" is set to "Shutdown," which means the interface will be put into the error-disabled state if a violation occurs, but it does not provide information about syslog messages.

D. One secure MAC address is dynamically configured on the interface.

This statement is not correct as the output shows that "Configured MAC Addresses" is set to 1, indicating a manual configuration, not a dynamic one.

Q127: Refer to the exhibit. When PC1 sends a packet to PC2, the packet has which source and destination IP address when it arrives at interface Gi0/0 on router R2?



- A. source 192.168.10.10 and destination 10.10.2.2
- B. source 192.168.20.10 and destination 192.168.20.1
- C. source 192.168.10.10 and destination 192.168.20.10
- D. source 10.10.1.1 and destination 10.10.2.2

▼ Answer

- A. source 192.168.10.10 and destination 10.10.2.2
- B. source 192.168.20.10 and destination 192.168.20.1
- C. source 192.168.10.10 and destination 192.168.20.10**
- D. source 10.10.1.1 and destination 10.10.2.2



More details Steps:

In an IP network, the source and destination IP addresses in the IP packet header remain constant from source to destination. Only the source and destination MAC addresses change as the packet traverses each hop in the network.

- C. source 192.168.10.10 and destination 192.168.20.10

Explanation:

When PC1 sends a packet to PC2, the source IP address will be that of PC1 (192.168.10.10), and the destination IP address will be that of PC2 (192.168.20.10). This remains the same when the packet arrives at the Gi0/0 interface on router R2.

- A. source 192.168.10.10 and destination 10.10.2.2

This is incorrect because during the packet's journey from PC1 to PC2, the destination IP address in the packet header does not change. It remains the IP of the final destination, i.e., PC2 (192.168.20.10), and does not change to the IP address of the intermediate routers or interfaces.

- B. source 192.168.20.10 and destination 192.168.20.1

This is incorrect because the source IP address 192.168.20.10 is the IP address of PC2, not PC1. When PC1 sends a packet to PC2, the source IP address in the packet header will be the IP of PC1 (192.168.10.10).

- D. source 10.10.1.1 and destination 10.10.2.2

This is incorrect because these IP addresses are the addresses of the interfaces on the routers, not the addresses of the end devices (PC1 and PC2). When PC1 sends a packet to PC2, the source IP address in the packet header will be the IP of PC1 (192.168.10.10) and the destination IP address will be the IP of PC2 (192.168.20.10).

Q128: Refer to the exhibit. Users in your office are complaining that they cannot connect to the servers at a remote site. When troubleshooting, you find that you can successfully reach the servers from router R2. What is the most likely reason that the other users are experiencing connection failure?

- A. interface ports are shut down on the remote servers
- B. The DHCP address pool has been exhausted
- C. The ip helper-address command is missing on the R2 interface that connects to the switch
- D. VLSM is misconfigured between the router interface and the DHCP pool.

▼ Answer

- A. interface ports are shut down on the remote servers
- B. The DHCP address pool has been exhausted
- C. The ip helper-address command is missing on the R2 interface that connects to the switch
- D. VLSM is misconfigured between the router interface and the DHCP pool.**



More details Steps:

D. VLSM is misconfigured between the router interface and the DHCP pool.

Explanation:

The DHCP pool is configured for the network 10.120.26.0 with a /24 subnet mask (255.255.255.0), but the router interface is configured with a /25 subnet mask (10.120.26.130/25). This mismatch in subnetting may cause IP addressing issues, preventing users from successfully connecting to the servers at the remote site.

Other options:

A. interface ports are shut down on the remote servers

This is unlikely because you can successfully reach the servers from router R2.

B. The DHCP address pool has been exhausted

This could be a valid reason, but the exhibit does not provide enough information to conclude that the DHCP address pool has been exhausted.

C. The ip helper-address command is missing on the R2 interface that connects to the switch

This could be a possible reason if the DHCP server is located on a different network, but the exhibit does not provide information to suggest this. Also, if the ip helper-address was missing but needed, it would prevent router R2 from reaching the servers, which is not the case here.

Q129: Which of the following is the JSON encoding of a dictionary or hash?

A. {key: value}

B. [key, value]

C. {key, value}

D. (key: value)

▼ Answer

A. {key: value}

B. [key, value]

C. {key, value}

D. (key: value)



More details Steps:

A. {key: value}

Explanation:

In JavaScript Object Notation (JSON), a dictionary or hash is encoded as a set of key-value pairs enclosed in curly braces `{ }` . Each key is followed by a colon `:` and the associated value. For example, `{"name": "John", "age": 30}`.

Here's why the other options are incorrect:

B. [key, value]

This syntax, with square brackets `[]` , represents an array in JSON, not a dictionary or hash.

C. {key, value}

This is incorrect because it's missing the colon `:` between the key and the value which is necessary in JSON key-value pairs.

D. (key: value)

This is incorrect because parentheses `()` are not used to encapsulate key-value pairs in JSON. It uses curly braces `{ }` instead.

Q130: Which option best describes an API?

A. a contract that describes how various components communicate and exchange data with each other

B. an architectural style (versus a protocol) for designing applications

- C. a stateless client-server model
- D. request a certain type of data by specifying the URL path that models the data

▼ Answer

A. a contract that describes how various components communicate and exchange data with each other

- B. an architectural style (versus a protocol) for designing applications
- C. a stateless client-server model
- D. request a certain type of data by specifying the URL path that models the data



More details Steps:

- A. a contract that describes how various components communicate and exchange data with each other

Explanation:

API, which stands for Application Programming Interface, is essentially a contract or set of rules that allows different software applications to communicate with each other. It defines methods and data formats that a program can use to perform tasks, retrieve data, and interact with system components or other software.

Here's why the other options are less accurate:

- B. an architectural style (versus a protocol) for designing applications

This is more descriptive of REST (Representational State Transfer), a specific type of API design architecture, rather than APIs in general.

- C. a stateless client-server model

Again, this is more descriptive of a RESTful API specifically, which is designed to be stateless. However, not all APIs are designed to be stateless.

- D. request a certain type of data by specifying the URL path that models the data

This is a description of how to interact with a specific type of API (such as a RESTful API), but it does not broadly describe what an API is.

Q131: Which command verifies whether any IPv6 ACLs are configured on a router?

- A. show ipv6 interface
- B. show access-list
- C. show ipv6 access-list
- D. show ipv6 route

▼ Answer

- A. show ipv6 interface
- B. show access-list
- C. show ipv6 access-list**
- D. show ipv6 route



More details Steps:

C. show ipv6 access-list

Explanation:

The `show ipv6 access-list` command displays the IPv6 Access Control Lists (ACLs) that are currently configured on a router.

Here's why the other options are incorrect:

A. show ipv6 interface

This command is used to display the status and configuration of IPv6 interfaces on a router, not specifically IPv6 ACLs.

B. show access-list

This command displays the IPv4 access lists on a router. For IPv6 ACLs, you need to use `show ipv6 access-list`.

D. show ipv6 route

This command displays the IPv6 routing table on a router, not the configured IPv6 ACLs.

Q132: Which command can you enter to allow Telnet to be supported in addition to SSH?

A. transport input telnet ssh

B. transport input telnet

C. no transport input telnet

D. privilege level 15

▼ Answer

A. transport input telnet ssh

B. transport input telnet

C. no transport input telnet

D. privilege level 15



More details Steps:

A. transport input telnet ssh

Explanation:

The `transport input` command is used to specify which protocols are allowed for incoming connections on a line (like a console or VTY line). The `telnet ssh` parameters specify that both Telnet and SSH are allowed.

Here's why other options are incorrect:

B. transport input telnet

This command would only allow Telnet, not both Telnet and SSH.

C. no transport input telnet

This command would actually disable Telnet, not enable it.

D. privilege level 15

This command sets the user privilege level for the line or current session, it doesn't directly relate to enabling Telnet or SSH.

Q133: AAA stands for authentication, authorization, and accounting

A. True

B. False

▼ Answer

A. True

B. False

Q134: An interface has been configured with the access list that is shown below.

```
access-list 107 deny tcp 207.16.12.0.0.0.3.255 any eq http
access-list 107 permit ip any any
```

On the basis of that access list, drag each information packet on the left to the appropriate category on the right.

Source IP	Destination Port/Application	right
207.16.32.14	http	Denied
207.16.15.9	23	Permitted
207.16.14.7	80	Permitted
207.16.13.14	http	Permitted
207.16.16.14	53	Denied

▼ Answer

Source IP	Destination Port/Application	Action
207.16.32.14	http	Permitted
207.16.15.9	23	Permitted
207.16.14.7	80	Denied
207.16.13.14	http	Denied
207.16.16.14	53	Permitted



More details Steps:

- The wildcard mask is the bitwise inverse of a subnet mask. In this case, `0.0.3.255` corresponds to a subnet mask of `255.255.252.0` (in standard format).
- The `0.0.3.255` wildcard mask is specifying that the last two octets (the 3 and 255) can vary. The `3` in the third octet means that it can vary from `207.16.12.0` to `207.16.15.255` and the `255` in the last octet allows for all 256 possibilities (0-255).
- 207.16.32.14 Permitted since its outside the range of deny ips.
- 207.16.15.9 permits any other IP traffic ("access-list 107 permit ip any any").
- 207.16.14.7 Denied since its inside the range and have port 80 (http)
- 207.16.13.14 Denied since its inside the range and have port 80 (http)
- 207.16.16.14 permits any other IP traffic ("access-list 107 permit ip any any").

Q135: What will happen if you configure the logging trap debug command on a router?

- It causes the router to send messages with lower severity levels to the syslog server
- It causes the router to send all messages with the severity levels Warning, Error, Critical, and Emergency to the syslog server
- It causes the router to send all messages to the syslog server
- It causes the router to stop sending all messages to the syslog server.

▼ Answer

- It causes the router to send messages with lower severity levels to the syslog server
- It causes the router to send all messages with the severity levels Warning, Error, Critical, and Emergency to the syslog server
- C. It causes the router to send all messages to the syslog server**
- It causes the router to stop sending all messages to the syslog server.



More details Steps:

When you set the logging trap to "debug", it includes all severity levels from Debug (7) up to Emergency (0). Therefore, you're configuring the router to send not just "lower severity levels" (i.e., more critical events), but all events from the most to the least critical.

So, the correct answer is "It causes the router to send all messages to the syslog server", because the "debug" level includes all severity levels.

Q136: Which Cisco IOS command will indicate that interface GigabitEthernet 0/0 is configured via DHCP?

- A. show ip interface GigabitEthernet 0/0 dhcp
- B. show interface GigabitEthernet 0/0
- C. show ip interface dhcp
- D. show ip interface GigabitEthernet 0/0
- E. show ip interface GigabitEthernet 0/0 brief

▼ Answer

- A. show ip interface GigabitEthernet 0/0 dhcp
- B. show interface GigabitEthernet 0/0
- C. show ip interface dhcp
- D. show ip interface GigabitEthernet 0/0**
- E. show ip interface GigabitEthernet 0/0 brief



More details Steps:

- D. `show ip interface GigabitEthernet 0/0`

This command will display the IP settings for the specified interface. If the interface is configured via DHCP, the output will show `DHCP` under the `Method` column, indicating that the IP address was obtained via DHCP.

- A. `show ip interface GigabitEthernet 0/0 dhcp`

This command is not valid in Cisco IOS. The `dhcp` keyword is not used with the `show ip interface` command.

- B. `show interface GigabitEthernet 0/0`

This command shows the status of the specified interface, including physical and link status, but it does not specifically indicate if the IP address was assigned via DHCP.

- C. `show ip interface dhcp`

This is not a valid command in Cisco IOS. The `show ip interface` command does not have a `dhcp` option.

- E. `show ip interface GigabitEthernet 0/0 brief`

This is not a valid command in Cisco IOS. The `brief` keyword is not used with the `show ip interface` command. The correct command to get a brief summary of interface IP information is `show ip interface brief`. However, this command also does not specifically indicate if the IP address was assigned via DHCP.

Q137: Which statement about the nature of NAT overload is true?

- A. applies a one-to-many relationship to internal IP addresses
- B. applies a one-to-one relationship to internal IP addresses
- C. applies a many-to-many relationship to internal IP addresses
- D. can be configured only on Gigabit interface

▼ Answer

- A. applies a one-to-many relationship to internal IP addresses**
- B. applies a one-to-one relationship to internal IP addresses
- C. applies a many-to-many relationship to internal IP addresses
- D. can be configured only on Gigabit interface



More details Steps:

- A. applies a one-to-many relationship to internal IP addresses

Explanation:

Network Address Translation (NAT) overload, also known as Port Address Translation (PAT), maps multiple private IP addresses to a single public IP address or a few public IP addresses. It is typically used by routers which connect private networks to the public Internet, and it conserves the number of public IP addresses that a company needs to use.

In the context of NAT overload, a "one-to-many" relationship refers to the fact that one public IP address can be used to represent multiple private IP addresses. The router keeps track of all outbound traffic and their specific sessions based on port numbers, ensuring that when the responses return, they are sent back to the correct private IP address, even though they all appear to be from the same public IP address to the outside world.

Options B and C are not typically associated with NAT overload. A one-to-one relationship (B) is more characteristic of static NAT, and a many-to-many relationship (C) is not a typical NAT scenario.

Option D is not correct because NAT overload is not limited to any specific type of interface, such as a Gigabit interface. It can be configured on any interface that supports IP.

Q138: Which command is used to configure an IPv6 static default route?

- A. ipv6 route ::/0 interface next-hop5
- B. ipv6 route default interface next-hop
- C. ipv6 route 0.0.0.0/0 interface next-hop
- D. ip route 0.0.0.0/0 interface next-hop

▼ Answer

A. ipv6 route ::/0 interface next-hop5

- B. ipv6 route default interface next-hop
- C. ipv6 route 0.0.0.0/0 interface next-hop
- D. ip route 0.0.0.0/0 interface next-hop



More details Steps:

- A. ipv6 route ::/0 interface next-hop

Explanation:

In IPv6, the default route is represented by `::/0`. The command to configure an IPv6 static default route on a Cisco router is `ipv6 route ::/0 {next-hop}` where `{next-hop}` is the address of the next hop or the exit interface.

Both options C and D use the IPv4 default route (`0.0.0.0/0`), not the IPv6 default.

Option B is not correct because `default` is not used to specify the default route in the `ipv6 route` command.

Q139: Which statement about static and dynamic routes is true?

- A. Dynamic routes are manually configured by a network administrator, while static routes are automatically learned and adjusted by a routing protocol.
- B. Static routes are manually configured by a network administrator, while dynamic routes are automatically learned and adjusted by a routing protocol.
- C. Static routes tell the router how to forward packets to networks that are not directly connected, while dynamic routes tell the router how to forward packets to networks that are directly connected.
- D. Dynamic routes tell the router how to forward packets to networks that are not directly connected, while static routes tell the router how to forward packets to networks that are directly connected.

▼ Answer

- A. Dynamic routes are manually configured by a network administrator, while static routes are automatically learned and adjusted by a routing protocol.

B. Static routes are manually configured by a network administrator, while dynamic routes are automatically learned and adjusted by a routing protocol.

- C. Static routes tell the router how to forward packets to networks that are not directly connected, while dynamic routes tell the router how to forward packets to networks that are directly connected.
- D. Dynamic routes tell the router how to forward packets to networks that are not directly connected, while static routes tell the router how to forward packets to networks that are directly connected.



More details Steps:

B. Static routes are manually configured by a network administrator, while dynamic routes are automatically learned and adjusted by a routing protocol.

Explanation:

Static routes are routes that are manually configured and entered into the routing table by a network administrator. They do not change unless the network administrator changes them.

Dynamic routes, on the other hand, are routes that are learned automatically through a routing protocol (like OSPF, EIGRP, BGP etc.). These routes can change dynamically as the network topology changes, or as routers exchange information about the network with each other.

Options A, C, and D are incorrect because they either mix up the definitions of static and dynamic routes, or they make incorrect statements about how these types of routes are used in relation to directly connected networks.

Q140: What is the purpose of the show ip ospf interface command?

- A. displaying OSPF-related interface information
- B. displaying general information about OSPF routing processes
- C. displaying OSPF neighbor information on a per-interface basis
- D. displaying OSPF neighbor information on a per-interface-type basis

▼ Answer

A. displaying OSPF-related interface information

- B. displaying general information about OSPF routing processes
- C. displaying OSPF neighbor information on a per-interface basis
- D. displaying OSPF neighbor information on a per-interface-type basis



More details Steps:

A. displaying OSPF-related interface information

Explanation:

The command `show ip ospf interface` is used in a Cisco IOS device to display detailed information about the OSPF (Open Shortest Path First) status of all OSPF-enabled interfaces on the device. This includes the interface's OSPF Area, OSPF Cost, OSPF State, OSPF Priority, OSPF timers and more.

Option B is not accurate because while the command does provide information about OSPF, it's specifically tied to interface information, not general OSPF routing processes.

Option C is not accurate because, while it does provide information related to OSPF on an interface, it does not specifically provide neighbor information. For OSPF neighbor information, you would use the `show ip ospf neighbor` command.

Option D is not accurate as the command does not categorize or display the information on a per-interface-type basis.

Q141: How can the Cisco Discovery Protocol be used?

- A. to allow a switch to discover the devices that are connected to its ports
- B. to determine the hardware platform of the device
- C. to determine the IP addresses of connected Cisco devices
- D. all of the above

▼ Answer

- A. to allow a switch to discover the devices that are connected to its ports
- B. to determine the hardware platform of the device

C. to determine the IP addresses of connected Cisco devices

D. all of the above



More details Steps:

D. all of the above

Explanation:

Cisco Discovery Protocol (CDP) is a proprietary protocol designed by Cisco to help administrators collect information about both locally attached and remote devices. By using CDP, you can gather hardware and protocol information about neighbor devices, which can be useful in a number of scenarios, including troubleshooting and documentation.

Here's how the options relate to CDP:

- A. CDP can indeed allow a switch to discover the devices that are connected to its ports. When a Cisco device boots up, it begins sending CDP packets from each of its connected interfaces, which can then be identified by other Cisco devices on the same network.
- B. CDP packets contain a wide variety of information, including the hardware platform of the device.
- C. CDP packets also contain IP address information about the device, making it possible to determine the IP addresses of connected Cisco devices.

Q142: How does STP prevent forwarding loops at OSI Layer 2?

- A. TTL
- B. MAC address forwarding
- C. Collision avoidance
- D. Port blocking

▼ **Answer**

- A. TTL
- B. MAC address forwarding
- C. Collision avoidance
- D. Port blocking**



More details Steps:

D. Port blocking

Explanation:

The Spanning Tree Protocol (STP) is a network protocol designed to prevent loops in a network topology at the data link layer (Layer 2) of the OSI model. It does this by selectively blocking some ports and leaving others open in a calculated manner to ensure there is only one active path between any two network nodes.

- A. TTL (Time to Live) is a mechanism used at the Network Layer (Layer 3) to prevent packets from looping forever in the network. It isn't applicable to Layer 2 where STP operates.
- B. MAC address forwarding refers to the operation of a switch where it learns MAC addresses and forwards frames based on that information. It doesn't inherently prevent loops.
- C. Collision avoidance is a mechanism used in wireless networks to prevent data collisions. It is not related to the prevention of forwarding loops.

Q143: Order the DHCP message types as they would occur between a DHCP client and a DHCP server.

Order		right
1		DHCPREQUEST
2		DHCPDISCOVER
3		DHCPOFFER
4		DHCPPACK

▼ Answer

Order	DHCP Message Type
1	DHCPDISCOVER
2	DHCPOFFER
3	DHCPREQUEST
4	DHCPACK



More details Steps:

1. **DHCPDISCOVER:** The client sends a DHCPDISCOVER message to locate any available DHCP servers in the network.
2. **DHCPOFFER:** DHCP servers receive the DHCPDISCOVER broadcast and respond with a DHCPOFFER which includes an available IP address for the client.
3. **DHCPREQUEST:** The client receives one or more DHCPOFFERS and responds to the selected server with a DHCPREQUEST message, requesting the offered IP address. It can also be used for lease renewal or extension.
4. **DHCPACK:** The server sends a DHCPACK (Acknowledgement) message to the client, confirming the lease of the IP address to the client. This message will include the lease duration and any other configuration information that the client might have requested.

Q144: Which two statements about EtherChannel technology are true? (Choose two.)

- A. EtherChannel provides increased bandwidth by bundling existing FastEthernet or Gigabit Ethernet interfaces into a single EtherChannel.
- B. STP does not block EtherChannel links.
- C. You can configure multiple EtherChannel links between two switches, using up to a limit of sixteen physical ports.
- D. EtherChannel does not allow load sharing of traffic among the physical links within the EtherChannel.
- E. EtherChannel allows redundancy in case one or more links in the EtherChannel fail.

▼ Answer

A. EtherChannel provides increased bandwidth by bundling existing FastEthernet or Gigabit Ethernet interfaces into a single EtherChannel.

- B. STP does not block EtherChannel links.
- C. You can configure multiple EtherChannel links between two switches, using up to a limit of sixteen physical ports.
- D. EtherChannel does not allow load sharing of traffic among the physical links within the EtherChannel.

E. EtherChannel allows redundancy in case one or more links in the EtherChannel fail.



More details Steps:

- A. EtherChannel provides increased bandwidth by bundling existing FastEthernet or Gigabit Ethernet interfaces into a single EtherChannel.
- E. EtherChannel allows redundancy in case one or more links in the EtherChannel fail.

Explanation:

- A. **EtherChannel** allows you to group several physical Ethernet links to create a logical Ethernet link for the purpose of providing fault-tolerance and high-speed links between switches, routers and servers. This provides increased bandwidth by bundling the capacity of the individual links.
- B. **STP (Spanning Tree Protocol)** views the entire EtherChannel as a single link, so it's not correct to say that STP does not block EtherChannel links. If necessary (for example, to prevent a loop), STP can indeed block an EtherChannel link.
- C. The maximum number of interfaces you can use in an EtherChannel depends on the platform and Cisco IOS software release. On some older switches, you can bundle up to 8 active links into a single EtherChannel. However, newer switches (like the Cisco Catalyst 3850 Series) do allow up to 16 active member ports per EtherChannel. This option needs clarification on the specific platform and software version.
- D. **EtherChannel** does allow load sharing of traffic among the physical links within the EtherChannel. The method of load balancing can be based on source or destination MAC addresses, IP addresses, or Layer 4 port numbers.
- E. **EtherChannel** indeed provides redundancy. If one of the physical links within the EtherChannel fails, traffic previously carried over the failed link switches over to the remaining operational links within the EtherChannel, providing a degree of fault tolerance.

Q145: Which three statements about MAC addresses are correct? (Choose three.)

- A. To communicate with other devices on a network, a network device must have a unique MAC address.
- B. The MAC address is also referred to as the IP address.
- C. The MAC address of a device must be configured in the Cisco IOS CLI by a user with administrative privileges.
- D. A MAC address contains two main components, the first of which identifies the manufacturer of the hardware and the second of which uniquely identifies the hardware.
- E. An example of a MAC address is 0A:26:38: D6:65:90.
- F. A MAC address contains two main components, the first of which identifies the network on which the host resides and the second of which uniquely identifies the host on the network.

▼ Answer

- A. To communicate with other devices on a network, a network device must have a unique MAC address.**
- B. The MAC address is also referred to as the IP address.
- C. The MAC address of a device must be configured in the Cisco IOS CLI by a user with administrative privileges.
- D. A MAC address contains two main components, the first of which identifies the manufacturer of the hardware and the second of which uniquely identifies the hardware.**
- E. An example of a MAC address is 0A:26:38: D6:65:90.**
- F. A MAC address contains two main components, the first of which identifies the network on which the host resides and the second of which uniquely identifies the host on the network.

**More details Steps:**

- A. To communicate with other devices on a network, a network device must have a unique MAC address.
- D. A MAC address contains two main components, the first of which identifies the manufacturer of the hardware and the second of which uniquely identifies the hardware.
- E. An example of a MAC address is 0A:26:38:D6:65:90.

Explanation:

- A. Each network device must indeed have a unique MAC (Media Access Control) address to communicate with other devices on a network. This Layer 2 address is used in Ethernet networking for data transfer across devices on the same network segment.
- B. A MAC address is not the same as an IP address. An IP address is a Layer 3 (Network Layer) address in the OSI model and is used to deliver packets to a specific network and specific host on that network.
- C. A MAC address is hardcoded on a network interface card (NIC) by its manufacturer and typically does not need to be manually configured in the Cisco IOS CLI by a user.
- D. A MAC address contains two main components. The first half of the MAC address is the Organizationally Unique Identifier (OUI), which identifies the manufacturer of the network card. The second half is the serial number of the adapter and is unique to the device.
- E. The provided string is indeed a valid format for a MAC address. MAC addresses are 48 bits long and typically displayed in hexadecimal format, separated by colons or hyphens.
- F. This statement is incorrect. The components of a MAC address do not identify the network on which the host resides nor the host on the network. They identify the manufacturer of the network card and the serial number of the adapter.

Q146: Which three statements about network characteristics are true? (Choose three.)

- A. Speed is a measure of the data rate in bits per second of a given link in the network.
- B. Scalability indicates how many nodes are currently on the network.
- C. The logical topology is the arrangement of cables, network devices, and end systems.
- D. Availability is a measure of the probability that the network will be available for use when it is required.
- E. Reliability indicates the dependability of the components that make up the network.

▼ Answer

- A. Speed is a measure of the data rate in bits per second of a given link in the network.**
- B. Scalability indicates how many nodes are currently on the network.
- C. The logical topology is the arrangement of cables, network devices, and end systems.
- D. Availability is a measure of the probability that the network will be available for use when it is required.**
- E. Reliability indicates the dependability of the components that make up the network.**



More details Steps:

- A. Speed is a measure of the data rate in bits per second of a given link in the network.
- D. Availability is a measure of the probability that the network will be available for use when it is required.
- E. Reliability indicates the dependability of the components that make up the network.

Explanation:

- A. The term "speed" in the context of networking usually refers to data transfer rate, which is indeed measured in bits per second (bps).
- B. Scalability does not indicate how many nodes are currently on the network. Instead, it refers to the network's capacity to grow and manage increased demand. A scalable network can expand to accommodate more users and devices without suffering performance degradation.
- C. The logical topology refers to the way a network transfers data between devices, not the physical arrangement of cables, devices, and systems. For example, in a ring topology, data travels in a circular direction from one device to another until it reaches its destination. The physical topology, on the other hand, describes the physical layout of the network.
- D. Availability in a network context refers to the system's readiness for correct service. It's essentially a measure of the system's uptime.
- E. Reliability in a network context refers to the ability of the network's components (e.g., routers, switches, software) to consistently perform according to their intended specifications. A reliable network minimizes the frequency of failures, quickly recovers from any failures that do occur, and helps to prevent failures from affecting other parts of the system.

Q147: Which two statements about the purpose of the OSI model are accurate? (Choose two.)

- A. Defines the network functions that occur at each layer
- B. Facilitates an understanding of how information travels throughout a network
- C. Changes in one layer do not impact other layer

▼ Answer

A. Defines the network functions that occur at each layer

B. Facilitates an understanding of how information travels throughout a network

- C. Changes in one layer do not impact other layer



More details Steps:

- A. Defines the network functions that occur at each layer
- B. Facilitates an understanding of how information travels throughout a network

Explanation:

- A. The Open Systems Interconnection (OSI) model is a conceptual framework that standardizes the functions of a communication system into seven categories, known as layers. This abstraction helps to define the network functions that occur at each layer.
- B. By abstracting the complex processes involved in data communication into more manageable layers, the OSI model facilitates a better understanding of how information travels from one network device to another. However, the statement - "C. Changes in one layer do not impact other layers" is not entirely accurate. While the OSI model is designed to allow changes in one layer without affecting other layers, in practice, changes in one layer could potentially impact the functionality of layers above or below it. For example, if the Physical Layer (Layer 1) is affected (e.g., a cable is cut), this will certainly affect the higher layers' ability to communicate.

Q148: You have two paths for the 10.10.10.0 network - one that has a feasible distance of 3072 and the other of 6144.

What do you need to do to load balance your EIGRP routes?

- A. Change the maximum paths to 2
- B. Change the configuration so they both have the same feasible distance
- C. Change the variance for the path that has a feasible distance of 3072 to 2
- D. Change the IP addresses so both paths have the same source IP address

▼ Answer

- A. Change the maximum paths to 2
- B. Change the configuration so they both have the same feasible distance
- C. Change the variance for the path that has a feasible distance of 3072 to 2**
- D. Change the IP addresses so both paths have the same source IP address



More details Steps:

- C. Change the variance for the path that has a feasible distance of 3072 to 2

Explanation:

Enhanced Interior Gateway Routing Protocol (EIGRP) uses a concept called "variance" to perform unequal cost load balancing. By default, EIGRP only load balances across paths that have an equal cost (feasible distance).

However, with the use of the variance command, EIGRP can load balance across paths that do not have an equal cost. The variance command multiplies the feasible distance of the successor route. Any feasible successor routes with a feasible distance less than the product of the variance and the feasible distance of the successor route will be included in load balancing.

In this case, to allow EIGRP to load balance between the two paths, you would need to set the variance to 2. This is because the feasible distance of the less desirable path (6144) is 2 times that of the more desirable path (3072).

The other options provided do not correctly address the issue:

- A. Changing the maximum paths to 2 is not necessary because the default maximum paths value for EIGRP is 4 (for Cisco IOS versions after 12.3).
- B. Changing the configuration so they both have the same feasible distance involves changing the network's physical configuration, which is usually not a practical solution.
- D. Changing the IP addresses so both paths have the same source IP address doesn't affect EIGRP's path selection or load balancing decision. EIGRP bases its decisions on metrics (such as bandwidth, delay, reliability, load, and MTU), not source IP addresses.

Q149: Which of the following dynamic routing protocols are Distance Vector routing protocols?

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

▼ Answer

- A. IS-IS
- B. EIGRP**
- C. OSPF
- D. BGP
- E. RIP**

**More details Steps:**

- B. EIGRP (Enhanced Interior Gateway Routing Protocol)
- E. RIP (Routing Information Protocol)

Explanation:

- A. **IS-IS (Intermediate System to Intermediate System)** is a Link-State routing protocol, not a Distance Vector protocol.
- B. **EIGRP (Enhanced Interior Gateway Routing Protocol)** is considered a Distance Vector protocol, although it has characteristics of both Distance Vector and Link-State protocols. It's sometimes referred to as a "hybrid" protocol.
- C. **OSPF (Open Shortest Path First)** is a Link-State routing protocol, not a Distance Vector protocol.
- D. **BGP (Border Gateway Protocol)** is technically a Path Vector protocol, which is a type of Distance Vector protocol. However, BGP is not typically grouped with traditional Distance Vector protocols like RIP and EIGRP because it operates quite differently.
- E. **RIP (Routing Information Protocol)** is a classic example of a Distance Vector routing protocol.

Q150: Refer to the exhibit. If R1 receives a packet destined to 172.16.1.1, to which IP address does it send the packet?

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, si - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.14.4 to network 0.0.0.0

C  192.168.12.0/24 is directly connected, FastEthernet0/0
C  192.168.13.0/24 is directly connected, FastEthernet0/1
C  192.168.14.0/24 is directly connected, FastEthernet1/0
  192.168.10.0/24 is variably subnetted, 3 subnets, 3 masks
O   192.168.10.0/24 [110/2] via 192.168.14.4, 00:02:01, FastEthernet1/0
O   192.168.10.32/27 [110/11] via 192.168.13.3, 00:00:52, FastEthernet0/1
O   192.168.0.0/16 [110/2] via 192.168.15.5, 00:05:01, FastEthernet1/1
D   192.168.10.1/32 [90/52778] via 192.168.12.2, 00:03:44, FastEthernet0/0
O*E2 0.0.0.0/0 [110/1] via 192.168.14.4, 00:00:10, FastEthernet1/0
```

- A. 192.168.14.4
- B. 192.168.12.2
- C. 192.168.13.3
- D. 192.168.15.5

▼ Answer

- A. 192.168.14.4**
- B. 192.168.12.2
- C. 192.168.13.3
- D. 192.168.15.5

**More details Steps:**

In the routing table, the default route is set to 192.168.14.4. The default route is used when no other more specific routes match the destination IP address of a packet. Hence, if there's no specific entry in the routing table for 172.16.1.1, the router will use the default route and send the packet to 192.168.14.4.

Q151: Which two VLAN IDs indicate a default VLAN? (Choose two.)

- A. 0
- B. 1
- C. 1005
- D. 1006
- E. 4096

▼ Answer

- A. 0
- B. 1**
- C. 1005**
- D. 1006
- E. 4096



More details Steps:

- B. VLAN ID 1 is the default Ethernet VLAN on all Cisco switches. All switch ports become members of VLAN 1 by default.
- C. VLAN IDs 1002-1005 are reserved by default for FDDI and Token Ring VLANs in Cisco switches. These VLANs exist to support legacy technologies and are present in all Cisco switches.

Q152: Refer to the exhibit. If RTR01 is configured as shown, which three addresses will be received by other routers that are running EIGRP on the network? (Choose three)

```
RTR01 (config) #router eigrp 103
RTR01 (config-router) #network 10.4.3.0
RTR01 (config-router) #network 172.16.4.0
RTR01 (config-router) #network 192.168.2.0
RTR01 (config-router) #auto-summary
```

- A. 172.16.4.0
- B. 10.0.0.0
- C. 172.16.0.0
- D. 192.168.2.0
- E. 192.168.0.0
- F. 10.4.3.0

▼ Answer

- A. 172.16.4.0
- B. 10.0.0.0**
- C. 172.16.0.0**
- D. 192.168.2.0**
- E. 192.168.0.0
- F. 10.4.3.0



More details Steps:

The `network` command in EIGRP, when used without a wildcard mask, will indeed include all interfaces that fall within the classful network boundary.

Explanation:

- B. The `network 10.4.3.0` command will include all interfaces that fall within the 10.0.0.0 classful boundary.
- C. The `network 172.16.4.0` command will include all interfaces that fall within the 172.16.0.0 classful boundary.
- D. The `network 192.168.2.0` command will include all interfaces that fall within the 192.168.2.0 classful boundary.

The `auto-summary` command enables the automatic summarization of routes at classful boundaries, which reinforces this classful network behavior.

Q153: Which two options are the best reasons to use an IPv4 private IP space? (Choose two.)

- A. to enable intra-enterprise communication
- B. to implement NAT
- C. to connect applications

- D. to conserve global address space
- E. to manage routing overhead

▼ Answer

A. to enable intra-enterprise communication

- B. to implement NAT
- C. to connect applications

D. to conserve global address space

- E. to manage routing overhead



More details Steps:

Explanation:

A. Intra-enterprise communication: Private IP addresses are typically used within a single enterprise. This allows devices within the network to communicate with each other using these private addresses.

D. Conserve global address space: Private IP addresses help to alleviate the problem of IPv4 address exhaustion. Because they are used within a private network, they do not need to be globally unique. This allows the same private IP addresses to be used by many different organizations in their internal networks, conserving the global IPv4 address space.

Note:

B. To implement NAT: While Network Address Translation (NAT) is often used with private IP addresses, it is not a reason to use a private IP space. Rather, NAT is a technique that allows private IP spaces to be used.

C. Connect applications: While applications can certainly communicate over a network using private IP addresses, this is not a specific reason to use a private IP space. Applications can also communicate using public IP addresses.

E. Manage routing overhead: Private IP addresses can help to reduce routing overhead within a private network because they can be summarized more efficiently. However, this is more a benefit of careful IP address allocation and subnetting practices than of using private IP addresses per se.

Q154: Which technique can you use to route IPv6 traffic over an IPv4 infrastructure?

- A. NAT
- B. 6 to 4 tunneling
- C. L2TPv3
- D. dual-stack

▼ Answer

- A. NAT

B. 6 to 4 tunneling

- C. L2TPv3
- D. dual-stack



More details Steps:

Explanation:

6 to 4 tunneling is a transition mechanism for migrating from IPv4 to IPv6. It allows IPv6 packets to be transmitted over an IPv4 network. This is done by encapsulating the IPv6 packets within IPv4 packets for transmission over the IPv4 network.

Here's a brief explanation of why the other options are not correct:

- A. NAT (Network Address Translation) is not typically used to route IPv6 traffic over an IPv4 infrastructure. NAT is typically used to map one IP address space into another by modifying network address information in the IP header.
- C. L2TPv3 (Layer 2 Tunneling Protocol version 3) is a method for transporting layer 2 packets over an IP network. It doesn't specifically cater to IPv6 over IPv4 scenarios.
- D. Dual-stack means running IPv4 and IPv6 simultaneously on a network device. It doesn't mean routing IPv6 traffic over IPv4. Rather, it allows devices to run IPv4 and IPv6 in parallel until IPv6 takes over completely.

Q155: Which three describe the reasons large OSPF networks use a hierarchical design? (Choose three.)

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

▼ Answer

A. to speed up convergence

B. to reduce routing overhead

C. to lower costs by replacing routers with distribution layer switches

D. to decrease latency by increasing bandwidth

E. to confine network instability to single areas of the network

F. to reduce the complexity of router configuration



More details Steps:

Explanation:

A. Speed up convergence: In a hierarchical OSPF network, changes in one area do not affect the other areas. This way, routes can be recalculated more quickly because the calculations are confined to a specific area.

B. Reduce routing overhead: Hierarchical design also reduces routing overhead because each router doesn't need to know the routing details for all networks, just those within its own area and how to reach other areas.

E. Confining network instability to single areas: If a change (such as a link going down or coming back up) occurs within an OSPF area, the update is confined to that area. This reduces the impact of instabilities on the overall network.

The other options (C, D, and F) are not typically reasons for using a hierarchical design in an OSPF network:

C. Lower costs by replacing routers with distribution layer switches: The decision to use routers or switches is dependent on the specific network requirements and not directly related to OSPF hierarchical design.

D. Decrease latency by increasing bandwidth: While increasing bandwidth can decrease latency, this is not directly related to OSPF hierarchical design.

F. Reduce the complexity of router configuration: While a hierarchical OSPF network can make the OSPF configuration easier to understand, it does not necessarily reduce the complexity of the overall router configuration.

Q156: Which statements describe the routing protocol OSPF? (Choose three.)

- A. It supports VLSM.
- B. It is used to route between autonomous systems.
- C. It confines network instability to one area of the network.
- D. It increases routing overhead on the network.
- E. It allows extensive control of routing updates.
- F. It is simpler to configure than RIP v2.

▼ Answer

A. It supports VLSM.

B. It is used to route between autonomous systems.

C. It confines network instability to one area of the network.

D. It increases routing overhead on the network.

E. It allows extensive control of routing updates.

F. It is simpler to configure than RIP v2.



More details Steps:

A. OSPF supports Variable Length Subnet Masking (VLSM) or subnetting, which allows for more efficient use of IP address space within a network.

C. OSPF confines network instability to single areas of the network. This is one of the key benefits of OSPF's area-based hierarchy. If a change (such as a link going down or coming back up) occurs within an OSPF area, the update is confined to that area, preventing the entire network from being affected.

E. OSPF allows extensive control of routing updates. For example, you can control the frequency of routing updates, determine which routes are advertised, and set the cost of routes.

The other options (B, D, and F) are not accurate descriptions of OSPF:

B. OSPF is used for routing within an autonomous system, not between autonomous systems. The protocol used for routing between autonomous systems is typically BGP (Border Gateway Protocol).

D. OSPF does not necessarily increase routing overhead on the network. In fact, by using a link-state database and SPF algorithm, OSPF can often reduce routing overhead compared to distance-vector protocols.

F. OSPF is not inherently simpler to configure than RIP v2. OSPF's configuration can be quite complex, especially in large networks with multiple areas. However, the complexity can be managed with good network design and configuration practices.

Q157: Which command should you enter to view the error log in an EIGRP for IPv6 environment?

- A. show ipv6 eigrp neighbors
- B. show ipv6 eigrp topology
- C. show ipv6 eigrp traffic
- D. show ipv6 eigrp events

▼ Answer

A. show ipv6 eigrp neighbors

B. show ipv6 eigrp topology

C. show ipv6 eigrp traffic

D. show ipv6 eigrp events

**More details Steps:**

D. show ipv6 eigrp events

Explanation:

The show ipv6 eigrp events command is used to display information about EIGRP for IPv6 events, which includes error messages and other significant events related to EIGRP operations.

Here's a brief explanation of why the other options are not correct:

A. show ipv6 eigrp neighbors is used to display the IPv6 EIGRP neighbors that the router has discovered.

B. show ipv6 eigrp topology is used to display the EIGRP for IPv6 topology table.

C. show ipv6 eigrp traffic is used to display statistics about EIGRP for IPv6 traffic. This includes the number of packets sent and received, as well as other traffic-related statistics.

Q158: Which component of an Ethernet frame is used to notify a host that traffic is coming?

- A. start of frame delimiter
- B. Type field
- C. preamble
- D. Data field

▼ Answer

A. start of frame delimiter

B. Type field

C. preamble

D. Data field

**More details Steps:**

Explanation:

The preamble of an Ethernet frame is used to notify the receiving system that a frame is starting and to synchronize the receiver's clock with the sender's clock. It consists of a 7-byte pattern of alternating ones and zeros, which prepares the receiving device for the upcoming frame reception.

Here's a brief explanation of why the other options are not correct:

A. Start of frame delimiter: This 1-byte field signals the end of the preamble and the start of the actual frame, but it does not "notify a host that traffic is coming."

B. Type field: The type field in an Ethernet frame is used to indicate the higher layer protocol of the payload (e.g., IPv4, IPv6, ARP), not to notify a host that traffic is coming.

D. Data field: The data field contains the payload of the Ethernet frame (i.e., the actual data being transmitted), not a notification that traffic is coming.

Q159: Which command must you enter to guarantee that an HSRP router with higher priority becomes the HSRP primary router after it is reloaded?

- A. standby 10 preempt
- B. standby 10 version 1
- C. standby 10 priority 150
- D. standby 10 version 2

▼ Answer

A. standby 10 preempt

B. standby 10 version 1

C. standby 10 priority 150

D. standby 10 version 2



More details Steps:

Explanation:

The `standby preempt` command allows a router with higher priority to take over as the active (primary) router, even if another router is already serving as the active router. This command can be useful in scenarios where the router with the highest priority was offline (e.g., for maintenance or due to an issue) and then comes back online.

Here's a brief explanation of why the other options are not correct:

- B. `standby 10 version 1`: This command would set the HSRP version to 1 for the specific group (group 10 in this case). But it does not affect which router becomes the primary.
- C. `standby 10 priority 150`: This command sets the HSRP priority to 150 for the specific group (group 10 in this case). While a higher priority would make the router more likely to become the primary, it doesn't guarantee that the router will take over as the primary when it comes back online. For that, you still need the `preempt` command.
- D. `standby 10 version 2`: This command would set the HSRP version to 2 for the specific group (group 10 in this case). But it does not affect which router becomes the primary.

Q160: Which configuration command can you apply to a HSRP router so that its local interface becomes active if all other routers in the group fail?

- A. no additional config is required
- B. standby 1 track ethernet
- C. standby 1 preempt
- D. standby 1 priority 250

▼ Answer

A. no additional config is required

- B. standby 1 track ethernet
- C. standby 1 preempt
- D. standby 1 priority 250



More details Steps:

- A. no additional config is required

Explanation:

In the basic operation of HSRP, if the active router fails, the standby router with the highest priority would automatically take over. This happens without needing any additional configuration beyond setting up HSRP and defining priorities. The `standby preempt` command is used when you want a router with a higher priority to preempt an active router with a lower priority, but it's not necessary just for a standby router to take over when the active router fails.

Q161: You are configuring your edge routers interface with a public IP address for Internet connectivity. The router needs to obtain the IP address from the service provider dynamically.

Which command is needed on interface FastEthernet 0/0 to accomplish this?

- A. ip default-gateway
- B. ip route
- C. ip default-network
- D. ip address dhcp
- E. ip address dynamic

▼ Answer

A. ip default-gateway

- B. ip route
- C. ip default-network
- D. ip address dhcp**
- E. ip address dynamic



More details Steps:

Explanation:

The `ip address dhcp` command is used on a Cisco router interface to enable the interface to dynamically obtain an IP address from a DHCP server. In this case, the DHCP server would be provided by the Internet service provider (ISP).

Here's a brief explanation of why the other options are not correct:

- A. `ip default-gateway`: This command is used to specify the default gateway of a router when IP routing is disabled. It's typically used on hosts, not routers.
- B. `ip route`: This command is used to manually add entries to the routing table.
- C. `ip default-network`: This command is used to specify the default network to which the router sends packets if it doesn't have a specific route for the destination network.
- E. `ip address dynamic`: This is not a valid command in Cisco IOS. The correct command to dynamically obtain an IP address via DHCP is `ip address dhcp`.

Q162: Which type does a port become when it receives the best BPDU on a bridge?

- A. The designated port
- B. The backup port
- C. The alternate port
- D. The root port

▼ Answer

- A. The designated port
- B. The backup port
- C. The alternate port
- D. The root port**



More details Steps:

Explanation:

In the Spanning Tree Protocol (STP), the root port on a non-root bridge (or switch) is the port that has the lowest path cost to the root bridge. This is determined by the Bridge Protocol Data Units (BPDUs) that the bridge receives. If a port receives the best (lowest cost) BPDU, it becomes the root port.

Here's a brief explanation of why the other options are not correct:

- A. The designated port: This is the port that has the lowest cost to the root bridge from a network (not a bridge). Every network segment has one designated port, which is on the bridge with the lowest path cost to the root bridge.
- B. The backup port: This is a port that provides a redundant (backup) path to a network segment where another bridge port already connects. The backup port applies to a situation where there are two connections between two devices, which is less common in most network configurations.
- C. The alternate port: This is a port that provides an alternate path to the root bridge, different from the path that the root port provides. It's part of the Rapid Spanning Tree Protocol (RSTP), not the original STP.

Q163: Which two command sequences must be configured on a switch to establish a Layer 3 EtherChannel with an open-standard protocol? (Choose two.)

- A. `interface GigabitEthernet0/0/1 channel-group 10 mode auto`
- B. `interface GigabitEthernet0/0/1 channel-group 10 mode on`
- C. `interface port-channel 10 no switchport ip address 172.16.0.1 255.255.255.0`
- D. `interface GigabitEthernet0/0/1 channel-group 10 mode active`
- E. `interface port-channel 10 switchport switchport mode trunk`

▼ Answer

- A. `interface GigabitEthernet0/0/1 channel-group 10 mode auto`
- B. `interface GigabitEthernet0/0/1 channel-group 10 mode on`**

C. interface port-channel 10 no switchport ip address 172.16.0.1 255.255.255.0

- D. interface GigabitEthernet0/0/1 channel-group 10 mode active
- E. interface port-channel 10 switchport switchport mode trunk



More details Steps:

Explanation:

B. The `channel-group [number] mode on` command forces the physical interfaces into an EtherChannel bundle without using a negotiation protocol. This means the EtherChannel is always on, assuming the other side is also configured with `mode on`.

C. The `no switchport` command is used to switch the interface from a Layer 2 interface to a Layer 3 interface. The following `ip address [IP address] [subnet mask]` command assigns the IP address to the Layer 3 EtherChannel interface.

other options are not correct:

A. interface GigabitEthernet0/0/1 channel-group 10 mode auto

This command is typically used to enable the PAgP protocol in auto mode, which allows the interface to passively respond to PAgP negotiations from other interfaces. However, it will not initiate PAgP negotiation. This is not suitable for establishing a Layer 3 EtherChannel with an open-standard protocol, which is typically done with LACP (`mode active`), not PAgP (`mode auto` or `mode desirable`).

D. interface GigabitEthernet0/0/1 channel-group 10 mode active

This command enables LACP on the interface and allows the interface to actively negotiate with other interfaces to establish an LACP EtherChannel. However, in the context of this question, it's assumed that the EtherChannel is to be established without a negotiation protocol, using `mode on` instead of `mode active`.

E. interface port-channel 10 switchport switchport mode trunk

This command would configure the EtherChannel as a Layer 2 trunk, not a Layer 3 EtherChannel.

The `switchport mode trunk` command enables trunking on the EtherChannel and the double `switchport` is likely a typo. For a Layer 3 EtherChannel, you would use the `no switchport` command to put the interface into Layer 3 mode, and then assign an IP address to the interface.

Q164: Which statement about VLAN configuration is true?

- A. The switch must be in VTP server or transparent mode before you can configure a VLAN
- B. The switch must be in config-vlan mode before you configure an extended VLAN
- C. Dynamic inter-VLAN routing is supported on VLAN2 through VLAN 4094
- D. A switch in VTP transparent mode save the VLAN databases to the running configuration only

▼ Answer

A. The switch must be in VTP server or transparent mode before you can configure a VLAN

- B. The switch must be in config-vlan mode before you configure an extended VLAN
- C. Dynamic inter-VLAN routing is supported on VLAN2 through VLAN 4094
- D. A switch in VTP transparent mode save the VLAN databases to the running configuration only



More details Steps:

With VTP (VLAN Trunking Protocol), you can add, delete, and rename VLANs — information that is then propagated to all other switches in the VTP domain. However, you can only create, modify, or delete VLANs on a switch in the VTP server mode or in the transparent mode.

In VTP server mode, the changes you make to the VLANs on one switch are propagated to all other switches in the VTP domain.

In VTP transparent mode, you can create, modify, or delete VLANs, but these changes are local to the specific switch and are not propagated to other switches in the VTP domain.

In contrast, a switch in VTP client mode cannot create, modify, or delete VLANs. Hence, the statement is correct that a switch must be in VTP server mode or transparent mode before you can configure a VLAN.

Q165: Refer to the exhibit. After you apply the given configuration to a router, the DHCP clients behind the device cannot communicate with hosts outside of their subnet. Which action is most likely to correct the problem?

```
ip dhcp pool test
  network 192.168.10.0 /27
  domain-name cisco.com
  dns-server 172.16.1.1 172.16.2.1
  netbios-name-server 172.16.1.10 172.16.2.10
```

- A. Configure the dns server on the same subnet as the clients
- B. Activate the dhcp pool
- C. Correct the subnet mask
- D. Configure the default gateway

▼ Answer

- A. Configure the dns server on the same subnet as the clients
- B. Activate the dhcp pool
- C. Correct the subnet mask
- D. Configure the default gateway**



More details Steps:

Explanation:

In the given DHCP configuration, there is no default gateway (or default router) specified. The default gateway is the IP address of the router or switch interface that connects the DHCP clients to other networks. Without this, the DHCP clients would not be able to communicate with hosts outside of their subnet.

To correct this issue, you would need to add the `default-router [ip address]` command to the DHCP pool configuration, where `[ip address]` is the IP address of the router interface that acts as a gateway for the DHCP clients.

Q166: Refer to the exhibit. How will the router handle a packet destined for 192.0.2.156?

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

Gateway of last resort is 192.168.4.1 to network 0.0.0.0

  10.0.0.0/24 is subnetted, 3 subnets
C        10.0.2.0 is directly connected, Ethernet1
D        10.0.3.0 [90/2195456] via 192.168.1.2, 00:03:01, Serial0
D        10.0.4.0 [90/2195456] via 192.168.3.1, 00:03:01, Serial1
C        192.168.1.0/24 is directly connected, Serial0
D        192.168.2.0/24 [90/2681856] via 192.168.1.2, 00:03:01, Serial0
                                         [90/2681856] via 192.168.3.1, 00:03:01, Serial1
C        192.168.3.0/24 is directly connected, Serial1
C        192.168.4.0/24 is directly connected, Serial2
```

- A. The router will forward the packet via either Serial0 or Serial1.
- B. The router will return the packet to its source.
- C. The router will forward the packet via Serial2.
- D. The router will drop the packet.

▼ Answer

- A. The router will forward the packet via either Serial0 or Serial1.
- B. The router will return the packet to its source.
- C. The router will forward the packet via Serial2.**
- D. The router will drop the packet.



More details Steps:

Explanation:

The router's routing table, displayed with the `show ip route` command, does not contain a specific entry for the network 192.0.2.0/24 (which contains the IP address 192.0.2.156). Therefore, the router will use the default route for this packet.

The last line of the output indicates that the "Gateway of last resort" (which is the default route) is set to 192.168.4.1. This means that any packet destined for a network not specifically listed in the routing table will be sent towards 192.168.4.1.

In the routing table, we can see that the network 192.168.4.0/24 is directly connected to Serial2 (`192.168.4.0/24 is directly connected, Serial2`). Therefore, the default route is out of Serial2, and the router will forward the packet destined for 192.0.2.156 via Serial2.

Q167: Which unified access point mode continues to serve wireless clients after losing connectivity to the Cisco Wireless LAN Controller?

- A. local
- B. mesh
- C. flexconnect
- D. sniffer

▼ Answer

- A. local
- B. mesh
- C. flexconnect**
- D. sniffer



More details Steps:

Explanation:

FlexConnect, formerly known as Hybrid Remote Edge Access Point (H-REAP), is a wireless solution for branch office and remote office deployments. It enables access points to remain functional when they lose their connection to the controller.

In FlexConnect mode, certain capabilities are moved from the controller to the access point, including the ability to forward data traffic locally, even when the connection to the controller is lost. FlexConnect APs can also switch client data traffic locally and perform client authentication locally when their connection to the controller is lost.

Here's why the other options are not correct:

- A. Local: In Local mode, which is the default mode of operation, the access point needs a CAPWAP connection to the controller to function. If the connection to the controller is lost, the AP will stop serving clients.
- B. Mesh: Mesh APs use wireless connections to communicate with the controller and other APs. Like Local mode APs, Mesh APs require a connection to the controller to function.
- D. Sniffer: Sniffer mode is used for troubleshooting and does not serve wireless clients. In this mode, the AP captures and forwards all the packets on the wireless channel to a remote machine running packet analysis software.

Q168: Refer to exhibit. What Administrative distance has route to 192.168.10.1?

```

R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.14.4 to network 0.0.0.0

C 192.168.12.0/24 is directly connected, FastEthernet0/0
C 192.168.13.0/24 is directly connected, FastEthernet0/1
C 192.168.14.0/24 is directly connected, FastEthernet1/0
192.168.10.0/24 is variably subnetted, 3 subnets, 3 masks
O   192.168.10.0/24 [110/2] via 192.168.14.4, 00:02:01, FastEthernet1/0
O   192.168.10.32/27 [110/11] via 192.168.13.3, 00:00:52, FastEthernet0/1
O   192.168.0.0/16 [110/2] via 192.168.15.5, 00:05:01, FastEthernet1/1
D   192.168.10.1/32 [90/52778] via 192.168.12.2, 00:03:44, FastEthernet0/0
o*E2 0.0.0.0/0 [110/1] via 192.168.14.4, 00:00:10, FastEthernet1/0

```

- A. 1
- B. 90
- C. 110
- D. 120

▼ Answer

- A. 1
- B. 90**
- C. 110
- D. 120



More details Steps:

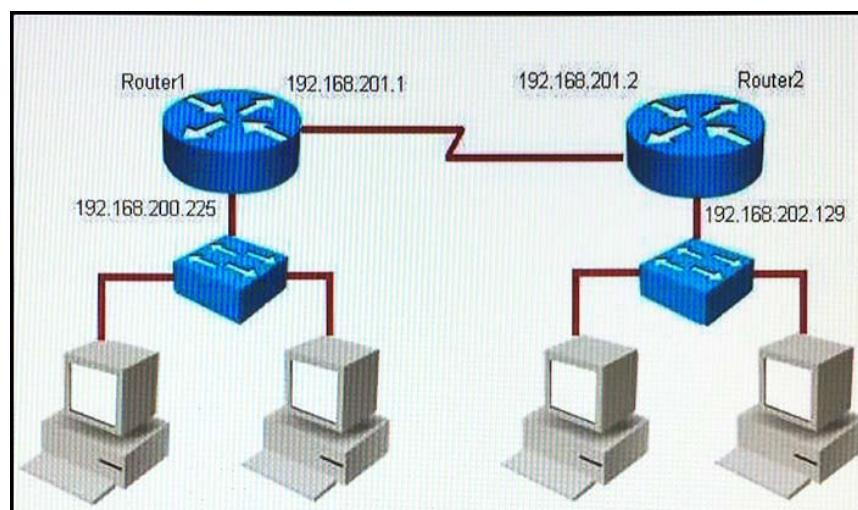
Looking at the provided route information:

```
192.168.10.1/32 [90/52778] via 192.168.12.2, 00:03:44, FastEthernet0/0
```

The administrative distance is represented by the first number in the brackets. Here, the administrative distance for the route to 192.168.10.1 is 90, which indicates that this route has been learned through EIGRP (Enhanced Interior Gateway Routing Protocol). The second number in the brackets is the metric for the route.

Administrative distance is a measure of the trustworthiness of the source of the routing information. Lower values indicate a more preferred source. For example, routes learned through EIGRP have an administrative distance of 90, OSPF has an administrative distance of 110, and RIP has an administrative distance of 120.

Q169: Refer to the exhibit. Which command would you use to configure a static route on Router1 to network 192.168.202.0/24 with a nondefault administrative distance?



- A. router1(config)#ip route 192.168.202.0 255.255.255.0 192.168.201.2 1
- B. router1(config)#ip route 192.168.202.0 255.255.255.0 192.168.201.2 5
- C. router1(config)#ip route 1 192.168.201.1 255.255.255.0 192.168.201.2
- D. router1(config)#ip route 5 192.168.202.0 255.255.255.0 192.168.201.2

▼ Answer

- A. router1(config)#ip route 192.168.202.0 255.255.255.0 192.168.201.2 1
- B. router1(config)#ip route 192.168.202.0 255.255.255.0 192.168.201.2 5**
- C. router1(config)#ip route 1 192.168.201.1 255.255.255.0 192.168.201.2
- D. router1(config)#ip route 5 192.168.202.0 255.255.255.0 192.168.201.2



More details Steps:

Explanation:

To configure a static route on a Cisco router, you use the `ip route` command. The syntax for the command is `ip route destination-network destination-subnet-mask next-hop-IP-address [administrative-distance]`. The `[administrative-distance]` part is optional and is used to set a nondefault administrative distance for the route.

In this case, you want to set a static route to the network 192.168.202.0/24 via the next hop 192.168.201.2. You also want to set a nondefault administrative distance. The administrative distance can be any integer from 1 to 255.

So, option B is the correct answer because it correctly specifies the destination network and subnet mask, the next hop IP address, and a nondefault administrative distance of 5.

Option A is incorrect because it uses an administrative distance of 1, which is typically reserved for directly connected networks. Options C and D are incorrect because they don't correctly specify the destination network and subnet mask.

Q170: Which feature or protocol is required for an IP SLA to measure UDP jitter?

- A. LLDP
- B. EEM
- C. CDP
- D. NTP

▼ Answer

- A. LLDP
- B. EEM
- C. CDP
- D. NTP**



More details Steps:

Explanation:

UDP Jitter IP SLA operation requires both the source router and the target router to have Network Time Protocol (NTP) synchronization. This is because the UDP Jitter operation measures the delay, packet loss, and jitter (delay variation) in the network by generating synthetic UDP traffic. The accuracy of these measurements is dependent on both the source and target devices having synchronized clocks, which is achieved by using NTP.

Here's why the other options are not correct:

- A. LLDP (Link Layer Discovery Protocol) is a vendor-neutral link layer protocol used by network devices for advertising their identity, capabilities, and neighbors on a local area network. It doesn't have a role in measuring UDP jitter.
- B. EEM (Embedded Event Manager) is a technology that allows you to automate tasks on Cisco devices. While it could potentially be used in conjunction with IP SLA to react to certain measurements, it's not required for measuring UDP jitter.
- C. CDP (Cisco Discovery Protocol) is a Cisco proprietary protocol used to discover Cisco devices in the network. It doesn't have a role in measuring UDP jitter.

Q171: Which effect does the aaa new-model configuration command have?

- A. It enables AAA services on the device.
- B. It configures the device to connect to a RADIUS server for AAA.
- C. It associates a RADIUS server to the group.
- D. It configures a local user on the device.

▼ Answer

A. It enables AAA services on the device.

- B. It configures the device to connect to a RADIUS server for AAA.
- C. It associates a RADIUS server to the group.
- D. It configures a local user on the device.



More details Steps:

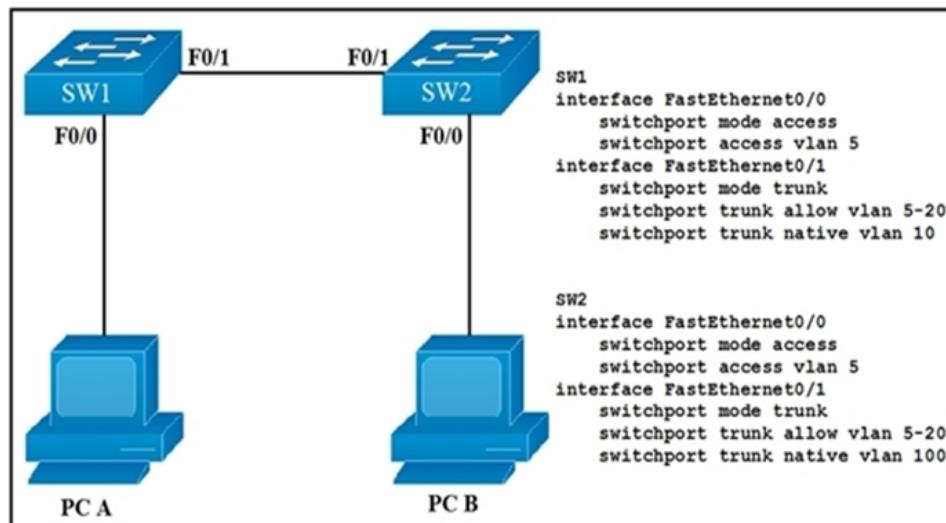
Explanation:

The `aaa new-model` command is used on Cisco devices to enable the Authentication, Authorization, and Accounting (AAA) framework. This framework provides a method of managing a device's services, controlling who can access those services, and tracking what actions each user takes while accessing the device.

Here's why the other options are not correct:

- B. The `aaa new-model` command does not in itself configure the device to connect to a RADIUS server for AAA. This requires additional configuration commands such as `radius-server host` and `aaa group server radius`.
- C. The `aaa new-model` command does not associate a RADIUS server to the group. This also requires further configuration commands such as `aaa group server radius`.
- D. The `aaa new-model` command does not configure a local user on the device. Local users are configured using the `username` command.

Q172: Refer to the exhibit. How will switch SW2 handle traffic from VLAN 10 on SW1?



- A. It sends the traffic to VLAN 10.
- B. It sends the traffic to VLAN 100.
- C. It drops the traffic.
- D. It sends the traffic to VLAN 1.

▼ Answer

- A. It sends the traffic to VLAN 10.
- B. It sends the traffic to VLAN 100.**
- C. It drops the traffic.
- D. It sends the traffic to VLAN 1.



More details Steps:

Explanation:

In the given configuration, SW1 has its FastEthernet0/1 interface configured as a trunk, with the native VLAN set to 10. This means that any untagged traffic coming from this interface will be associated with VLAN 10.

On the other side, SW2 also has its FastEthernet0/1 interface configured as a trunk, but with the native VLAN set to 100. This means that any untagged traffic received on this interface will be associated with VLAN 100.

As a result, when SW1 sends untagged traffic from VLAN 10 on its FastEthernet0/1 interface, SW2 will receive this traffic on its FastEthernet0/1 interface and associate it with VLAN 100, thus sending the traffic to VLAN 100. This is due to the mismatch in native VLAN configuration between SW1 and SW2.

Q173: Which two commands can you use to configure an actively negotiate EtherChannel? (Choose two.)

- A. channel-group 10 mode on
- B. channel-group 10 mode auto
- C. channel-group 10 mode passive
- D. channel-group 10 mode desirable
- E. channel-group 10 mode active

▼ Answer

- A. channel-group 10 mode on
- B. channel-group 10 mode auto
- C. channel-group 10 mode passive
- D. channel-group 10 mode desirable**
- E. channel-group 10 mode active**



More details Steps:

Explanation:

EtherChannel in Cisco devices can be configured using either Port Aggregation Protocol (PAgP) or Link Aggregation Control Protocol (LACP). Both PAgP and LACP support the concept of actively negotiating the formation of an EtherChannel.

- In the context of PAgP, `desirable` mode is used for active negotiation. `Desirable` means the interface will actively attempt to negotiate an EtherChannel.
- In the context of LACP, `active` mode is used for active negotiation. `Active` is similar to PAgP's `desirable`.

remaining options:

- A. channel-group 10 mode on

This option forces the EtherChannel to be formed without any negotiation process. Hence, it does not actively negotiate, which does not meet the criteria of the question.

- B. channel-group 10 mode auto

This option sets the interface to a passive negotiating state, using the Port Aggregation Protocol (PAgP). In the `auto` mode, the interface responds to PAgP packets it receives but does not initiate PAgP negotiation. This is a passive operation, not active.

- C. channel-group 10 mode passive

This option sets the interface to a passive negotiating state, using the Link Aggregation Control Protocol (LACP). In the `passive` mode, the interface responds to LACP packets that it receives, but does not initiate LACP negotiation. This is also a passive operation, not active.

Q174: What is the binary pattern of unique ipv6 unique local address?

- A. 00000000
- B. 11111100
- C. 11111111
- D. 11111101

▼ Answer

- A. 00000000
- B. 11111100**
- C. 11111111
- D. 11111101



More details Steps:

Explanation:

IPv6 Unique Local Addresses (ULAs) are similar to IPv4 private addresses. Just like IPv4 private addresses, these addresses are not routable on the internet. They are meant to be used in local communication within a site and between a limited number of sites.

The binary pattern for an IPv6 Unique Local Address is 11111100 at the start of the address, which corresponds to FC00::/7 in hexadecimal. However, it's worth noting that the lower half of this block (FC00::/8) has been reserved for future use. The currently used ULA range is FD00::/8, which still matches the 11111100 binary pattern at the start.

Q175: Which two statements about exterior routing protocols are true? (Choose two.)

- A. They determine the optimal within an autonomous system.
- B. They determine the optimal path between autonomous systems.
- C. BGP is the current standard exterior routing protocol.
- D. Most modern networking supports both EGP and BGP for external routing.
- E. Most modern network routers support both EGP and EIGRP for external routing.

▼ Answer

- A. They determine the optimal within an autonomous system.
- B. They determine the optimal path between autonomous systems.**
- C. BGP is the current standard exterior routing protocol.**
- D. Most modern networking supports both EGP and BGP for external routing.
- E. Most modern network routers support both EGP and EIGRP for external routing.



More details Steps:

- B. They determine the optimal path between autonomous systems.
- C. BGP is the current standard exterior routing protocol.

Explanation:

Exterior routing protocols, also known as Exterior Gateway Protocols (EGPs), are used to exchange routing information between autonomous systems (AS). BGP, or Border Gateway Protocol, is the current standard exterior routing protocol used on the internet. BGP is used to find the best path between autonomous systems, which is why option B is also correct.

Option A is incorrect because interior routing protocols, not exterior ones, are used to find the optimal path within an autonomous system.

Options D and E are incorrect. EGP is an outdated protocol and is not typically supported by modern network routers. EIGRP, although it can be used in some multi-AS deployments, is primarily an Interior Gateway Protocol (IGP), not an Exterior Gateway Protocol.

Q176: What is the destination MAC address of a broadcast frame?

- A. ff:ff:ff:ff:ff:ff
- B. 43:2e:08:00:00:0c
- C. 00:00:0c:43:2e:08
- D. 00:00:0c:ff:ff:ff

▼ Answer

- A. ff:ff:ff:ff:ff:ff
- B. 43:2e:08:00:00:0c
- C. 00:00:0c:43:2e:08
- D. 00:00:0c:ff:ff:ff



More details Steps:

- A. ff:ff:ff:ff:ff:ff

Explanation:

In Ethernet networking, the MAC (Media Access Control) address ff:ff:ff:ff:ff:ff is reserved for broadcast traffic. This address is recognized by all devices within the local network. When a frame with this destination MAC address is sent, it will be received and processed by every device in the broadcast domain.

Q177: You have configured a router with an OSPF router ID, but its IP address still reflects the physical interface.

Which action can you take to correct the problem in the least disruptive way?

- A. Reload the OSPF process
- B. Specify a loopback address
- C. Reboot the router
- D. Save the router configuration

▼ Answer

- A. Reload the OSPF process**
- B. Specify a loopback address
- C. Reboot the router
- D. Save the router configuration



More details Steps:

- A. Reload the OSPF process: This is the correct answer. As explained before, the OSPF router ID is determined when the OSPF process starts. If you change the router ID or add a new loopback interface with a higher IP address, you need to reload the OSPF process to make OSPF use the new router ID.
- B. Specify a loopback address: While it's true that OSPF prefers a loopback interface's IP address over a physical interface's IP address when choosing a router ID, simply adding a loopback address will not change the router ID of an OSPF process that's already running. You would still need to reload the OSPF process to make it recognize the new address as the router ID.
- C. Reboot the router: This would indeed cause the OSPF process to use the new router ID or loopback address, but it's more disruptive than simply reloading the OSPF process. If the only thing you need to do is make OSPF recognize a new router ID, reloading the OSPF process is sufficient and less disruptive.
- D. Save the router configuration: While it's always a good idea to save your router configuration, doing so will not cause OSPF to recognize a new router ID or loopback address. Saving the configuration simply ensures that your settings are retained the next time the router reboots. You would still need to reload the OSPF process or reboot the router for OSPF to recognize a new router ID.

Q178: Which two statements about VTP are true? (Choose two.)

- A. All switches must be configured with the same VTP domain name
- B. All switches must be configured to perform trunk negotiation
- C. All switches must be configured with a unique VTP domain name
- D. The VTP server must have the highest revision number in the domain
- E. All switches must use the same VTP version

▼ Answer

- A. All switches must be configured with the same VTP domain name**
- B. All switches must be configured to perform trunk negotiation
- C. All switches must be configured with a unique VTP domain name

D. The VTP server must have the highest revision number in the domain

E. All switches must use the same VTP version



More details Steps:

Explanation:

VTP (VLAN Trunking Protocol) is a Cisco proprietary protocol that propagates the definition of Virtual Local Area Networks (VLAN) on the whole local area network.

A. All switches in the same VTP management domain must be configured with the same domain name. This allows them to share VLAN configuration information.

B. Trunk negotiation is not a requirement for VTP. It's a separate process that can be manually configured or automatically negotiated via DTP (Dynamic Trunking Protocol).

C. All switches in the same VTP management domain must use the same domain name, not unique ones. Using the same name allows them to share VLAN configuration information.

D. The VTP server does not need to have the highest revision number. However, any switch with a higher revision number can overwrite VLAN information in the entire VTP domain. Therefore, caution must be exercised when adding a switch to a VTP domain.

E. All switches in the same VTP management domain should use the same VTP version (either VTP version 1, 2, or 3) to ensure compatibility and proper propagation of VLAN information.

Q179: Which two pieces of information about a Cisco device can Cisco Discovery Protocol communicate? (Choose two.)

- A. the native VLAN
- B. the trunking protocol
- C. the VTP domain
- D. the spanning-tree priority
- E. the spanning-tree protocol

▼ Answer

A. the native VLAN

B. the trunking protocol

C. the VTP domain

D. the spanning-tree priority

E. the spanning-tree protocol



More details Steps:

Explanation:

Cisco Discovery Protocol (CDP) is a proprietary Data Link Layer protocol developed by Cisco. It's used to share information about directly connected Cisco equipment.

A. Native VLAN: CDP can share information about the native VLAN configured on a switch port.

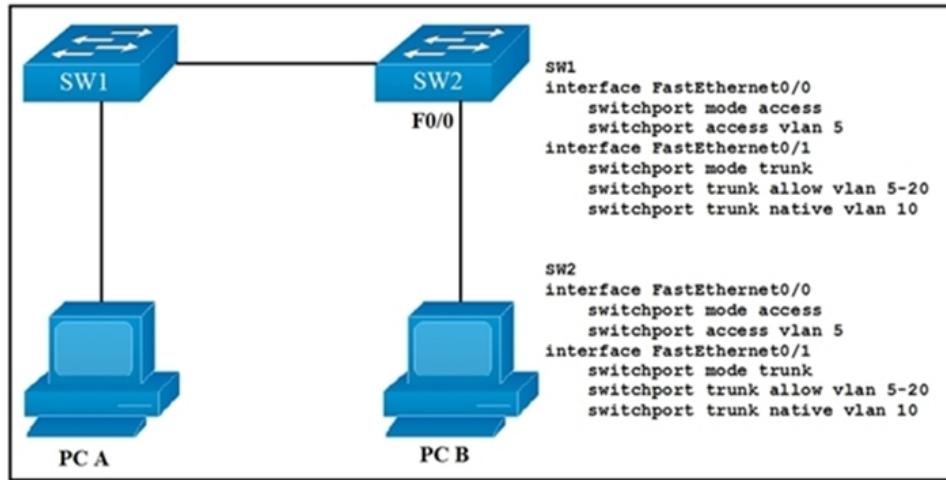
B. Trunking Protocol: CDP does not communicate the trunking protocol used (like ISL or 802.1Q).

C. VTP domain: CDP can share information about the VTP (VLAN Trunking Protocol) domain to which a switch belongs.

D. Spanning-tree Priority: CDP does not communicate spanning-tree priority.

E. Spanning-tree Protocol: While CDP can identify the type of device connected and some of its capabilities, it does not specifically communicate the spanning-tree protocol used on the device.

Q180: Refer to the exhibit. Which VLAN ID is associated with the default VLAN in the given environment?



- A. VLAN 1
- B. VLAN 5
- C. VLAN 10
- D. VLAN 20

▼ Answer

A. VLAN 1

- B. VLAN 5
- C. VLAN 10
- D. VLAN 20



More details Steps:

Explanation:

In a Cisco switch environment, the default VLAN is always VLAN 1. This is a factory-set default and cannot be changed.

VLAN 1 is the default management and native VLAN on Cisco switches. All switch ports become a member of VLAN 1 by default.

In the exhibit, there are configurations for VLANs 5, 10, and 20, but none of these are the default VLAN. The native VLAN for the trunk links has been changed to VLAN 10, but this does not change the default VLAN of the switch itself, which remains as VLAN 1.

Q181: Which two circumstances can prevent two routers from establishing an OSPF neighbor adjacency? (Choose two.)

- A. mismatched autonomous system numbers
- B. an ACL blocking traffic from multicast address 224.0.0.10
- C. mismatched process IDs
- D. mismatched hello timers and dead timers
- E. use of the same router ID on both devices

▼ Answer

- A. mismatched autonomous system numbers
- B. an ACL blocking traffic from multicast address 224.0.0.10
- C. mismatched process IDs
- D. mismatched hello timers and dead timers**
- E. use of the same router ID on both devices**



More details Steps:

Explanation:

D. OSPF Hello and Dead timers must match between neighbors. If these values do not match, OSPF will not form a neighbor relationship. Hello packets are used by OSPF to establish and maintain neighbor relationships. The Hello timer specifies how frequently these packets are sent. The Dead timer is the time that an OSPF router will wait to receive a Hello packet from a neighbor before declaring the neighbor down.

E. Each router in an OSPF deployment must have a unique Router ID. If two routers are configured with the same Router ID, they cannot establish adjacency. The Router ID is an IP address used to identify the router and is chosen using the highest loopback interface or the highest active IP address on the router.

other options:

A. Mismatched autonomous system numbers: Autonomous System numbers are associated with BGP (Border Gateway Protocol), not OSPF. OSPF uses areas for its topology, not autonomous system numbers. So, mismatched autonomous system numbers would not prevent OSPF neighbor relationships.

B. An ACL blocking traffic from multicast address 224.0.0.10: While this statement is technically true because OSPF uses the 224.0.0.5 and 224.0.0.6 multicast addresses to send hello packets and link-state updates, it's often considered a bit of a trick answer. In actual practice, it is very rare to see an Access Control List (ACL) blocking OSPF multicast addresses, because doing so would effectively disable OSPF.

C. Mismatched process IDs: In OSPF, the process ID is locally significant, which means it's only relevant to the local router and doesn't have to match on neighboring routers. Routers with different OSPF process IDs can form neighbor relationships with each other.

Q182: Which two statements about eBGP neighbor relationships are true? (Choose two.)

- A. The two devices must reside in different autonomous systems
- B. Neighbors must be specifically declared in the configuration of each device
- C. They can be created dynamically after the network statement is configured
- D. The two devices must reside in the same autonomous system
- E. The two devices must have matching timer settings

▼ Answer

- A. The two devices must reside in different autonomous systems**
- B. Neighbors must be specifically declared in the configuration of each device**
- C. They can be created dynamically after the network statement is configured
- D. The two devices must reside in the same autonomous system
- E. The two devices must have matching timer settings



More details Steps:

Explanation:

A. eBGP (External Border Gateway Protocol) is used to establish connections between different autonomous systems (AS). So, for an eBGP neighbor relationship to be established, the two devices must indeed reside in different autonomous systems.

B. In BGP (both iBGP and eBGP), neighbors must be manually configured. This means the IP address of the neighboring device needs to be explicitly stated in the BGP configuration of each device. BGP does not automatically discover neighbors like some other routing protocols (like OSPF or EIGRP).

C. This statement is incorrect. BGP does not create neighbor relationships dynamically based on network statements. Neighbors must be explicitly configured.

D. This statement is incorrect. When devices reside in the same AS, iBGP (Internal Border Gateway Protocol) is used, not eBGP.

E. This statement is incorrect. Although having matching timer settings can help maintain a stable relationship, BGP does not require matching timer settings to establish a neighbor relationship.

Q183: Which two pieces of information can you determine from the output of the show ntp status command? (Choose two.)

- A. whether the NTP peer is statically configured
- B. the IP address of the peer to which the clock is synchronized
- C. the configured NTP servers
- D. whether the clock is synchronized
- E. the NTP version number of the peer.

▼ Answer

- A. whether the NTP peer is statically configured
- B. the IP address of the peer to which the clock is synchronized**
- C. the configured NTP servers
- D. whether the clock is synchronized**
- E. the NTP version number of the peer.



More details Steps:

Explanation:

- A. The `show ntp status` command doesn't directly provide information about whether the NTP peer is statically configured. It mainly gives information about the synchronization status.
- B. `show ntp status` will show the IP of the peer to which the device is synchronized. It is included in the line that starts with "system peer".
- C. The `show ntp status` command doesn't directly provide information about the configured NTP servers. To see the list of configured NTP servers, you'd use the `show ntp associations` or `show running-config` command.
- D. `show ntp status` will show whether the clock is synchronized. It will display "Clock is synchronized" if it is synced. If not, it will display "Clock is unsynchronized".
- E. The `show ntp status` command does not directly provide the NTP version number of the peer. This kind of detail is typically found by using the `show ntp associations detail` command.

Q184: Which keyword in a NAT configuration enables the use of one outside IP address for multiple inside hosts?

- A. source
- B. static
- C. pool
- D. overload.

▼ Answer

- A. source
- B. static
- C. pool
- D. overload.**



More details Steps:

Explanation:

The 'overload' keyword in NAT (Network Address Translation) configuration is used to enable PAT (Port Address Translation), which allows multiple inside hosts to share one outside IP address.

This is typically used when there are more private network hosts than public IP addresses available. Each internal host is mapped to the same public IP address, but with a different port number, allowing multiple hosts to share the same public IP address. This is sometimes referred to as "NAT Overloading".

The other options don't facilitate the use of one outside IP address for multiple inside hosts:

- A. 'source' refers to source NAT, where the source IP address is changed. It doesn't imply the use of a single IP for multiple hosts.
- B. 'static' refers to static NAT, where there is a one-to-one mapping between inside and outside addresses.
- C. 'pool' refers to a pool of outside addresses that can be used for NAT. Again, this doesn't imply the use of a single IP for multiple hosts.

Q185: Which two pieces of information can you learn by viewing the routing table? (Choose two.)

- A. whether an ACL was applied inbound or outbound to an interface
- B. the EIGRP or BGP autonomous system
- C. whether the administrative distance was manually or dynamically configured
- D. which neighbor adjacencies are established
- E. the length of time that a route has been known.

▼ Answer

- A. whether an ACL was applied inbound or outbound to an interface
- B. the EIGRP or BGP autonomous system
- C. whether the administrative distance was manually or dynamically configured**
- D. which neighbor adjacencies are established
- E. the length of time that a route has been known.**



More details Steps:

Explanation:

- C. The administrative distance is a feature used by routers to select the best path when there are two or more different routes to the same destination from two different routing protocols. The administrative distance of a route can be manually configured (i.e., it can be set by a network administrator). If it is not manually set, it will be assigned a default value based on the routing protocol (e.g., EIGRP has a default administrative distance of 90). The routing table does not explicitly tell you whether the administrative distance was manually or dynamically configured, but by knowing the default administrative distances for the various routing protocols, you can infer this information.
- E. The routing table shows the length of time that a route has been known. This is sometimes referred to as the "uptime" for the route. The time starts counting from when the route was first learned by the router.
- A. Whether an ACL was applied inbound or outbound to an interface: Access Control Lists (ACLs) are used to filter traffic and control network access. However, information about whether an ACL is applied to an interface, and in which direction, is not indicated in the routing table. You would typically use commands like `show ip access-lists` or `show running-config` to gather this information.
- B. The EIGRP or BGP autonomous system: While it's true that the routing table displays routes from various protocols including EIGRP and BGP, the autonomous system number (AS) associated with these protocols is not typically displayed in the routing table itself. You would use other commands, such as `show ip protocols`, `show ip bgp summary`, or `show ip eigrp neighbors`, to find out the AS number.
- D. Which neighbor adjacencies are established: The routing table shows you which routes are currently in use, but it does not provide information about which neighbor adjacencies are established. Information about neighbor adjacencies can be found using protocol-specific commands, such as `show ip ospf neighbor` for OSPF or `show ip eigrp neighbors` for EIGRP.

Q186: Which NAT term is defined as a group of addresses available for NAT use?

- A. NAT pool
- B. dynamic NAT
- C. static NAT
- D. one-way NAT

▼ Answer

- A. NAT pool**
- B. dynamic NAT
- C. static NAT
- D. one-way NAT



More details Steps:

Explanation:

- A. 'NAT pool' refers to a group of IP addresses that are available for use in Network Address Translation (NAT). This pool of addresses is typically used in dynamic NAT configurations.
- B. 'Dynamic NAT' is a type of NAT where multiple unregistered (inside, local) IP addresses are mapped to multiple registered (outside, global) IP addresses from a pool of registered IP addresses.
- C. 'Static NAT' is a type of NAT where there is a one-to-one mapping between local and global addresses. It's typically used when a device needs to be accessible from the outside world, such as a web server.
- D. 'One-way NAT' is a term to describe a NAT setup where translations work in one direction but not the other. This is not a term used to describe a group of addresses available for NAT use.

Q187: Which command is used to enable LLDP globally on a Cisco IOS ISR?

- A. lldp run
- B. lldp enable
- C. lldp transmit
- D. cdp run
- E. cdp enable

▼ Answer

A. lldp run

- B. lldp enable
- C. lldp transmit
- D. cdp run
- E. cdp enable



More details Steps:

Explanation:

- A. The `lldp run` command is used to enable Link Layer Discovery Protocol (LLDP) globally on a Cisco IOS device.
- B. There is no `lldp enable` command in Cisco IOS.
- C. `lldp transmit` is not a valid command in Cisco IOS.
- D. `cdp run` is used to enable Cisco Discovery Protocol (CDP), not LLDP. CDP is a Cisco proprietary protocol, while LLDP is an industry-standard protocol.
- E. There is no `cdp enable` command in Cisco IOS. You would use `cdp run` to enable CDP globally, or `cdp enable` on a specific interface to enable CDP on that interface.

Q188: Refer to the exhibit. After you apply the given configurations to R1 and R2 you notice that OSPFv3 fails to start.

```
R1
ipv6 unicast-routing

interface FastEthernet0/0
    no ip address
    ipv6 enable
        ipv6 address 3001:DBB:13::1/64
        ipv6 ospf 1 area 0
    ipv6 router ospf 1
    router-id 172.16.1.1

R2
ipv6 unicast-routing

interface FastEthernet0/0
    no ip address
    ipv6 enable
        ipv6 address 2001:DBB:12::12/64
        ipv6 ospf 1 area 3
    ipv6 router ospf 1
    router-id 172.16.3.3
```

- A. The area numbers on R1 and R2 are mismatched
- B. The IPv6 network addresses on R1 and R2 are mismatched
- C. The autonomous system numbers on R1 and R2 are mismatched
- D. The router ids on R1 and R2 are mismatched

▼ Answer

A. The area numbers on R1 and R2 are mismatched

- B. The IPv6 network addresses on R1 and R2 are mismatched
- C. The autonomous system numbers on R1 and R2 are mismatched
- D. The router ids on R1 and R2 are mismatched



More details Steps:

Explanation:

In your setup, R1 is configured to be in area 0 (`ipv6 ospf 1 area 0`) and R2 is configured to be in area 3 (`ipv6 ospf 1 area 3`). For OSPFv3 to form adjacency and exchange routes, both routers need to be in the same OSPF area on the connecting interface.

The other options are not the cause of the issue:

- B. The IPv6 network addresses do not need to be the same for OSPFv3 to start. OSPFv3, like OSPFv2, is a link-state protocol that can exchange routes of different networks.
- C. The autonomous system numbers are not mismatched. Both R1 and R2 are using the same OSPF process ID of 1 (`ipv6 router ospf 1`).
- D. The router IDs do not need to be the same for OSPFv3 to start. In fact, they should be unique per router. Here, R1 has a router ID of 172.16.1.1 and R2 has a router ID of 172.16.3.3, which is the correct configuration.

Soultion

R1 ----- R2 ----- R3

- R1 and R2 are connected (e.g., on the left side), and they belong to Area 0.
- R2 and R3 are connected (e.g., on the right side), and they belong to Area 3.

Q189: Which command must be entered when a device is configured as an NTP server?

- A. `ntp peer`
- B. `ntp master`
- C. `ntp authenticate`
- D. `ntp server`

▼ Answer

- A. `ntp peer`
- B. `ntp master`**
- C. `ntp authenticate`
- D. `ntp server`



More details Steps:

Explanation:

To configure a device as an NTP (Network Time Protocol) server, you would use the `ntp master` command in global configuration mode. This command configures the device to act as an NTP master clock, which other devices can use as their time source.

- A. `ntp peer` is used to configure the device to establish a peer relationship with another NTP device.
- C. `ntp authenticate` enables the NTP authentication feature, which is used to ensure the authenticity of received NTP time updates.
- D. `ntp server` is used to configure the device to synchronize its clock with a specified NTP server. It's used when the device is a client, not a server.

Q190: Which feature or protocol determines whether the QoS on the network is sufficient to support IP services?

- A. LLDP
- B. CDP
- C. IP SLA
- D. EEM.

▼ Answer

- A. LLDP
- B. CDP
- C. IP SLA**
- D. EEM.



More details Steps:

Explanation:

IP SLA (IP Service Level Agreement) is a feature set of the Cisco IOS that allows administrators to collect information about network performance in real time. With IP SLA, you can analyze performance metrics such as network latency, packet loss, jitter and many more, which are critical for determining the Quality of Service (QoS) on the network.

- A. LLDP (Link Layer Discovery Protocol) is a vendor-neutral link layer protocol used by network devices for advertising their identity and capabilities to neighbors on a LAN.
- B. CDP (Cisco Discovery Protocol) is a proprietary protocol designed by Cisco to help administrators collect information about both locally attached and remote devices.
- C. EEM (Embedded Event Manager) is a technology that allows you to automate tasks on your Cisco device. It can react to certain events and execute predefined tasks, but it doesn't determine the QoS.

Q191: Refer to the exhibit. Which feature is enabled by this configuration?

```
R1(config)#ip nat pool cisco 10.1.1.0 10.1.1.50 255.255.255.0
```

- A. static NAT translation
- B. a DHCP pool
- C. a dynamic NAT address pool
- D. PAT

▼ Answer

- A. static NAT translation
- B. a DHCP pool
- C. a dynamic NAT address pool**
- D. PAT



More details Steps:

Explanation:

The configuration `ip nat pool cisco 10.1.1.0 10.1.1.50 255.255.255.0` is used to define a pool of addresses for dynamic NAT (Network Address Translation) on a Cisco IOS device.

- A. Static NAT translation involves a one-to-one mapping between local and global addresses. It's not what's being configured here.
- B. A DHCP pool is used for dynamically allocating IP addresses to hosts on a network. The `ip nat pool` command does not configure a DHCP pool.
- D. PAT (Port Address Translation) allows multiple devices on a local network to be mapped to a single public IP address. While NAT and PAT are related, the given configuration defines a pool of addresses for dynamic NAT, not PAT. PAT would involve the use of a single IP address or a few IP addresses, not a range as indicated here.

Q192: In a CDP environment, what happens when the CDP interface on an adjacent device is configured without an IP address?

- A. CDP becomes inoperable on that neighbor
- B. CDP uses the IP address of another interface for that neighbor
- C. CDP operates normally, but it cannot provide IP address information for that neighbor
- D. CDP operates normally, but it cannot provide any information for that neighbor

▼ Answer

- A. CDP becomes inoperable on that neighbor
- B. CDP uses the IP address of another interface for that neighbor
- C. CDP operates normally, but it cannot provide IP address information for that neighbor**
- D. CDP operates normally, but it cannot provide any information for that neighbor



More details Steps:

Explanation:

CDP (Cisco Discovery Protocol) is a layer 2 protocol used to share information about directly connected Cisco devices. CDP can share a variety of information, including device ID, software version, platform, capabilities, and interface IP addresses.

If the CDP interface on a neighbor device is configured without an IP address, CDP can still operate normally and share other information about the device. However, it will not be able to provide IP address information for that interface because it doesn't have one. Therefore, while CDP can still discover the device and collect other information, it will not be able to provide IP address information for that specific interface.

Q193: Which two statements about NTP operations are true? (Choose two.)

- A. NTP uses UDP over IP.
- B. Cisco routers can act as both NTP authoritative servers and NTP clients.
- C. Cisco routers can act only as NTP servers.
- D. Cisco routers can act only as NTP clients.
- E. NTP uses TCP over IP.

▼ Answer

- A. NTP uses UDP over IP.**
- B. Cisco routers can act as both NTP authoritative servers and NTP clients.**
- C. Cisco routers can act only as NTP servers.
- D. Cisco routers can act only as NTP clients.
- E. NTP uses TCP over IP.



More details Steps:

Explanation:

- A. NTP (Network Time Protocol) operates over UDP (User Datagram Protocol), using port 123. Therefore, it's correct to say that NTP uses UDP over IP.
- B. Cisco routers can indeed act as both NTP authoritative servers and NTP clients. As NTP servers, they can provide the time to other devices. As NTP clients, they can receive the time from an NTP server.
- C. It's incorrect to say that Cisco routers can only act as NTP servers. As mentioned above, they can also act as NTP clients.
- D. Likewise, it's incorrect to say that Cisco routers can only act as NTP clients. They can also act as NTP servers.
- E. NTP does not use TCP over IP. As mentioned above, NTP operates over UDP.

Q194: Which command should you enter to configure an LLDP delay time of 5 seconds?

- A. `lldp timer 5000`
- B. `lldp holdtime 5`
- C. `lldp reinit 5000`
- D. `lldp reinit 5`

▼ Answer

- A. `lldp timer 5000`
- B. `lldp holdtime 5`
- C. `lldp reinit 5000`
- D. lldp reinit 5**



More details Steps:

Explanation:

The `lldp reinit` command is used to set the delay time for LLDP (Link Layer Discovery Protocol) to initialize (or reinitialize) on an interface. The delay time is specified in seconds, so `lldp reinit 5` sets a delay time of 5 seconds.

- A. `lldp timer` is used to set the transmission frequency (how often LLDP updates are sent), not the delay time. And it's specified in seconds, not milliseconds, so `lldp timer 5000` would set a transmission frequency of 5000 seconds, not a delay time.
- B. `lldp holdtime` is used to specify how long a receiving device should hold the information received from a neighbor before discarding it. It's not used to set the delay time.
- C. `lldp reinit 5000` would set a delay time of 5000 seconds, which is not the same as 5 seconds.

Q195: Which value is used to determine the active router in an HSRP default configuration?

- A. Router loopback address
- B. Router IP address
- C. Router priority
- D. Router tracking number

▼ Answer

- A. Router loopback address
- B. Router IP address**
- C. Router priority
- D. Router tracking number



More details Steps:

Explanation:

In an HSRP (Hot Standby Router Protocol) configuration, if no priorities are explicitly set, the router with the highest IP address on the HSRP-configured interface becomes the active router. This is indeed the default behavior when no other configuration changes are made.

Q196: Which statement about Cisco Discovery Protocol is true?

- A. It is a Cisco-proprietary protocol.
- B. It runs on the network layer.
- C. It can discover information from routers, firewalls, and switches.
- D. It runs on the physical layer and the data link layer.

▼ Answer

A. It is a Cisco-proprietary protocol.

- B. It runs on the network layer.
- C. It can discover information from routers, firewalls, and switches.
- D. It runs on the physical layer and the data link layer.



More details Steps:

Explanation:

- A. Cisco Discovery Protocol (CDP) is indeed a Cisco-proprietary protocol. It's used to discover information about directly connected Cisco devices.
- B. CDP operates at the Data Link layer (Layer 2) of the OSI model, not the Network layer (Layer 3).
- C. While CDP can discover information from routers, switches, and other network devices, it's not limited to just Cisco devices. Other vendors' devices that support CDP can also be discovered, so this statement is not entirely accurate.
- D. CDP operates at the Data Link layer (Layer 2) of the OSI model, not the Physical layer (Layer 1). It uses the source MAC address to identify the sending device, which is a Layer 2 function.

Q197: Which value can you modify to configure a specific interface as the preferred forwarding interface?

- A. The interface number
- B. The port priority
- C. The VLAN priority
- D. The hello time

▼ Answer

- A. The interface number

B. The port priority

- C. The VLAN priority
- D. The hello time



More details Steps:

Explanation:

In certain network protocols such as Spanning Tree Protocol (STP), you can modify the port priority to influence which interface is chosen as the preferred forwarding interface. The interface with the lower port priority value has a higher chance of being selected as the forwarding port.

- A. The interface number is a fixed attribute determined by the device and cannot be modified to influence forwarding decisions.
- C. VLAN priority (or priority level) can be used in some cases to prioritize traffic, but it's not typically used to select a preferred forwarding interface.
- D. The hello time is a parameter used in various network protocols to determine the frequency of certain types of communication (like sending hello packets), but it doesn't typically influence the selection of a preferred forwarding interface.

Q198: When configuring an EtherChannel bundle, which mode enables LACP only if a LACP device is detected?

- A. Passive
- B. Desirable
- C. On
- D. Auto
- E. Active

▼ Answer

A. Passive

- B. Desirable
- C. On
- D. Auto
- E. Active



More details Steps:

Explanation:

When configuring Link Aggregation Control Protocol (LACP) as part of an EtherChannel bundle on Cisco devices, the `passive` mode enables LACP only if an LACP device is detected.

- A. `Passive`: In this mode, the interface responds to LACP packets that it receives but does not initiate LACP packet negotiation.
- B. `Desirable`: This is a PAgP term (Cisco's proprietary protocol similar to LACP), not an LACP mode.
- C. `on`: This forces the interface to channel without LACP or PAgP. With the `on` mode, a functional EtherChannel exists only when an interface group in `on` mode is connected to another interface group in `on` mode.
- D. `Auto`: This is a PAgP term, not an LACP mode.
- E. `Active`: In this mode, the interface is in an active negotiating state, in which the interface initiates negotiations with interfaces by sending LACP packets.

Q199: Which command should you enter to verify the priority of a router in an HSRP group?

- A. show hsrp
- B. show sessions
- C. show interfaces
- D. show standby.

▼ Answer

- A. show hsrp
- B. show sessions
- C. show interfaces
- D. show standby.**



More details Steps:

Explanation:

The `show standby` command is used on a Cisco router to display information about the Hot Standby Router Protocol (HSRP) groups, including the priority of the router in the HSRP group.

- A. The `show hsrp` command is not a valid Cisco IOS command.
- B. The `show sessions` command is used to display information about Telnet and SSH connections, not HSRP groups.
- C. The `show interfaces` command is used to display information about the router's interfaces, but it doesn't specifically provide information about HSRP group priorities.

Q200: Refer to the exhibit. Which Command do you enter so that R1 advertises the loopback0 interface to the BGP Peers?

```
R1
interface Loopback0
    ip address 172.16.1.33 255.255.255.224

interface FastEthernet0/0
    ip address 192.168.12.1 255.255.255.0

router bgp 100
    neighbor 192.168.12.2 remote-as 100
```

- A. Network 172.16.1.32 mask 255.255.255.224
- B. Network 172.16.1.0 0.0.0.255
- C. Network 172.16.1.32 255.255.255.224
- D. Network 172.16.1.33 mask 255.255.255.224
- E. Network 172.16.1.32 mask 0.0.0.31
- F. Network 172.16.1.32 0.0.0.31

▼ Answer

A. Network 172.16.1.32 mask 255.255.255.224

- B. Network 172.16.1.0 0.0.0.255
- C. Network 172.16.1.32 255.255.255.224
- D. Network 172.16.1.33 mask 255.255.255.224
- E. Network 172.16.1.32 mask 0.0.0.31
- F. Network 172.16.1.32 0.0.0.31



More details Steps:

When using the `network` command in BGP, we need to specify the network address, not the exact IP address of the interface. The network address is the first IP address in the subnet.

Given the IP address 172.16.1.33 and the subnet mask 255.255.255.224, the network address is 172.16.1.32.

So, the correct command to advertise the Loopback0 interface to BGP peers is:

- A. Network 172.16.1.32 mask 255.255.255.224

Q201: For what two purposes does the Ethernet protocol use physical addresses?

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

▼ Answer

A. to uniquely identify devices at Layer 2

- B. to allow communication with devices on a different network
- C. to differentiate a Layer 2 frame from a Layer 3 packet
- D. to establish a priority system to determine which device gets to transmit first

E. to allow communication between different devices on the same network

- F. to allow detection of a remote device when its physical address is unknown.



More details Steps:

Explanation:

- A. Physical addresses (also known as MAC addresses) are used to uniquely identify devices at Layer 2 of the OSI model. Each network interface controller has a unique MAC address.
- E. MAC addresses are used to allow communication between different devices on the same network. They are used to direct data to the appropriate device on a local network.
- B. Communication with devices on a different network is typically managed at Layer 3 (the Network layer) using IP addresses, not physical addresses.
- C. The differentiation between a Layer 2 frame and a Layer 3 packet is determined by the information contained within the Ethernet frame or IP packet, not the physical address.
- D. Ethernet does not use physical addresses to establish a priority system for transmission.
- F. Detection of a remote device when its physical address is unknown is not typically a function performed using physical addresses.

Q202: Which command is used to display the collection of OSPF link states?

- A. show ip ospf link-state
- B. show ip ospf lsa database
- C. show ip ospf neighbors
- D. show ip ospf database.

▼ Answer

- A. show ip ospf link-state
- B. show ip ospf lsa database
- C. show ip ospf neighbors
- D. show ip ospf database.**



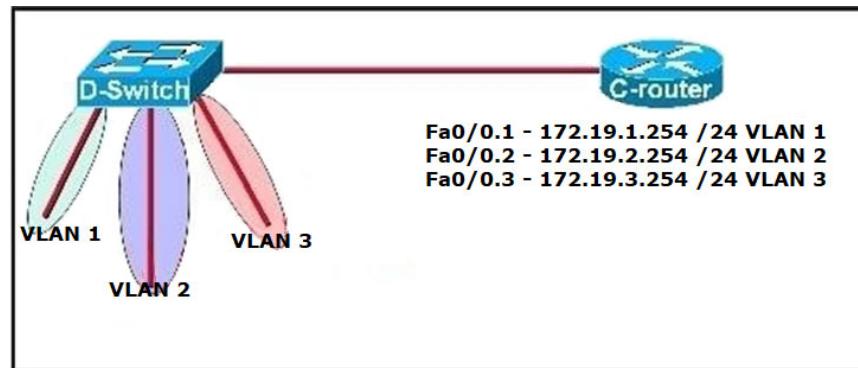
More details Steps:

Explanation:

The `show ip ospf database` command is used to display the collection of OSPF link states. This command shows the Open Shortest Path First (OSPF) Link-State Advertisement (LSA) database, which contains all the link-state information for the OSPF network.

- A. The `show ip ospf link-state` is not a valid Cisco IOS command.
- B. The `show ip ospf lsa database` is not a valid Cisco IOS command.
- C. The `show ip ospf neighbors` command displays OSPF-related information about OSPF adjacencies (neighbors), not the link-state database.

Q203: Refer to the exhibit. C-router is to be used as a "router-on-a-stick" to route between the VLANs. All the interfaces have been properly configured and IP routing is operational. The hosts in the VLANs have been configured with the appropriate default gateway. What is true about this configuration?



- A. These commands need to be added to the configuration: C-router(config)# router eigrp 123 C-router(config-router)# network 172.19.0.0
- B. These commands need to be added to the configuration: C-router(config)# router ospf 1 C-router(config-router)# network 172.19.0.0 0.0.3.255 area 0
- C. These commands need to be added to the configuration: C-router(config)# router rip C-router(config-router)# network 172.19.0.0
- D. No further routing configuration is required.

▼ Answer

- A. These commands need to be added to the configuration: C-router(config)# router eigrp 123 C-router(config-router)# network 172.19.0.0
- B. These commands need to be added to the configuration: C-router(config)# router ospf 1 C-router(config-router)# network 172.19.0.0 0.0.3.255 area 0
- C. These commands need to be added to the configuration: C-router(config)# router rip C-router(config-router)# network 172.19.0.0
- D. No further routing configuration is required.**



More details Steps:

Explanation:

In a "router-on-a-stick" configuration, the router is capable of routing between multiple VLANs on a single interface. This is accomplished by configuring sub-interfaces on the router's physical interface and assigning each sub-interface to a different VLAN. The router uses the IP address assigned to each sub-interface to route between the VLANs.

In the given configuration, the C-router has been properly set with sub-interfaces for VLAN 1, VLAN 2, and VLAN 3, each with the appropriate IP address. Therefore, no further routing configuration is needed for the router to route between these VLANs.

The router will use the sub-interfaces and their associated IP addresses to route between the VLANs. The hosts in the VLANs use the IP address of the corresponding sub-interface as their default gateway.

Remember, the router needs to have routing enabled (which the question states is operational), and each host needs to be configured with the correct default gateway.

The other options (A, B, and C) involve adding routing protocols (EIGRP, OSPF, and RIP respectively) to the configuration, but these are not necessary for the router to route between the VLANs. These protocols would be used if the router needed to share its routing information with other routers, but there's no indication in the question that this is required.

Q204: A user configured OSPF in a single area between two routers A serial interface connecting R1 and R2 is running encapsulation PPP. By default which OSPF network type is seen on this interface when the user types show ip ospf interface on R1 or R2?

- A. port-to-multipoint
- B. broadcast
- C. point-to-point
- D. non-broadcast

▼ Answer

- A. port-to-multipoint
- B. broadcast
- C. point-to-point**
- D. non-broadcast



More details Steps:

Explanation:

By default, OSPF treats all serial interfaces configured with HDLC or PPP encapsulation as point-to-point connections.

A point-to-point OSPF network type is used between two routers when there is a direct connection between them, which is the case when using a serial interface with PPP encapsulation.

- A. The point-to-multipoint OSPF network type is used in hub-and-spoke topologies, not default for serial interfaces.
- B. The broadcast OSPF network type is the default on Ethernet and other broadcast capable multi-access networks, not on serial interfaces.
- D. The non-broadcast OSPF network type is typically used in Frame Relay or other non-broadcast multi-access (NBMA) networks. It is not the default for serial interfaces.

Q205: Refer to the exhibit. Which address and mask combination represents a summary of the routes learned by EIGRP?

Gateway of last resort is not set

192.168.25.0/30 is subnetted, 4 subnets

- D 192.168.25.20 [90/2681856] via 192.168.15.5, 00:00:10, Serial0/1
- D 192.168.25.16 [90/1823638] via 192.168.15.5, 00:00:50, Serial0/1
- D 192.168.25.24 [90/3837233] via 192.168.15.5, 00:05:23, Serial0/1
- D 192.168.25.28 [90/8127323] via 192.168.15.5, 00:06:45, Serial0/1
- C 192.168.15.4/30 is directly connected, Serial0/1
- C 192.168.2.0/24 is directly connected, FastEthernet0/0

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

▼ Answer

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



More details Steps:

Explanation:

The question seems to be asking for a summary route that includes all the given subnets. We have four subnets in the 192.168.25.0/24 network: 192.168.25.0/30, 192.168.25.16/30, 192.168.25.20/30, and 192.168.25.24/30.

A /30 subnet has a subnet mask of 255.255.255.252, which allows for 2 usable IP addresses. But the four subnets we have don't fit into a /30, /29, or /28 mask.

A /28 subnet has a subnet mask of 255.255.255.240, which allows for 14 usable IP addresses. The network 192.168.25.0 with a /28 mask (255.255.255.240) will include the addresses from 192.168.25.0 to 192.168.25.15, which encompasses our four subnets. So the correct answer is 192.168.25.0 255.255.255.240.

The other options (B, C, D, E, and F) either do not encompass all four subnets or do not represent a summary route.

Q206: Refer to the exhibit. A network associate has configured OSPF with the command: City(config-router)# network 192.168.12.64 0.0.0.63 area 0.

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

City#show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	192.168.12.48	Yes	manual	up	up
FastEthernet0/1	192.168.12.65	Yes	manual	up	up
Serial0/0	192.168.12.121	Yes	manual	up	up
Seriak0/1	unassigned	Yes	unset	up	up
Serial0/1.102	192.168.12.125	Yes	manual	up	up
Serial0/1.103	192.168.12.129	Yes	manual	up	up
Serial0/1.104	192.168.12.133	Yes	manual	up	up

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

▼ Answer

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



More details Steps:

The network range for the network 192.168.12.64 0.0.0.63 is 192.168.12.64 to 192.168.12.127.

If we look at the IP addresses of the interfaces:

- FastEthernet0/0: 192.168.12.65 (Not in range)
- FastEthernet0/1: 192.168.12.121 (In range)
- Serial0/0: Unassigned
- Serial0/1: Unassigned
- Serial0/1.102: 192.168.12.125 (In range)
- Serial0/1.103: 192.168.12.129 (Not in range)
- Serial0/1.104: 192.168.12.133 (Not in range)

Q207: A network administrator is troubleshooting the OSPF configuration of routers R1 and R2. The routers cannot establish an adjacency relationship on their common Ethernet link. The graphic shows the output of the show ip ospf interface e0 command for routers R1 and R2. Based on the information in the graphic, what is the cause of this problem?

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

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

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

▼ Answer

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



More details Steps:

Explanation:

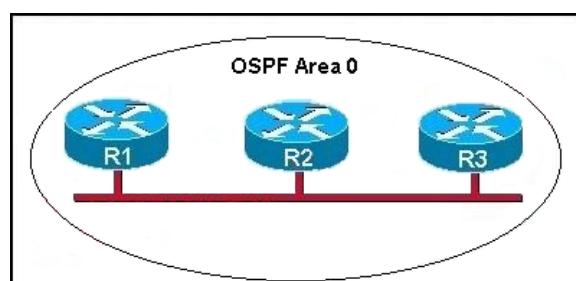
OSPF routers must have matching hello and dead intervals in order to form an adjacency. The hello interval specifies how often the router sends hello packets, and the dead interval specifies how long the router waits to hear a hello before it declares the OSPF neighbor as down.

In the provided output, we can see that on R1 the hello interval is 5 and the dead interval is 20, while on R2 the hello interval is 10 and the dead interval is 40. Because these intervals do not match, the two routers cannot establish an OSPF adjacency.

The other options:

- A. The OSPF area is configured properly as both are in Area 0.
- B. The priority on R1 does not need to be set higher. Both routers have the same priority, and priority only becomes an issue when selecting the designated router.
- C. The cost on R1 does not need to be set higher. The costs are the same and would not prevent an adjacency.
- E. A backup designated router is not required for an adjacency to be established.
- F. The OSPF process ID numbers do not have to match. They are locally significant and do not prevent an adjacency.

Q208: Refer to the graphic. R1 is unable to establish an OSPF neighbor relationship with R3. What are possible reasons for this problem? (Choose two.)



- A. All of the routers need to be configured for backbone Area 1.
- B. R1 and R2 are the DR and BDR, so OSPF will not establish neighbor adjacency with R3.
- C. A static route has been configured from R1 to R3 and prevents the neighbor adjacency from being established.
- D. The hello and dead interval timers are not set to the same values on R1 and R3.
- E. EIGRP is also configured on these routers with a lower administrative distance.
- F. R1 and R3 are configured in different areas.

▼ Answer

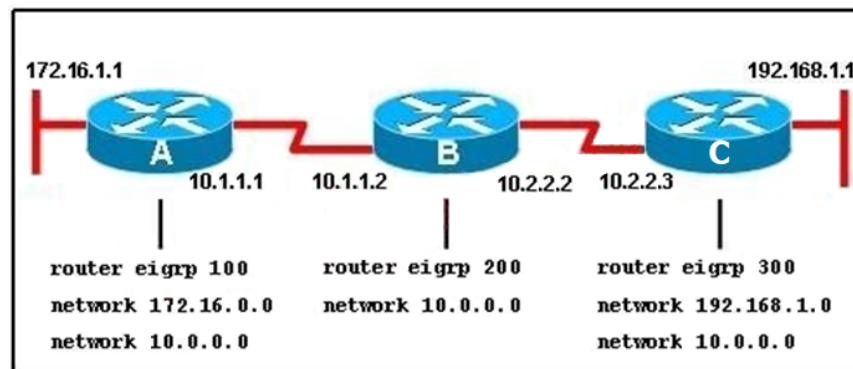
- A. All of the routers need to be configured for backbone Area 1.
- B. R1 and R2 are the DR and BDR, so OSPF will not establish neighbor adjacency with R3.
- C. A static route has been configured from R1 to R3 and prevents the neighbor adjacency from being established.
- D. The hello and dead interval timers are not set to the same values on R1 and R3.**
- E. EIGRP is also configured on these routers with a lower administrative distance.
- F. R1 and R3 are configured in different areas.**



More details Steps:

- D. The hello and dead interval timers are not set to the same values on both routers. These timers must match on both routers for the OSPF neighbor adjacency to be established.
 - F. The routers are configured in different areas. In OSPF, only routers in the same area can form a neighbor relationship.
- Let's analyze the other options:
- A. Not all routers need to be in the backbone area (Area 0 in OSPF). Routers in different areas can still form OSPF adjacencies, provided that those areas are connected to the backbone area.
 - B. The DR and BDR are only relevant on multiaccess networks (like Ethernet). They will not prevent OSPF from establishing neighbor relationships with other routers.
 - C. A static route would not prevent an OSPF adjacency. In fact, static routes and OSPF can coexist.
 - E. The presence of EIGRP with a lower administrative distance will not prevent OSPF from establishing neighbor relationships. It might affect the routing table and the path of the traffic, but it won't stop OSPF adjacencies.

Q209: Refer to the exhibit. When running EIGRP, what is required for RouterA to exchange routing updates with RouterC?



- A. AS numbers must be changed to match on all the routers
- B. Loopback interfaces must be configured so a DR is elected
- C. The no auto-summary command is needed on Router A and Router C
- D. Router B needs to have two network statements, one for each connected network

▼ Answer

- A. AS numbers must be changed to match on all the routers**
- B. Loopback interfaces must be configured so a DR is elected
- C. The no auto-summary command is needed on Router A and Router C
- D. Router B needs to have two network statements, one for each connected network



More details Steps:

In EIGRP (Enhanced Interior Gateway Routing Protocol), for routers to exchange routing updates, they must be in the same autonomous system (AS). That's the main way routers running EIGRP identify each other as being in the same routing domain.

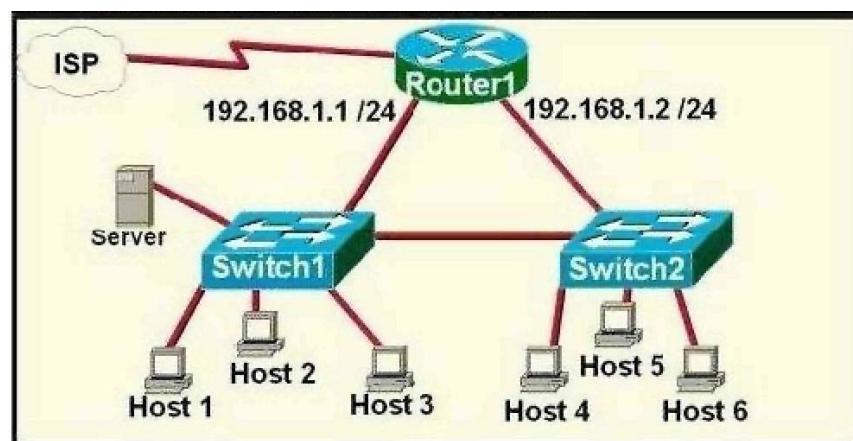
In the exhibit, RouterA is running EIGRP in AS 100, RouterB is running EIGRP in AS 200, and RouterC is running EIGRP in AS 300. Also, RouterB has the network statement `network 10.0.0.0` under both AS 100 and AS 300, which means it's able to exchange routes with both RouterA and RouterC.

However, for RouterA and RouterC to exchange routes, they must be part of the same AS. Thus, the correct answer is:

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

In order to facilitate communication between RouterA and RouterC, either the AS number on RouterA or RouterC (or both) must be changed so they match. RouterB already has network statements in both AS, so it can facilitate the route exchange once RouterA and RouterC are in the same AS.

Q210: Refer to the exhibit. A network technician is asked to design a small network with redundancy. The exhibit represents this design, with all hosts configured in the same VLAN. What conclusions can be made about this design?



- A. This design will function as intended.
- B. Spanning-tree will need to be used.
- C. The router will not accept the addressing scheme.
- D. The connection between switches should be a trunk.
- E. The router interfaces must be encapsulated with the 802.1Q protocol.

▼ Answer

- A. This design will function as intended.
- B. Spanning-tree will need to be used.
- C. The router will not accept the addressing scheme.**
- D. The connection between switches should be a trunk.
- E. The router interfaces must be encapsulated with the 802.1Q protocol.



More details Steps:

this could be due to an IP addressing conflict, or perhaps the router has been configured with a different subnet than what's being used in the network design. However, without additional context or information, it's hard to definitively say why the router would not accept the addressing scheme based on the provided exhibit.

Remember, in a typical scenario, routers should be able to accept a wide range of addressing schemes as long as they are correctly configured and the network design adheres to standard IP networking principles.

Q211: What benefit does controller-based networking provide versus traditional networking?

- A. moves from a two-tier to a three-tier network architecture to provide maximum redundancy
- B. provides an added layer of security to protect from DDoS attacks
- C. allows configuration and monitoring of the network from one centralized port
- D. combines control and data plane functionality on a single device to minimize latency

▼ Answer

- A. moves from a two-tier to a three-tier network architecture to provide maximum redundancy
- B. provides an added layer of security to protect from DDoS attacks
- C. allows configuration and monitoring of the network from one centralized port**
- D. combines control and data plane functionality on a single device to minimize latency



More details Steps:

Controller-based networking, also known as Software-Defined Networking (SDN), separates the control plane from the data plane and centralizes network control. This allows for a more flexible and programmable network, which can be managed and configured from a single point.

Therefore, the correct answer is:

C. allows configuration and monitoring of the network from one centralized point

Here's why the other options are incorrect:

- **A. moves from a two-tier to a three-tier network architecture to provide maximum redundancy:** Controller-based networking doesn't inherently change the network architecture tiers. It's about centralizing control, not changing the architecture.
- **B. provides an added layer of security to protect from DDoS attacks:** While SDN can enhance security through centralized control and visibility, it doesn't inherently provide an added layer of DDoS protection.
- **D. combines control and data plane functionality on a single device to minimize latency:** This is actually the opposite of what controller-based networking does. It separates the control plane from the data plane, with the control plane centralized in the controller.

Q212: A network engineer must create a diagram of a multivendor network. Which command must be configured on the Cisco devices so that the topology of the network can be mapped?

- A. Device(config)#lldp run
- B. Device(config)#cdp run
- C. Device(config-if)#cdp enable
- D. Device(config)#flow-sampler-map topology

▼ Answer

- A. Device(config)#lldp run**
- B. Device(config)#cdp run
- C. Device(config-if)#cdp enable
- D. Device(config)#flow-sampler-map topology



More details Steps:

To map the topology of a multivendor network, you'd need a protocol that works across different network device vendors. Cisco Discovery Protocol (CDP) is proprietary and only works on Cisco devices. In contrast, Link Layer Discovery Protocol (LLDP) is a vendor-neutral protocol that can discover multivendor devices connected to a network.

Therefore, the command you need to configure on Cisco devices to allow the topology of the network to be mapped is:

A. Device(config)#lldp run

This command enables LLDP globally on the device, allowing it to discover and be discovered by other devices that also have LLDP enabled, regardless of their manufacturer.

The other options are either Cisco-specific (B and C) or not directly related to network topology mapping (D).

Q213: What are two descriptions of three-tier network topologies? (Choose two)

- A. The core and distribution layers perform the same functions
- B. The access layer manages routing between devices in different domains
- C. The network core is designed to maintain continuous connectivity when devices fail.
- D. The core layer maintains wired connections for each host
- E. The distribution layer runs Layer 2 and Layer 3 technologies

▼ Answer

- A. The core and distribution layers perform the same functions
- B. The access layer manages routing between devices in different domains
- C. The network core is designed to maintain continuous connectivity when devices fail.**
- D. The core layer maintains wired connections for each host
- E. The distribution layer runs Layer 2 and Layer 3 technologies**



More details Steps:

Three-tier network topologies, commonly seen in enterprise settings, consist of a core layer, a distribution layer, and an access layer. Each of these layers has specific functions and characteristics. Based on these, two accurate descriptions would be:

C. The network core is designed to maintain continuous connectivity when devices fail.

The core layer is responsible for fast and reliable transportation of data across the network. It is designed for redundancy and high availability to maintain connectivity in case of device or link failures.

E. The distribution layer runs Layer 2 and Layer 3 technologies.

The distribution layer, also known as the aggregation layer, typically runs both Layer 2 (switching) and Layer 3 (routing) technologies. It connects the access and core layers, routing and controlling data flow between them, and can implement policies for things like access control and QoS.

The other options are not accurate:

- **A. The core and distribution layers perform the same functions.** This is not correct. Each layer in the three-tier topology has distinct functions.
- **B. The access layer manages routing between devices in different domains.** This is not typically accurate. The access layer primarily connects end devices to the network and is not usually responsible for inter-domain routing.
- **D. The core layer maintains wired connections for each host.** This is not correct. The core layer is responsible for interconnecting distribution layer devices and ensuring high-speed, reliable transport of data, not directly connecting hosts.

Q214: What is the expected outcome when an EUI-64 address is generated?

- A. The seventh bit of the original MAC address of the interface is inverted
- B. The interface ID is configured as a random 64-bit value
- C. The characters FE80 are inserted at the beginning of the MAC address of the interface
- D. The MAC address of the interface is used as the interface ID without modification

▼ Answer

- A. The seventh bit of the original MAC address of the interface is inverted**
- B. The interface ID is configured as a random 64-bit value
- C. The characters FE80 are inserted at the beginning of the MAC address of the interface
- D. The MAC address of the interface is used as the interface ID without modification



More details Steps:

EUI-64 is a method of creating an IPv6 Interface Identifier from a device's MAC address. It's commonly used in stateless address autoconfiguration (SLAAC) where IPv6 hosts generate their own addresses using a combination of locally available information and information advertised by routers.

When an EUI-64 address is generated from a 48-bit MAC address, the process involves the following steps:

1. The MAC address is split into two halves.
2. The hexadecimal value **FFFE** is inserted in the middle.
3. The seventh bit in the first byte (the "Universal/Local" or "U/L" bit) is flipped. This bit is set to 0 in globally unique MAC addresses, indicating universal scope. When generating an EUI-64 address, this bit is set to 1, indicating local scope.

Q215: Which function does an SNMP agent perform?

- A. it sends information about MIB variables in response to requests from the NMS
- B. it coordinates user authentication between a network device and a TACACS+ or RADIUS server
- C. it requests information from remote network nodes about catastrophic system events.
- D. it manages routing between Layer 3 devices in a network

▼ Answer

A. it sends information about MIB variables in response to requests from the NMS

- B. it coordinates user authentication between a network device and a TACACS+ or RADIUS server
- C. it requests information from remote network nodes about catastrophic system events.
- D. it manages routing between Layer 3 devices in a network



More details Steps:

The Simple Network Management Protocol (SNMP) is a protocol used for managing devices on IP networks. Devices that support SNMP include routers, switches, servers, workstations, printers, modem racks, and more.

An SNMP agent is a program that runs on a network device. Its primary function is to provide information about the device's Management Information Base (MIB) to an SNMP manager (also known as a Network Management System, or NMS). The MIB is a structured database of information about the device, including metrics and configuration parameters.

Therefore, the correct answer is:

A. It sends information about MIB variables in response to requests from the NMS.

The other options are not primary functions of an SNMP agent:

- **B. It coordinates user authentication between a network device and a TACACS+ or RADIUS server.** This is not a function of an SNMP agent. Authentication coordination is typically the role of an Authentication, Authorization, and Accounting (AAA) server or service.
- **C. It requests information from remote network nodes about catastrophic system events.** While an SNMP agent can send traps (unsolicited alerts) to an NMS about certain events, it doesn't request information about catastrophic system events from remote nodes.
- **D. It manages routing between Layer 3 devices in a network.** Routing management is not a function of an SNMP agent. This is typically handled by routing protocols like OSPF, EIGRP, BGP, etc.

Q216: R1 has learned route 10.10.10.0/24 via numerous routing protocols. Which route is installed?

- A. route with the lowest cost
- B. route with the next hop that has the highest IP
- C. route with the shortest prefix length
- D. route with the lowest administrative distance

▼ Answer

- A. route with the lowest cost
- B. route with the next hop that has the highest IP
- C. route with the shortest prefix length
- D. route with the lowest administrative distance**



More details Steps:

When a router learns about the same route from multiple sources or routing protocols, the decision on which route to install in the routing table is made based on the Administrative Distance (AD).

Administrative Distance is a measure of the trustworthiness of the source of the routing information. Each routing protocol is assigned a default AD. The lower the AD, the more preferable the source.

Therefore, the correct answer is:

D. Route with the lowest administrative distance.

The other options are not the primary factors in this decision:

- **A. Route with the lowest cost.** While cost or metric is a factor in route selection, it is considered only after administrative distance. If multiple routes have the same AD, then the route with the lowest cost would be chosen.
- **B. Route with the next hop that has the highest IP.** The IP address of the next hop is not a factor in route selection.
- **C. Route with the shortest prefix length.** When dealing with routes to the same network, prefix length is not a factor in route selection. However, when dealing with different networks where one network is a subnet of another, the route with the longer prefix (more specific route) would be chosen.

Q216: What is a characteristic of spine-and-leaf architecture?

- A. Each device is separated by the same number of hops
- B. It provides variable latency
- C. It provides greater predictability on STP blocked ports.
- D. Each link between leaf switches allows for higher bandwidth.

▼ Answer

- A. Each device is separated by the same number of hops**
- B. It provides variable latency
- C. It provides greater predictability on STP blocked ports.
- D. Each link between leaf switches allows for higher bandwidth.



More details Steps:

Spine-and-leaf architecture is a two-tier network topology composed of spine (backbone) switches and leaf (access) switches. It's a type of fat-tree architecture designed to minimize latency and maximize data flow between different nodes in a network.

The key characteristic described in the options provided is:

A. Each device is separated by the same number of hops.

In a spine-and-leaf architecture, all devices are equidistant to each other in terms of hops, which aids in providing predictable latency and balanced bandwidth use across the network. This is because every leaf switch (where the endpoints are connected) is interconnected through the spine switches, but not to each other.

The other options are not typical characteristics of a spine-and-leaf architecture:

- **B. It provides variable latency.** This is not correct; spine-and-leaf architecture is designed to provide consistent, predictable latency due to its equal hop count between devices.
- **C. It provides greater predictability on STP blocked ports.** This is not relevant to spine-and-leaf architecture. In fact, spine-and-leaf architectures are often used with protocols that avoid STP, like TRILL or Shortest Path Bridging, or in environments where STP is not needed because there are no loops, like in modern data center networks using VXLAN and EVPN.
- **D. Each link between leaf switches allows for higher bandwidth.** This is incorrect; in a typical spine-and-leaf architecture, the leaf switches are not directly connected to each other. They connect to the spine switches, which handle intercommunication between leaf switches.

Q217: Which action must be taken to assign a global unicast IPv6 address on an interface that is derived from the MAC address of that interface?

- A. configure a stateful DHCPv6 server on the network
- B. enable SLAAC on an interface
- C. disable the EUI-64 bit process
- D. explicitly assign a link-local address

▼ Answer

- A. configure a stateful DHCPv6 server on the network
- B. enable SLAAC on an interface**
- C. disable the EUI-64 bit process
- D. explicitly assign a link-local address



More details Steps:

The action needed to assign a global unicast IPv6 address on an interface that is derived from the MAC address of that interface is:

B. Enable SLAAC on an interface.

SLAAC stands for Stateless Address Autoconfiguration. It's a method that allows a device to automatically configure an IPv6 address for its interface using the network prefix advertised by a router and its own interface's MAC address (through the EUI-64 process).

Here's why the other options are incorrect:

- **A. Configure a stateful DHCPv6 server on the network.** While DHCPv6 can be used to assign IPv6 addresses, it does not inherently use the MAC address of the interface to generate the IPv6 address.
- **C. Disable the EUI-64 bit process.** The EUI-64 process is precisely what you want to use here. Disabling it would prevent the generation of an IPv6 address based on the MAC address.
- **D. Explicitly assign a link-local address.** While IPv6 interfaces do have link-local addresses, these are not the same as global unicast addresses and are used for different purposes. Assigning a link-local address does not satisfy the question's requirement for a global unicast address.

Q218: Refer to the exhibit. Router R1 is running three different routing protocols. Which route characteristic is used by the router to forward the packet that it receives for destination IP 172.16.32.1?

```
R1# show ip route
...
D 172.16.32.0/27      [90/2888597172] via 20.1.1.1
O 172.16.32.0/19      [110/292094] via 20.1.1.10
R 172.16.32.0/24      [120/2] via 20.1.1.3
```

- A. longest prefix
- B. metric
- C. cost
- D. administrative distance

▼ Answer

A. longest prefix

- B. metric
- C. cost
- D. administrative distance



More details Steps:

The routing table of a router stores the best paths to reach a network. When a router has to make a decision about how to route packets to a given IP address, it uses a process called "longest prefix match" to select the best route. This means the router selects the route with the most specific (longest) subnet mask that matches the destination IP.

In the provided exhibit, there are three routes to the 172.16.32.0 network, each with different subnet masks (/27, /19, /24). The destination IP 172.16.32.1 would match all these routes, but the route selected for forwarding the packet would be the one with the longest prefix.

Therefore, the correct answer is:

A. longest prefix

The other options are not the primary considerations in this case:

- **B. Metric** and **C. Cost** are considered when choosing between routes learned from the same routing protocol, and only if they have the same prefix length.
- **D. Administrative distance** is considered when choosing between routes learned from different routing protocols, and again, only if they have the same prefix length.

Q219: Router R1 must send all traffic without a matching routing-table entry to 192.168.1.1. Which configuration accomplishes this task?

```
R1#Config t
R1(config)#ip routing
R1(config)#ip route default-route 192.168.1.1

R1#Config t
R1(config)#ip routing
R1(config)#ip route 192.168.1.1 0.0.0.0 0.0.0.0

R1#Config t
R1(config)#ip routing
R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1

R1#Config t
R1(config)#ip routing
R1(config)#ip default-gateway 192.168.1.1
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

▼ Answer

- A. Option A
- B. Option B
- C. Option C**
- D. Option D



More details Steps:

The requirement here is to send all traffic that doesn't have a matching entry in the routing table to the IP address 192.168.1.1. This is accomplished by setting a default route (also known as a gateway of last resort) on the router.

The correct configuration to accomplish this task is:

Option C.

The command `ip route 0.0.0.0 0.0.0.0 192.168.1.1` sets a static default route, directing any traffic that does not have a more specific route in the routing table to the IP address 192.168.1.1.

Here's why the other options are not correct:

- **Option A.** The command `ip route default-route 192.168.1.1` is not a valid command in Cisco IOS.
- **Option B.** The command `ip route 192.168.1.1 0.0.0.0 0.0.0.0` is not correct because it attempts to set a static route for the specific IP 192.168.1.1, not a default route.
- **Option D.** The command `ip default-gateway 192.168.1.1` is typically used in a scenario where the device is not routing (like in a switch in default mode or a router in non-IP routing mode). In a scenario where the device is routing, the `ip route 0.0.0.0 0.0.0.0 [next-hop-ip]` command is used instead.

Q220: Which WPA3 enhancement protects against hackers viewing traffic on the Wi-Fi network?

- A. TKIP encryption
- B. AES encryption
- C. scrambled encryption key
- D. SAE encryption

▼ Answer

- A. TKIP encryption
- B. AES encryption
- C. scrambled encryption key
- D. SAE encryption**



More details Steps:

Wi-Fi Protected Access 3 (WPA3) is the latest version of the Wi-Fi security protocol. It introduces several improvements over its predecessor, WPA2, to enhance network security.

One of the major enhancements in WPA3 is the use of Simultaneous Authentication of Equals (SAE), also known as Dragonfly Key Exchange, which provides protection against offline dictionary attacks and key replay attacks.

Therefore, the correct answer is:

D. SAE encryption

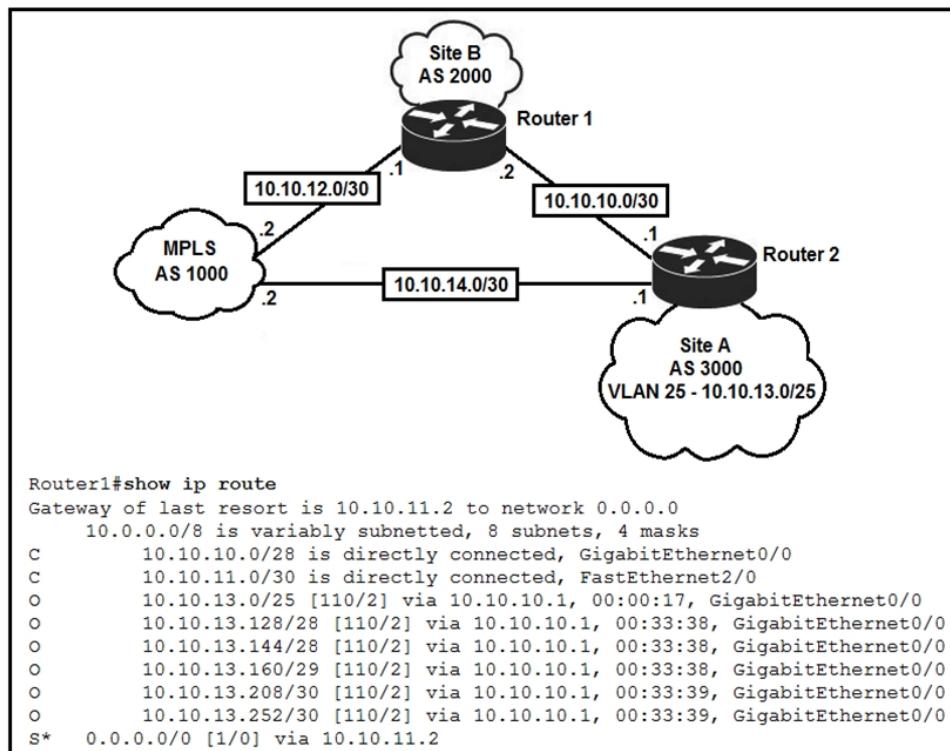
Here's why the other options are not correct:

- **A. TKIP encryption.** TKIP (Temporal Key Integrity Protocol) is an older encryption protocol used in WPA and has known vulnerabilities. It's not used in WPA3.
- **B. AES encryption.** While AES (Advanced Encryption Standard) is a strong encryption method used in WPA2 and WPA3, it's not a new enhancement in WPA3.
- **C. Scrambled encryption key.** This is not a specific encryption technique or feature in WPA3.

Q221: Refer to the exhibit. An engineer is bringing up a new circuit to the MPLS provider on the Gi0/1 interface of Router 1. The new circuit uses eBGP and learns the route to VLAN25

from the BGP path.

What is the expected behavior for the traffic flow for route 10.10.13.0/25?



- A. Traffic to 10.10.13.0/25 is load balanced out of multiple interfaces.
- B. Traffic to 10.10.13.0/25 is asymmetrical.
- C. Route 10.10.13.0/25 is updated in the routing table as being learned from interface Gi0/1.
- D. Route 10.10.13.0/25 learned via the Gi0/0 interface remains in the routing table.

▼ Answer

- A. Traffic to 10.10.13.0/25 is load balanced out of multiple interfaces.
- B. Traffic to 10.10.13.0/25 is asymmetrical.
- C. Route 10.10.13.0/25 is updated in the routing table as being learned from interface Gi0/1.
- D. Route 10.10.13.0/25 learned via the Gi0/0 interface remains in the routing table.**



More details Steps:

In a typical scenario, eBGP (with a lower administrative distance) would take precedence over OSPF. However, since no BGP configuration or routes are shown in the exhibit, we cannot assume that the BGP route to 10.10.13.0/25 has been successfully learned and installed in the routing table.

Moreover, it's important to note that even if the BGP route was learned, it wouldn't necessarily replace the OSPF route. Both routes could exist in the routing table. The actual route selection for forwarding traffic depends on the longest prefix match, not just the administrative distance.

So, based on the current information in the exhibit, the route to 10.10.13.0/25 via OSPF (learned from the Gi0/0 interface) would indeed remain in the routing table:

D. Route 10.10.13.0/25 learned via the Gi0/0 interface remains in the routing table.

Q222: Refer to the exhibit. How does router R1 handle traffic to 192.168.10.16?

```
R1# show ip route
D    192.168.10.0/24      [90/2679326] via 192.168.1.1
R    192.168.10.0/27      [120/3] via 192.168.1.2
O    192.168.10.0/23      [110/2] via 192.168.1.3
i L1   192.168.10.0/13     [115/30] via 192.168.1.4
```

- A. It selects the IS-IS route because it has the shortest prefix inclusive of the destination address.
- B. It selects the EIGRP route because it has the lowest administrative distance.
- C. It selects the OSPF route because it has the lowest cost.
- D. It selects the RIP route because it has the longest prefix inclusive of the destination address.

▼ Answer

- A. It selects the IS-IS route because it has the shortest prefix inclusive of the destination address.
- B. It selects the EIGRP route because it has the lowest administrative distance.
- C. It selects the OSPF route because it has the lowest cost.
- D. It selects the RIP route because it has the longest prefix inclusive of the destination address.**



More details Steps:

The exhibit indicates that router R1 has learned about the network 192.168.10.0 via four different routes:

- From EIGRP with a /24 subnet mask ([90/2679326] via 192.168.1.1)
- From RIP with a /27 subnet mask ([120/3] via 192.168.1.2)
- From OSPF with a /23 subnet mask ([110/2] via 192.168.1.3)
- From IS-IS with a /13 subnet mask ([115/30] via 192.168.1.4)

The question asks how router R1 handles traffic to 192.168.10.16. The choice of the route will be based on the longest prefix match principle (the router will choose the most specific route to the destination).

Looking at the subnet masks, the /27 mask is the most specific (longest prefix). Therefore, the router should select the RIP route.

So, the correct answer is:

- D. It selects the RIP route because it has the longest prefix inclusive of the destination address.**

Q223: Refer to the exhibit, Which two commands were used to create port channel 10? (Choose two)

Switch#show etherchannel summary [output omitted]				
Group	Port-channel	Protocol	Ports	
10	Po10(SU)	LACP	Gi0/0(P)	Gi0/1(P)
20	Po20(SU)	LACP	Gi0/2(P)	Gi0/3(P)

- A. int range g0/0-1 channel-group 10 mode active
- B. int range g0/0-1 channel-group 10 mode desirable
- C. int range g0/0-1 channel-group 10 mode passive
- D. int range g0/0-1 channel-group 10 mode auto
- E. int range g0/0-1 channel-group 10 mode on

▼ Answer

- **A. int range g0/0-1 channel-group 10 mode active**
- B. int range g0/0-1 channel-group 10 mode desirable
- **C. int range g0/0-1 channel-group 10 mode passive**
- D. int range g0/0-1 channel-group 10 mode auto
- E. int range g0/0-1 channel-group 10 mode on



More details Steps:

The output of the "show etherchannel summary" command indicates that the EtherChannels are using the Link Aggregation Control Protocol (LACP), which is a protocol for the collective handling of multiple physical ports that can be seen as a single channel for network traffic purposes.

LACP has two modes: `active` and `passive`. An `active` port sends LACP packets, while a `passive` port only responds to them. At least one end of the link must be `active` for LACP to work.

Therefore, to create EtherChannel 10, the appropriate commands would be:

- **A. int range g0/0-1 channel-group 10 mode active**
- **C. int range g0/0-1 channel-group 10 mode passive**

Both commands would place interfaces G0/0 and G0/1 into the same EtherChannel group (10). The mode (active or passive) determines how the LACP protocol is handled.

Here's why the other options are not correct:

- **B. int range g0/0-1 channel-group 10 mode desirable** and **D. int range g0/0-1 channel-group 10 mode auto** are associated with the Cisco proprietary protocol (PAgP) and not with LACP.
- **E. int range g0/0-1 channel-group 10 mode on** forces the interfaces into an EtherChannel without any LACP negotiation, which is not indicated in the exhibit.

Q224: What is a difference between RADIUS and TACACS+?

- A. RADIUS is most appropriate for dial authentication, but TACACS+ can be used for multiple types of authentication
- B. TACACS+ encrypts only password information and RADIUS encrypts the entire payload
- C. TACACS+ separates authentication and authorization, and RADIUS merges them
- D. RADIUS logs all commands that are entered by the administrator, but TACACS+ logs only start, stop, and interim commands

▼ Answer

- A. RADIUS is most appropriate for dial authentication, but TACACS+ can be used for multiple types of authentication
- B. TACACS+ encrypts only password information and RADIUS encrypts the entire payload
- C. TACACS+ separates authentication and authorization, and RADIUS merges them**
- D. RADIUS logs all commands that are entered by the administrator, but TACACS+ logs only start, stop, and interim commands



More details Steps:

The key difference between RADIUS (Remote Authentication Dial-In User Service) and TACACS+ (Terminal Access Controller Access-Control System Plus) is how they handle the AAA (Authentication, Authorization, and Accounting) process.

- **C. TACACS+ separates authentication and authorization, and RADIUS merges them.**

TACACS+ handles authentication, authorization, and accounting as separate processes, which gives more control over the authorization levels and command sets that a user can access after being authenticated.

On the other hand, RADIUS combines authentication and authorization as a single process. Once a user is authenticated, the RADIUS server sends the authorization data, which includes what the user is allowed to do.

Here's why the other options are incorrect:

- **A. RADIUS is most appropriate for dial authentication, but TACACS+ can be used for multiple types of authentication:** Both RADIUS and TACACS+ can be used for various types of network access, including dial-up, VPN, 802.1X, etc.
- **B. TACACS+ encrypts only password information and RADIUS encrypts the entire payload:** It's the other way around. TACACS+ encrypts the entire payload, while RADIUS only encrypts the password.
- **D. RADIUS logs all commands that are entered by the administrator, but TACACS+ logs only start, stop, and interim commands:** Again, it's the other way around. TACACS+ can log all commands entered by the administrator, while RADIUS typically logs only start, stop, and interim commands.

Q225: Refer to the exhibit. How does the router manage traffic to 192.168.12.16?

EIGRP: 192.168.12.0/24
RIP: 192.168.12.0/27
OSPF: 192.168.12.0/28

- A. It selects the RIP route because it has the longest prefix inclusive of the destination address.
- B. It chooses the OSPF route because it has the longest prefix inclusive of the destination address.
- C. It load-balances traffic between all three routes
- D. It chooses the EIGRP route because it has the lowest administrative distance

▼ Answer

- A. It selects the RIP route because it has the longest prefix inclusive of the destination address.**
- B. It chooses the OSPF route because it has the longest prefix inclusive of the destination address.
- C. It load-balances traffic between all three routes
- D. It chooses the EIGRP route because it has the lowest administrative distance



More details Steps:

The IP address 192.168.12.16 falls within the range of the /27 subnet (192.168.12.0 - 192.168.12.31), but not within the range of the /28 subnet (192.168.12.0 - 192.168.12.15).

Therefore, the correct answer is:

A. It selects the RIP route because it has the longest prefix inclusive of the destination address.

other options are not correct:

B. It chooses the OSPF route because it has the longest prefix inclusive of the destination address.

This option is incorrect because while the OSPF route has the longest prefix length (/28), the IP address 192.168.12.16 does not fall within the range of this subnet (192.168.12.0 - 192.168.12.15).

C. It load-balances traffic between all three routes

This option is incorrect because routers use the longest prefix match rule to determine the best route. In this case, the RIP route is the longest prefix match that includes the IP address 192.168.12.16. Load balancing would only occur if there were multiple routes with the same longest prefix match.

D. It chooses the EIGRP route because it has the lowest administrative distance

This option is incorrect because administrative distance is only considered when there are multiple routes to the same network with the same prefix length. In this case, the longest prefix match rule selects the RIP route before considering administrative distance.

Q226: What is an advantage of Cisco DNA Center versus traditional campus device management?

- A. It supports numerous extensibility options including cross-domain adapters and third-party SDKs.
- B. It supports high availability for management functions when operating in cluster mode.
- C. It enables easy autodiscovery of network elements in a brownfield deployment.
- D. It is designed primarily to provide network assurance.

▼ Answer

- A. It supports numerous extensibility options including cross-domain adapters and third-party SDKs.**
- B. It supports high availability for management functions when operating in cluster mode.
- C. It enables easy autodiscovery of network elements in a brownfield deployment.
- D. It is designed primarily to provide network assurance.



More details Steps:

A. It supports numerous extensibility options including cross-domain adapters and third-party SDKs.

This indeed is a significant advantage of Cisco DNA Center over traditional campus device management. The ability to support a wide range of extensibility options, including cross-domain adapters and third-party Software Development Kits (SDKs), allows for greater flexibility and integration with other systems. This ability can enhance the functionality and interoperability of the network management system, providing a more comprehensive and adaptable solution.

other options might not be considered as correct in this context:

B. It supports high availability for management functions when operating in cluster mode.

While it's true that Cisco DNA Center supports high availability when operating in cluster mode, this might not be seen as a unique advantage over traditional campus device management. Many traditional systems also support high availability, so while it's an important feature, it may not distinguish Cisco DNA Center from other solutions.

C. It enables easy autodiscovery of network elements in a brownfield deployment.

Auto-discovery of network elements is a feature that is becoming increasingly common in network management solutions. While it's an important feature for managing and integrating existing systems in a brownfield deployment, it may not be seen as a unique advantage of Cisco DNA Center.

D. It is designed primarily to provide network assurance.

Network assurance is an important goal of any network management solution. While Cisco DNA Center does provide advanced network assurance capabilities, so do many traditional campus device management solutions. The primary design goal of a solution may not necessarily represent an advantage over other solutions.

In contrast, the extensibility of Cisco DNA Center, including its support for cross-domain adapters and third-party SDKs (Option A), allows for a level of customization and integration that may not be possible with more traditional solutions. This can enable more efficient and effective network management, making it a significant advantage of Cisco DNA Center.

Q227: While examining excessive traffic on the network, it is noted that all incoming packets on an interface appear to be allowed even though an IPv4 ACL is applied to the interface. Which two misconfigurations cause this behavior? (Choose two)

- A. The packets fail to match any permit statement
- B. A matching permit statement is too high in the access test
- C. A matching permit statement is too broadly defined
- D. The ACL is empty
- E. A matching deny statement is too high in the access list

▼ Answer

- A. The packets fail to match any permit statement
- B. A matching permit statement is too high in the access test**
- C. A matching permit statement is too broadly defined**
- D. The ACL is empty
- E. A matching deny statement is too high in the access list



More details Steps:

C. A matching permit statement is too broadly defined

In Access Control Lists (ACLs), the order of the rules is very important because the device processes the rules from top to bottom. If a packet matches a rule, the device applies the action (permit/deny) specified by that rule and stops processing further rules.

- **B.** If a matching permit statement is too high in the access list, it may allow the traffic before it reaches a more specific deny statement further down the list. Hence, unwanted traffic might be permitted.
- **C.** If a permit statement is too broadly defined, it might allow more traffic than intended. For example, if a rule allows all traffic from the 10.0.0.0/8 network, it would permit traffic from any IP address between 10.0.0.1 and 10.255.255.254, which could include unwanted traffic.

The other options are incorrect because:

- **A.** If the packets fail to match any permit statement, they would be denied because there is an implicit deny at the end of every ACL.
- **D.** If the ACL were empty, it wouldn't allow any traffic because of the implicit deny all rule at the end of an ACL.
- **E.** A matching deny statement being too high in the access list would block traffic, not allow it.

Q228: How do traditional campus device management and Cisco DNA Center device management differ in regards to deployment?

- A. Cisco DNA Center device management can deploy a network more quickly than traditional campus device management
- B. Traditional campus device management allows a network to scale more quickly than with Cisco DNA Center device management
- C. Cisco DNA Center device management can be implemented at a lower cost than most traditional campus device management options
- D. Traditional campus device management schemes can typically deploy patches and updates more quickly than Cisco DNA Center device management

▼ Answer

A. Cisco DNA Center device management can deploy a network more quickly than traditional campus device management

- B. Traditional campus device management allows a network to scale more quickly than with Cisco DNA Center device management
- C. Cisco DNA Center device management can be implemented at a lower cost than most traditional campus device management options
- D. Traditional campus device management schemes can typically deploy patches and updates more quickly than Cisco DNA Center device management



More details Steps:

A. Cisco DNA Center device management can deploy a network more quickly than traditional campus device management

Cisco DNA Center uses automation and artificial intelligence to simplify many aspects of network management, including deployment. This can significantly reduce the time required to deploy a network compared to traditional campus device management. Traditional methods often require a lot of manual configuration and troubleshooting, which can be time-consuming.

Let's briefly touch on the other options:

B. Traditional campus device management allows a network to scale more quickly than with Cisco DNA Center device management

This is typically not the case. Traditional management methods often struggle with scalability due to the increasing complexity as the network grows. Cisco DNA Center, with its automation capabilities, is designed to handle network growth more efficiently.

C. Cisco DNA Center device management can be implemented at a lower cost than most traditional campus device management options

While Cisco DNA Center can potentially lower operational costs by reducing manual labor and downtime with its automation and AI capabilities, the initial implementation cost might not necessarily be lower than traditional methods. The total cost would depend on various factors, including the specific solutions being compared.

D. Traditional campus device management schemes can typically deploy patches and updates more quickly than Cisco DNA Center device management

This is also typically not the case. With its automation capabilities, Cisco DNA Center can often deploy patches and updates more quickly and reliably than traditional methods, which often rely on manual processes.

Q229: How do AAA operations compare regarding user identification, user services and access control?

- A. Authorization provides access control and authentication tracks user services
- B. Authentication identifies users and accounting tracks user services
- C. Accounting tracks user services, and authentication provides access control
- D. Authorization identifies users and authentication provides access control

▼ Answer

- A. Authorization provides access control and authentication tracks user services

B. Authentication identifies users and accounting tracks user services

- C. Accounting tracks user services, and authentication provides access control
- D. Authorization identifies users and authentication provides access control



More details Steps:

AAA stands for Authentication, Authorization, and Accounting. Here's what each operation does:

- **Authentication** is the process of identifying users. This typically involves verifying the user's identity through credentials, such as a username and password.
- **Authorization** is the process of granting or denying a user's access to specific resources or services based on their authenticated identity. This provides access control by determining what resources a user is allowed to access.
- **Accounting** is the process of tracking user activity. This often includes logging when users log in and out, what actions they perform, and other relevant information. This provides a record of user services.

The other options (A, C, D) do not correctly describe the roles of Authentication, Authorization, and Accounting in AAA operations.

Q230: What is a difference between local AP mode and FlexConnect AP mode?

- A. Local AP mode creates two CAPWAP tunnels per AP to the WLC
- B. FlexConnect AP mode fails to function if the AP loses connectivity with the WLC
- C. FlexConnect AP mode bridges the traffic from the AP to the WLC when local switching is configured
- D. Local AP mode causes the AP to behave as if it were an autonomous AP

▼ Answer

A. Local AP mode creates two CAPWAP tunnels per AP to the WLC

- B. FlexConnect AP mode fails to function if the AP loses connectivity with the WLC
- C. FlexConnect AP mode bridges the traffic from the AP to the WLC when local switching is configured
- D. Local AP mode causes the AP to behave as if it were an autonomous AP



More details Steps:

A. Local AP mode creates two CAPWAP tunnels per AP to the WLC

Local AP mode and FlexConnect AP mode are different operational modes for Cisco Access Points (APs) in a wireless LAN controller (WLC) architecture.

In Local mode (also known as Centralized mode), the AP creates two Control and Provisioning of Wireless Access Points (CAPWAP) tunnels to the WLC - one for control traffic and one for data traffic. All the traffic from wireless clients is sent through these CAPWAP tunnels to the WLC, where it is then forwarded onto the wired network.

The other options do not correctly describe the differences between Local AP mode and FlexConnect AP mode:

B. FlexConnect AP mode fails to function if the AP loses connectivity with the WLC

Incorrect. FlexConnect mode (also known as H-REAP) allows APs to continue to function and provide access to wireless clients even if their connection to the WLC is lost. This is one of the key benefits of FlexConnect mode.

C. FlexConnect AP mode bridges the traffic from the AP to the WLC when local switching is configured

Incorrect. When local switching is configured in FlexConnect mode, client data traffic is not sent to the WLC. Instead, it is bridged directly onto the local wired network by the AP, helping to reduce unnecessary WAN traffic.

D. Local AP mode causes the AP to behave as if it were an autonomous AP

Incorrect. In local mode, the AP is not autonomous. It is centrally managed by the WLC and all its traffic is forwarded to the WLC. Autonomous APs, on the other hand, operate independently of a WLC and handle their own management and client traffic forwarding.

Q231: Which function does the range of private IPv4 addresses perform?

- A. allows multiple companies to each use the same addresses without conflicts
- B. provides a direct connection for hosts from outside of the enterprise network
- C. ensures that NAT is not required to reach the internet with private range addressing
- D. enables secure communications to the internet for all external hosts

▼ Answer

A. allows multiple companies to each use the same addresses without conflicts

- B. provides a direct connection for hosts from outside of the enterprise network
- C. ensures that NAT is not required to reach the internet with private range addressing
- D. enables secure communications to the internet for all external hosts



More details Steps:

A. Allows multiple companies to each use the same addresses without conflicts

Private IPv4 addresses are used in local networks such as home, office, and enterprise LANs. They are not routed on the internet, which allows multiple organizations or individuals to use the same private address ranges in their separate networks without conflicts.

Let's take a look at the other options:

B. Provides a direct connection for hosts from outside of the enterprise network

Incorrect. Private IP addresses cannot be directly reached from the internet. For hosts outside of the network to reach a device with a private IP address, techniques like Port Forwarding or Virtual Private Network (VPN) are used.

C. Ensures that NAT is not required to reach the internet with private range addressing

Incorrect. In fact, Network Address Translation (NAT) is necessary for devices with private IP addresses to reach the internet. NAT translates the private IP addresses to public ones that can be routed on the internet.

D. Enables secure communications to the internet for all external hosts

Incorrect. While private addresses can contribute to network security by hiding internal network structure and hosts from the internet, they do not inherently provide secure communications to the internet for external hosts. Security measures like encryption, firewalls, and secure protocols are needed for that.

Q232: What event has occurred if a router sends a notice level message to a syslog server?

- A. A TCP connection has been torn down
- B. An ICMP connection has been built
- C. An interface line has changed status
- D. A certificate has expired.

▼ Answer

- A. A TCP connection has been torn down
- B. An ICMP connection has been built
- C. An interface line has changed status**
- D. A certificate has expired.



More details Steps:

C. An interface line has changed status

Syslog is a standard for message logging. It allows a device to send event notification messages across IP networks to event message collectors, also known as Syslog servers. Syslog messages are classified based on their severity levels, with 'Notice' being one of them.

A 'Notice' level message, which indicates conditions that are not error conditions, but that may require special handling, is often generated when there are significant changes in the status of a device. Interface up/down events are typically logged at this level. So, if an interface line has changed status on a router, it might generate a 'Notice' level syslog message.

The other options typically wouldn't generate a 'Notice' level message:

A. A TCP connection has been torn down

This is a normal event and typically wouldn't generate a 'Notice' level message.

B. An ICMP connection has been built

ICMP is a protocol used for error reporting and diagnostics. Building an ICMP connection is a normal event that typically wouldn't generate a 'Notice' level message.

D. A certificate has expired

This is a critical event that would likely generate a 'Warning' or 'Error' level message, which are higher severity levels than 'Notice'.

Q233: Refer to the exhibit. An administrator configures four switches for local authentication using passwords that are stored in a cryptographic hash. The four switches must also support SSH access for administrators to manage the network infrastructure. Which switch is configured correctly to meet these requirements?

```
SW1(config-line) #line vty 0 15
SW1(config-line) #no login local
SW1(config-line) #password cisco

SW2(config) #username admin1 password abcd1234
SW2(config) #username admin2 password abcd1234
SW2(config-line) #line vty 0 15
SW2(config-line) #login local

SW3(config) #username admin1 secret abcd1234
SW3(config) #username admin2 secret abcd1234
SW3(config-line) #line vty 0 15
SW3(config-line) #login local

SW4(config) #username admin1 secret abcd1234
SW4(config) #username admin2 secret abcd1234
SW4(config-line) #line console 0
SW4(config-line) #login local
```

- A. SW1
- B. SW2
- C. SW3
- D. SW4

▼ Answer

- A. SW1
- B. SW2
- C. SW3**
- D. SW4



More details Steps:

C. SW3

The requirement is to configure switches for local authentication using passwords that are stored in a cryptographic hash, and the switches must also support SSH access for administrators to manage the network infrastructure.

Using the "secret" keyword when defining the password as in SW3 and SW4 stores the password in a cryptographic hash. However, SW4 has the login local command applied to the console line, not the vty lines, so it wouldn't support SSH access because SSH access is configured on vty lines.

SW3 configures the vty lines for local login, which is required for SSH access, and it also stores the passwords in a cryptographic hash, so it's the only switch that meets all the requirements.

The configurations of SW1 and SW2 are not correct because they do not store passwords in a cryptographic hash. In SW1, the "no login local" command is used, which disables local login, and a clear-text password is used. In SW2, even though the usernames are set up and vty lines are configured for local login, the passwords are not stored as a cryptographic hash.

Q234: What are two fundamentals of virtualization? (choose two)

- A. The environment must be configured with one hypervisor that serves solely as a network manager to monitor SNMP traffic
- B. It allows logical network devices to move traffic between virtual machines and the rest of the physical network
- C. It allows multiple operating systems and applications to run independently on one physical server.
- D. It allows a physical router to directly connect NICs from each virtual machine into the network
- E. It requires that some servers, virtual machines and network gear reside on the Internet

▼ Answer

- A. The environment must be configured with one hypervisor that serves solely as a network manager to monitor SNMP traffic
- B. It allows logical network devices to move traffic between virtual machines and the rest of the physical network**
- C. It allows multiple operating systems and applications to run independently on one physical server.**

- D. It allows a physical router to directly connect NICs from each virtual machine into the network
- E. It requires that some servers, virtual machines and network gear reside on the Internet



More details Steps:

B. It allows logical network devices to move traffic between virtual machines and the rest of the physical network

and

C. It allows multiple operating systems and applications to run independently on one physical server

Virtualization is a technology that separates hardware from software by using a software layer, called a hypervisor, to emulate hardware. This allows multiple virtual machines (VMs), each with their own operating system and applications, to run independently on a single physical server.

Virtualization also allows logical network devices, such as virtual switches or routers, to move traffic between VMs and the rest of the physical network. This enables networking within and between VMs, as well as communication with external networks.

The other options do not correctly describe the fundamentals of virtualization:

A. The environment must be configured with one hypervisor that serves solely as a network manager to monitor SNMP traffic

This is not a fundamental of virtualization. While a hypervisor is essential in a virtualized environment, its primary function is not to serve as a network manager to monitor SNMP traffic. Its primary function is to manage the virtual machines.

D. It allows a physical router to directly connect NICs from each virtual machine into the network

Incorrect. In a virtualized environment, VMs connect to the network through virtual network interfaces, not physical ones.

E. It requires that some servers, virtual machines and network gear reside on the Internet

Incorrect. Virtualization does not inherently require any servers, VMs, or network gear to reside on the Internet. It's possible to have a completely isolated, offline virtualized environment.

Q235: Refer to the exhibit. What two conclusions should be made about this configuration? (Choose two)

```
SW1#show spanning-tree vlan 30
VLAN0030
Spanning tree enabled protocol rstp
Root ID      Priority      32798
              Address       0025.63e9.c800
              Cost          19
              Port          1 (FastEthernet 2/1)
              Hello Time    2 sec
              Max Age       30 sec
              Forward Delay 20 sec
[Output suppressed]
```

- A. The designated port is FastEthernet 2/1
- B. This is a root bridge
- C. The spanning-tree mode is Rapid PVST+
- D. The spanning-tree mode is PVST+
- E. The root port is FastEthernet 2/1

▼ Answer

- A. The designated port is FastEthernet 2/1
- B. This is a root bridge
- C. The spanning-tree mode is Rapid PVST+**
- D. The spanning-tree mode is PVST+
- E. The root port is FastEthernet 2/1**



More details Steps:

C. The spanning-tree mode is Rapid PVST+

and

E. The root port is FastEthernet 2/1

The command "show spanning-tree vlan 30" shows information about the spanning-tree status for VLAN 30. In the output, we see that the protocol is RSTP (Rapid Spanning Tree Protocol), which indicates that the mode is Rapid PVST+ (Per-VLAN Spanning Tree Plus).

The output also shows that the root port for this VLAN is FastEthernet 2/1. The root port is the port on a non-root bridge that has the best path to the root bridge.

The other options are not correct based on the provided output:

A. The designated port is FastEthernet 2/1

This is incorrect. The output shows FastEthernet 2/1 as the root port, not the designated port.

B. This is a root bridge

This is incorrect. In the output, there is a root port listed, which means this switch is not the root bridge. A root bridge doesn't have a root port.

D. The spanning-tree mode is PVST+

This is incorrect. The output shows that the protocol is RSTP, which indicates Rapid PVST+ mode, not PVST+.

Q236: Refer to the exhibit. A router reserved these five routes from different routing information sources. Which two routes does the router install in its routing table? (Choose two)

IBGP route 10.0.0.0/30
RIP route 10.0.0.0/30
OSPF route 10.0.0.0/16
OSPF route 10.0.0.0/30
EIGRP route 10.0.0.1/32

- A. RIP route 10.0.0.0/30
- B. iBGP route 10.0.0.0/30
- C. OSPF route 10.0.0.0/30
- D. EIGRP route 10.0.0.1/32
- E. OSPF route 10.0.0.0/16

▼ **Answer**

- A. RIP route 10.0.0.0/30
- B. iBGP route 10.0.0.0/30
- C. OSPF route 10.0.0.0/30**
- D. EIGRP route 10.0.0.1/32**
- E. OSPF route 10.0.0.0/16



More details Steps:

Without actual administrative distances (AD) or metrics provided in the question, we have to rely on the default AD values for these routing protocols:

- EIGRP: 90 (internal), 170 (external)
- OSPF: 110
- RIP: 120
- iBGP: 200

Lower AD is preferred over higher. Therefore, the routes that would be installed in the routing table based on default AD values would be:

D. EIGRP route 10.0.0.1/32

and

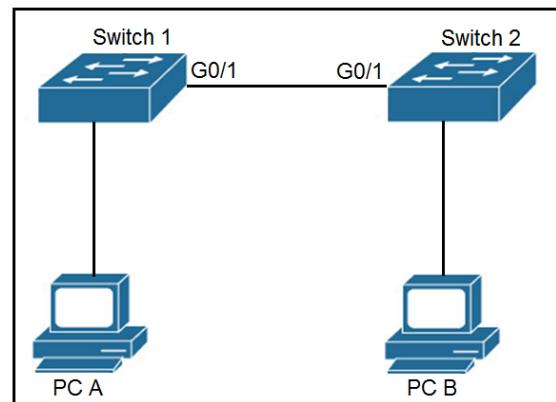
C. OSPF route 10.0.0.0/30

The EIGRP route is selected because EIGRP has a lower default AD than OSPF, RIP, and iBGP.

Among the routes for 10.0.0.0, the OSPF route with the /30 subnet mask is chosen over the /16 route because in case of a tie in AD, the route with the longest prefix (the most specific route) is chosen.

Please note that in a real-world situation, other factors could influence the route selection process, such as manual changes to AD, route redistribution, route summarization, and others.

Q237: Refer to the exhibit. The network administrator wants VLAN 67 traffic to be untagged between Switch 1 and Switch 2 while all other VLANs are to remain tagged. Which command accomplishes this task?



- A. switchport access vlan 67
- B. switchport trunk allowed vlan 67
- C. switchport private-vlan association host 67
- D. switchport trunk native vlan 67

▼ Answer

- A. switchport access vlan 67
- B. switchport trunk allowed vlan 67
- C. switchport private-vlan association host 67
- D. switchport trunk native vlan 67**



More details Steps:

D. switchport trunk native vlan 67

The `switchport trunk native vlan` command is used to set the native VLAN ID on a trunk port. The native VLAN traffic is sent across the trunk link untagged. By default, this value is VLAN 1.

So, if the network administrator wants VLAN 67 traffic to be untagged between Switch 1 and Switch 2, they should set VLAN 67 as the native VLAN on the trunk link between the two switches.

The other options do not meet the requirement:

A. switchport access vlan 67

This command is used to set the access VLAN on an access port, not a trunk port.

B. switchport trunk allowed vlan 67

This command is used to specify which VLANs are allowed to cross the trunk link, but it doesn't control whether the traffic is tagged or untagged.

C. switchport private-vlan association host 67

This command is used to associate a private VLAN with a primary VLAN, which is not the requirement in this case.

Q238: What are two differences between optical-fiber cabling and copper cabling? (Choose two)

- A. Light is transmitted through the core of the fiber
- B. A BNC connector is used for fiber connections
- C. The glass core component is encased in a cladding
- D. Fiber connects to physical interfaces using Rj-45 connections
- E. The data can pass through the cladding

▼ Answer

A. Light is transmitted through the core of the fiber

- B. A BNC connector is used for fiber connections
- C. The glass core component is encased in a cladding**

- D. Fiber connects to physical interfaces using Rj-45 connections
- E. The data can pass through the cladding



More details Steps:

A. Light is transmitted through the core of the fiber

and

C. The glass core component is encased in a cladding

Optical fiber cabling uses light to transmit data, and the signal is confined to a glass or plastic core within the fiber. This is different from copper cabling, which uses electrical signals to transmit data.

The core of the fiber optic cable is surrounded by a layer of material called cladding, which reflects the light back into the core and helps to keep the signal within the fiber. This is a characteristic unique to fiber optic cables and is not found in copper cabling.

The other statements are incorrect:

B. A BNC connector is used for fiber connections

BNC connectors are typically used for coaxial cable, not fiber optic cable. Fiber optic cables use various types of connectors, such as SC, ST, LC, and others.

D. Fiber connects to physical interfaces using Rj-45 connections

RJ-45 connectors are typically used for Ethernet cabling (copper), not fiber optic cabling.

E. The data can pass through the cladding

Data (in the form of light signals) is transmitted through the core of the fiber, not the cladding. The cladding's function is to reflect the light back into the core to prevent signal loss.

Q239: Which two minimum parameters must be configured on an active interface to enable OSPFv2 to operate? (Choose two)

- A. OSPF area
- B. OSPF MD5 authentication key
- C. IPv6 address
- D. OSPf process ID
- E. OSPf stub flag

▼ Answer

A. OSPF area

- B. OSPF MD5 authentication key
- C. IPv6 address

D. OSPf process ID

- E. OSPf stub flag



More details Steps:

A. OSPF area

and

D. OSPF process ID

Open Shortest Path First version 2 (OSPFv2) is a routing protocol for IPv4. To enable OSPF on an interface, at minimum, you must specify the OSPF area and the OSPF process ID.

The OSPF process ID is a numerical identifier (1-65535) used on a router to identify an OSPF instance. This allows for multiple OSPF processes to run on the same router.

The OSPF area is a logical grouping of network segments, and each interface participating in OSPF must be assigned to an area.

The other options are not required to enable OSPFv2:

B. OSPF MD5 authentication key

While OSPF supports authentication (including MD5), it's not required to enable OSPF operation. It's an optional security measure.

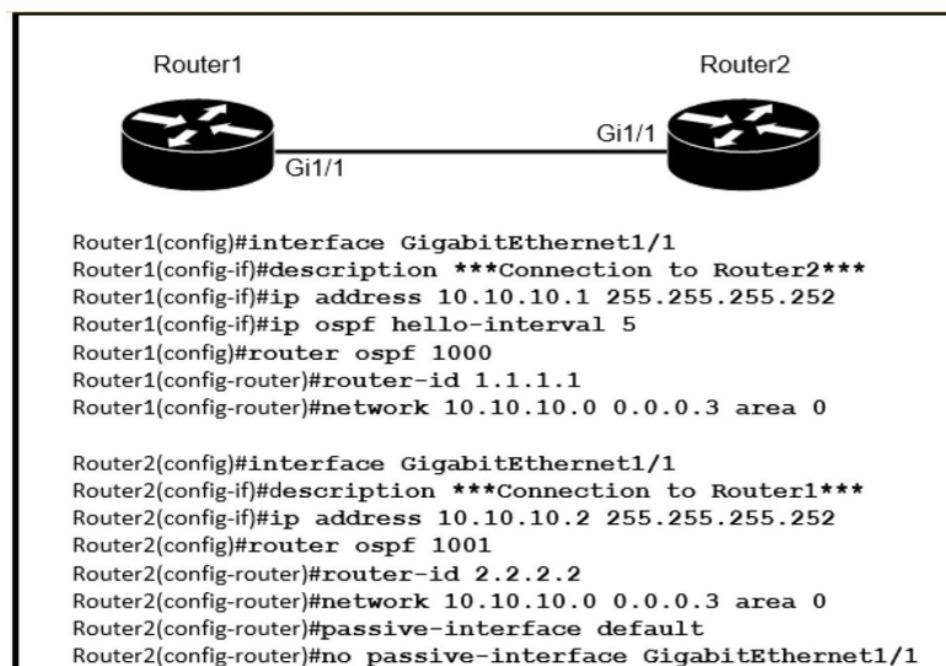
C. IPv6 address

OSPFv2 is for IPv4, not IPv6. For IPv6, OSPFv3 is used.

E. OSPF stub flag

Stub flags are used in specific OSPF network types (i.e., stub areas or totally stubby areas), but they are not required to enable basic OSPF operation.

Q240: Refer to the exhibit. After the configuration is applied, the two routers fail to establish an OSPF neighbor relationship. what is the reason for the problem?



- A. The OSPF router IDs are mismatched.
- B. Router2 is using the default hello timer.
- C. The network statement on Router1 is misconfigured.
- D. The OSPF process IDs are mismatched.

▼ Answer

- A. The OSPF router IDs are mismatched.
- B. Router2 is using the default hello timer.**
- C. The network statement on Router1 is misconfigured.
- D. The OSPF process IDs are mismatched.



More details Steps:

B. Router2 is using the default hello timer.

OSPF neighbors must have matching hello and dead intervals in order to form a neighbor relationship. In the exhibit, Router1 has its hello interval configured to 5 seconds on the interface connecting to Router2 (`ip ospf hello-interval 5`). However, Router2 is using the default hello interval, which is 10 seconds. This mismatch in hello intervals is preventing the OSPF neighbor relationship from being established.

The other options are not correct:

A. The OSPF router IDs are mismatched.

Router IDs do not have to match for OSPF neighborship to form. They must simply be unique.

C. The network statement on Router1 is misconfigured.

Both Router1 and Router2 have correct network statements considering the subnet they are on (10.10.10.0/30).

D. The OSPF process IDs are mismatched.

OSPF process IDs are locally significant, which means they don't have to match on neighboring routers. They are used to identify the OSPF process within the router itself.

Q241: How do TCP and UDP differ in the way they provide reliability for delivery of packets?

- A. TCP is a connectionless protocol that does not provide reliable delivery of data, UDP is a connection-oriented protocol that uses sequencing to provide reliable delivery.
- B. TCP does not guarantee delivery or error checking to ensure that there is no corruption of data UDP provides message acknowledgement and retransmits data if lost.
- C. TCP provides flow control to avoid overwhelming a receiver by sending too many packets at once, UDP sends packets to the receiver in a continuous stream without checking for sequencing
- D. TCP uses windowing to deliver packets reliably; UDP provides reliable message transfer between hosts by establishing a three-way handshake

▼ Answer

- A. TCP is a connectionless protocol that does not provide reliable delivery of data, UDP is a connection-oriented protocol that uses sequencing to provide reliable delivery.
- B. TCP does not guarantee delivery or error checking to ensure that there is no corruption of data UDP provides message acknowledgement and retransmits data if lost.
- C. TCP provides flow control to avoid overwhelming a receiver by sending too many packets at once, UDP sends packets to the receiver in a continuous stream without checking for sequencing**
- D. TCP uses windowing to deliver packets reliably; UDP provides reliable message transfer between hosts by establishing a three-way handshake



More details Steps:

C. TCP provides flow control to avoid overwhelming a receiver by sending too many packets at once, UDP sends packets to the receiver in a continuous stream without checking for sequencing

TCP (Transmission Control Protocol) is a connection-oriented protocol and provides reliability through various mechanisms including sequencing, acknowledgments, and flow control. Flow control in TCP ensures that a sender does not overwhelm a receiver by sending too many packets at once.

On the other hand, UDP (User Datagram Protocol) is a connectionless protocol and does not provide reliability features like sequencing, acknowledgments, or flow control. It sends packets to the receiver in a continuous stream without checking if the receiver is ready to receive them or if the packets are received in the correct order.

The other options are incorrect:

A. TCP is a connectionless protocol that does not provide reliable delivery of data, UDP is a connection-oriented protocol that uses sequencing to provide reliable delivery.

This statement is incorrect. TCP is a connection-oriented protocol and provides reliable delivery, while UDP is a connectionless protocol and does not provide reliable delivery.

B. TCP does not guarantee delivery or error checking to ensure that there is no corruption of data UDP provides message acknowledgement and retransmits data if lost.

This statement is incorrect. TCP does provide guarantees for delivery through acknowledgments and error checking through checksums. UDP does not provide these features.

D. TCP uses windowing to deliver packets reliably; UDP provides reliable message transfer between hosts by establishing a three-way handshake.

This statement is incorrect. While it's true that TCP uses windowing for reliable delivery, UDP does not provide reliable message transfer and does not use a three-way handshake. The three-way handshake is a feature of TCP, not UDP.

Q242: A packet is destined for 10.10.1.22. Which static route does the router choose to forward the packet?

- A. ip route 10.10.1.0 255.255.255.240 10.10.255.1
- B. ip route 10.10.1.16 255.255.255.252 10.10.255.1
- C. ip route 10.10.1.20 255.255.255.252 10.10.255.1
- D. ip route 10.10.1.20 255.255.255.254 10.10.255.1

▼ Answer

- A. ip route 10.10.1.0 255.255.255.240 10.10.255.1
- B. ip route 10.10.1.16 255.255.255.252 10.10.255.1
- C. ip route 10.10.1.20 255.255.255.252 10.10.255.1**
- D. ip route 10.10.1.20 255.255.255.254 10.10.255.1



More details Steps:

C. ip route 10.10.1.20 255.255.255.252 10.10.255.1

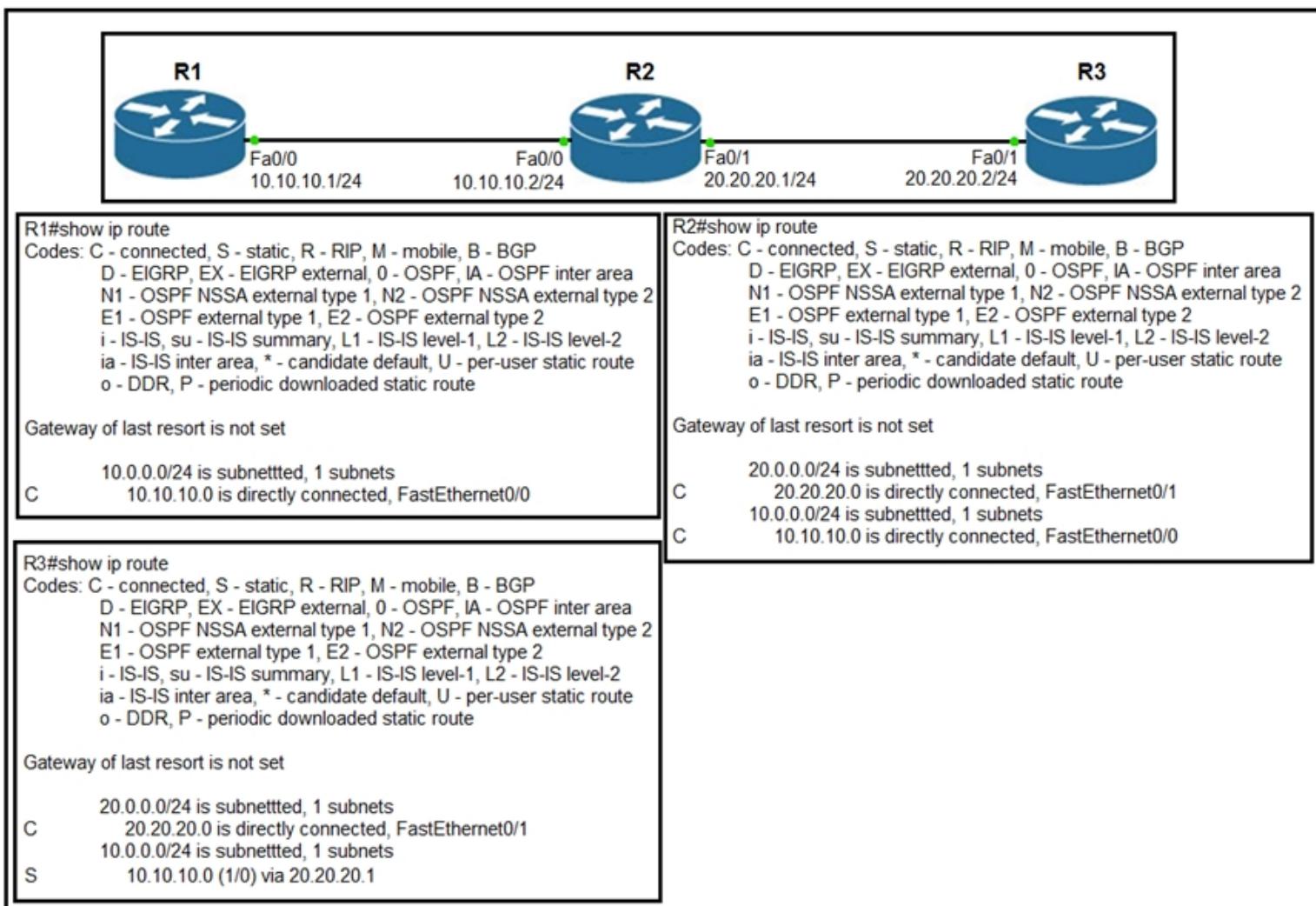
When a router chooses a static route, it uses the longest prefix match, meaning it chooses the route with the subnet that most specifically matches the destination IP address.

In the provided options:

- Route A: `ip route 10.10.1.0 255.255.255.240 10.10.255.1` covers addresses from 10.10.1.1 to 10.10.1.14.
- Route B: `ip route 10.10.1.16 255.255.255.252 10.10.255.1` covers addresses from 10.10.1.17 to 10.10.1.18.
- Route C: `ip route 10.10.1.20 255.255.255.252 10.10.255.1` covers addresses from 10.10.1.21 to 10.10.1.22.
- Route D: `ip route 10.10.1.20 255.255.255.254 10.10.255.1` covers the single address 10.10.1.21.

Therefore, the router will choose the static route C (`ip route 10.10.1.20 255.255.255.252 10.10.255.1`) to forward a packet destined for 10.10.1.22 because it is the only route that includes the destination IP address in its subnet.

Q243: Refer to the exhibit. Router R1 Fa0/0 cannot ping router R3 Fa0/1. Which action must be taken in router R1 to help resolve the configuration issue?



- A. set the default network as 20.20.20.0/24
- B. set the default gateway as 20.20.20.2
- C. configure a static route with Fa0/1 as the egress interface to reach the 20.20.20.0/24 network
- D. configure a static route with 10.10.10.2 as the next hop to reach the 20.20.20.0/24 network

▼ Answer

- A. set the default network as 20.20.20.0/24
- B. set the default gateway as 20.20.20.2
- C. configure a static route with Fa0/1 as the egress interface to reach the 20.20.20.0/24 network
- D. configure a static route with 10.10.10.2 as the next hop to reach the 20.20.20.0/24 network**



More details Steps:

D. configure a static route with 10.10.10.2 as the next hop to reach the 20.20.20.0/24 network

From the exhibit, it seems that router R1 doesn't have a route to the 20.20.20.0/24 network. This is likely why it can't ping router R3's Fa0/1 interface. To fix this issue, a static route can be added on R1 to reach the 20.20.20.0/24 network using 10.10.10.2 (which appears to be the IP address of router R2's interface connected to R1) as the next hop. This can be achieved with the following command on R1:\

```
R1(config)# ip route 20.20.20.0 255.255.255.0 10.10.10.2
```

This will create a static route that tells R1 to forward packets destined to the 20.20.20.0/24 network to R2, which appears to already have a route to that network.

The other options are incorrect because:

- A. set the default network as 20.20.20.0/24

A default network command would help if the router needed to reach an unknown network, not a specific known one.

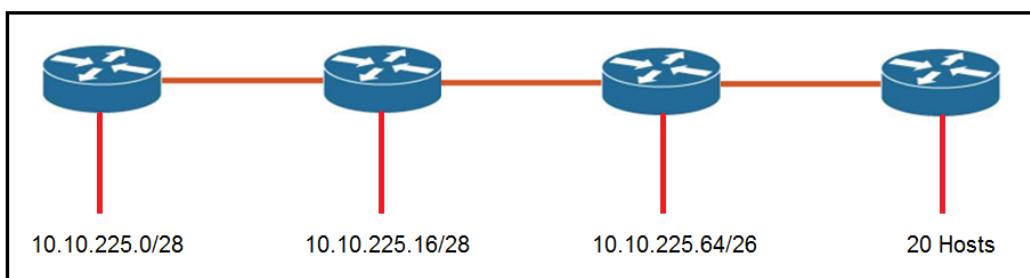
- B. set the default gateway as 20.20.20.2

Setting the default gateway to an IP address that is not directly reachable won't help. R1 doesn't have a route to the 20.20.20.0/24 network to begin with.

- C. configure a static route with Fa0/1 as the egress interface to reach the 20.20.20.0/24 network

R1 does not appear to have a FastEthernet0/1 interface based on the exhibit, and even if it did, we can't be sure that this interface is in the correct direction towards the 20.20.20.0/24 network.

Q244: Refer to the exhibit. An engineer must add a subnet for a new office that will add 20 users to the network. Which IPv4 network and subnet mask combination does the engineer assign to minimize wasting addresses?



- A. 10.10.225.48 255.255.255.240
- B. 10.10.225.32 255.255.255.240
- C. 10.10.225.48 255.255.255.224
- D. 10.10.225.32 255.255.255.224

▼ Answer

- A. 10.10.225.48 255.255.255.240
- B. 10.10.225.32 255.255.255.240
- C. 10.10.225.48 255.255.255.224
- D. 10.10.225.32 255.255.255.224**



More details Steps:

D. 10.10.225.32 255.255.255.224

The subnet 10.10.225.32/27 (with subnet mask 255.255.255.224) would provide up to 30 usable IP addresses (32 total addresses, minus the network address and broadcast address), which is sufficient for 20 users.

It is also the next available subnet after the already allocated subnets in the exhibit. The subnets 10.10.225.0/28 and 10.10.225.16/28 take up the range from 10.10.225.0 to 10.10.225.31, and the next subnet, 10.10.225.64/26, starts from 10.10.225.64. So, the range from 10.10.225.32 to 10.10.225.63 is available, and 10.10.225.32/27 fits in this range without wasting addresses.

The other options either do not provide enough addresses (options A and B) or they overlap with the existing 10.10.225.64/26 subnet (option C).

Q245: A corporate office uses four floors in a building

- Floor 1 has 24 users
- Floor 2 has 29 users
- Floor 3 has 28 users
- Floor 4 has 22 users

Which subnet summarizes and gives the most efficient distribution of IP addresses for the router configuration?

- A. 192.168.0.0/26 as summary and 192.168.0.0/29 for each floor
- B. 192.168.0.0/24 as summary and 192.168.0.0/28 for each floor
- C. 192.168.0.0/23 as summary and 192.168.0.0/25 for each floor
- D. 192.168.0.0/25 as summary and 192.168.0.0/27 for each floor

▼ Answer

- A. 192.168.0.0/26 as summary and 192.168.0.0/29 for each floor
- B. 192.168.0.0/24 as summary and 192.168.0.0/28 for each floor
- C. 192.168.0.0/23 as summary and 192.168.0.0/25 for each floor
- D. 192.168.0.0/25 as summary and 192.168.0.0/27 for each floor**



More details Steps:

D. 192.168.0.0/25 as summary and 192.168.0.0/27 for each floor

This means that the overall network would be defined as 192.168.0.0/25, and each floor would be assigned a /27 subnet within that range. This would provide sufficient addresses for each floor and the entire network.

other options:

A. 192.168.0.0/26 as summary and 192.168.0.0/29 for each floor

A /29 subnet only provides 6 usable IP addresses (8 total - 2 for network and broadcast addresses), which is not enough for any floor as they all have more than 6 users. Also, a /26 summary address only provides 64 total addresses, which would not be enough for four /29 subnets (if they were to be adequate in the first place), let alone four /27 subnets.

B. 192.168.0.0/24 as summary and 192.168.0.0/28 for each floor

A /28 subnet provides 14 usable IP addresses (16 total - 2 for network and broadcast addresses), which is not enough for any floor as they all have more than 14 users. The /24 summary address would provide 256 total addresses, which is more than needed for four /27 subnets, but the /28 for each floor isn't sufficient.

C. 192.168.0.0/23 as summary and 192.168.0.0/25 for each floor

A /25 subnet provides 126 usable IP addresses (128 total - 2 for network and broadcast addresses), which is too many for each floor and would result in a lot of wasted addresses. The /23 summary address provides 512 total addresses, which is significantly more than needed for four /27 subnets, leading to an inefficient use of address space.

So, considering the need to provide enough addresses for each floor while also making efficient use of the address space, option **D. 192.168.0.0/25 as summary and 192.168.0.0/27 for each floor** is the best choice among the given options.

Q246: By default, how Does EIGRP determine the metric of a route for the routing table?

- A. it uses the bandwidth and delay values of the path to calculate the route metric
- B. it uses a default metric of 10 for all routes that are learned by the router
- C. it uses a reference Bandwidth and the actual bandwidth of the connected link to calculate the route metric
- D. it counts the number of hops between the receiving and destination routers and uses that value as the metric

▼ Answer

- A. it uses the bandwidth and delay values of the path to calculate the route metric**
- B. it uses a default metric of 10 for all routes that are learned by the router
- C. it uses a reference Bandwidth and the actual bandwidth of the connected link to calculate the route metric
- D. it counts the number of hops between the receiving and destination routers and uses that value as the metric



More details Steps:

- A. it uses the bandwidth and delay values of the path to calculate the route metric

EIGRP (Enhanced Interior Gateway Routing Protocol) is an advanced distance-vector routing protocol that is used on a computer network for automating routing decisions and configuration. By default, EIGRP uses bandwidth and delay of the line to compute the route metric. These metrics are used to calculate the cost of a particular route, with lower cost routes preferred when multiple paths to the same destination exist.

The other options are incorrect:

- B. it uses a default metric of 10 for all routes that are learned by the router

EIGRP does not use a default metric for all routes. It calculates the metric based on the bandwidth and delay values.

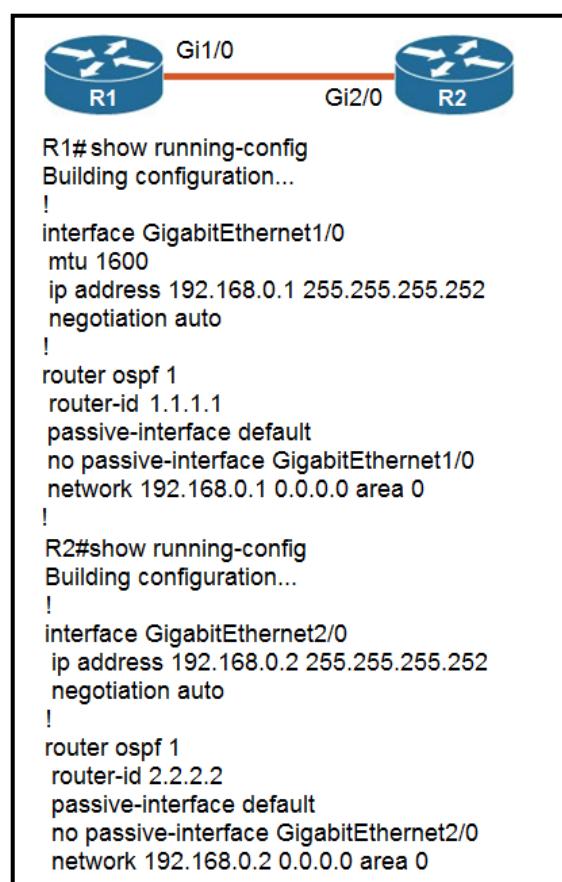
- C. it uses a reference Bandwidth and the actual bandwidth of the connected link to calculate the route metric

This statement is more accurate for OSPF (Open Shortest Path First) which uses a reference bandwidth to calculate the cost, not for EIGRP.

- D. it counts the number of hops between the receiving and destination routers and uses that value as the metric

This method is used by RIP (Routing Information Protocol), not EIGRP. EIGRP uses a more sophisticated metric calculation taking into account bandwidth and delay.

Q247: Refer to the exhibit. Which configuration issue is preventing the OSPF neighbor relationship from being established between the two routers?



- A. R2 is using the passive-interface default command
- B. R1 has an incorrect network command for interface Gi1/0
- C. R2 should have its network command in area 1
- D. R1 interface Gi1/0 has a larger MTU size

▼ Answer

- A. R2 is using the passive-interface default command
- B. R1 has an incorrect network command for interface Gi1/0
- C. R2 should have its network command in area 1
- D. R1 interface Gi1/0 has a larger MTU size**



More details Steps:

D. R1 interface Gi1/0 has a larger MTU size

In OSPF, the MTU (Maximum Transmission Unit) size must match on both sides of the point-to-point link for the OSPF adjacency to form. In the provided configuration, R1 has an MTU size of 1600 on its GigabitEthernet1/0 interface, while R2 has the default MTU size (which is 1500 for Ethernet interfaces) on its GigabitEthernet2/0 interface. This mismatch in MTU size is preventing the OSPF neighbor relationship from being established between R1 and R2.

The other options are incorrect because:

- A. R2 is using the **passive-interface default** command

Both R1 and R2 have the "passive-interface default" command configured under OSPF, but they also both have "no passive-interface" configured on the interfaces that are part of the OSPF network. This means that these interfaces are not passive and can form OSPF adjacencies.

- B. R1 has an incorrect network command for interface Gi1/0

The network command under OSPF on R1 is correct. It is correctly specifying the IP address of the GigabitEthernet1/0 interface and the area it should be part of.

- C. R2 should have its network command in area 1

Both R1 and R2 are configured to be in OSPF area 0 for their respective interfaces, so there is no issue with the area configuration.

Q248: What are two roles of the Dynamic Host Configuration Protocol (DHCP)? (Choose two)

- A. The DHCP server offers the ability to exclude specific IP addresses from a pool of IP addresses
- B. The DHCP client can request up to four DNS server addresses
- C. The DHCP server assigns IP addresses without requiring the client to renew them
- D. The DHCP server leases client IP addresses dynamically.
- E. The DHCP client maintains a pool of IP addresses it can assign.

▼ Answer

- A. The DHCP server offers the ability to exclude specific IP addresses from a pool of IP addresses**
- B. The DHCP client can request up to four DNS server addresses
- C. The DHCP server assigns IP addresses without requiring the client to renew them
- D. The DHCP server leases client IP addresses dynamically.**
- E. The DHCP client maintains a pool of IP addresses it can assign.



More details Steps:

- A. The DHCP server offers the ability to exclude specific IP addresses from a pool of IP addresses**
- D. The DHCP server leases client IP addresses dynamically.**

DHCP (Dynamic Host Configuration Protocol) is a network management protocol used to automate the process of configuring devices on IP networks. Here are the reasons why options A and D are correct:

- **A.** The DHCP server does indeed have the ability to exclude specific IP addresses from the pool it manages. This is useful in situations where certain IP addresses are reserved for specific devices or purposes and should not be assigned to general devices.
- **D.** One of the primary functions of DHCP is to dynamically lease IP addresses to client devices. This means that client devices receive an IP address for a fixed period of time (the lease period) and must renew their lease before it expires to continue using that IP address.

The other options are incorrect because:

- **B.** While DHCP can assign DNS server addresses to clients, the number is not limited to four. The number of DNS servers a DHCP server can assign is not specifically limited by the DHCP protocol.
- **C.** The DHCP server does assign IP addresses dynamically, but these addresses must be renewed by the client. The lease time is determined by the server's configuration, after which the client must renew the lease to continue using the IP address.
- **E.** This statement is incorrect. DHCP clients do not maintain a pool of IP addresses. It is the DHCP server that maintains a pool of IP addresses to assign to clients.

Q249: How does CAPWAP communicate between an access point in local mode and a WLC?

- A. The access point must directly connect to the WLC using a copper cable
- B. The access point must not be connected to the wired network, as it would create a loop
- C. The access point must be connected to the same switch as the WLC
- D. The access point has the ability to link to any switch in the network, assuming connectivity to the WLC

▼ Answer

- A. The access point must directly connect to the WLC using a copper cable
- B. The access point must not be connected to the wired network, as it would create a loop
- C. The access point must be connected to the same switch as the WLC
- D. The access point has the ability to link to any switch in the network, assuming connectivity to the WLC**



More details Steps:

- D. The access point has the ability to link to any switch in the network, assuming connectivity to the WLC**

CAPWAP (Control And Provisioning of Wireless Access Points) is a standard, interoperable protocol that enables a controller (WLC - Wireless LAN Controller) to manage access points (AP) over a network. The AP can be connected to any switch in the network, as long as it has network connectivity to the WLC. It does not have to be directly connected to the WLC or to the same switch as the WLC.

The other options are incorrect because:

- **A. The access point must directly connect to the WLC using a copper cable**
CAPWAP can operate across any IP network, not just directly connected devices.
- **B. The access point must not be connected to the wired network, as it would create a loop**
APs in fact do need to be connected to the wired network to communicate with the WLC and to provide network access to wireless clients.
- **C. The access point must be connected to the same switch as the WLC**
As stated above, the AP does not need to be connected to the same switch as the WLC. It can connect to any switch as long as it has IP connectivity to the WLC.

Q250: Refer to the exhibit. Which action is expected from SW1 when the untagged frame is received on the GigabitEthernet0/1 interface?

```
SW1#show run int gig 0/1
interface GigabitEthernet0/1
  switchport access vlan 11
  switchport trunk allowed vlan 1-10
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 5
  switchport mode trunk
  speed 1000
  duplex full
```

- A. The frame is processed in VLAN 5.
- B. The frame is processed in VLAN 11
- C. The frame is processed in VLAN 1
- D. The frame is dropped

▼ Answer

A. The frame is processed in VLAN 5.

- B. The frame is processed in VLAN 11
- C. The frame is processed in VLAN 1
- D. The frame is dropped



More details Steps:

A. The frame is processed in VLAN 5.

The command "switchport trunk native vlan 5" on the GigabitEthernet0/1 interface means that untagged traffic coming into this port will be associated with VLAN 5. So, if an untagged frame is received on this interface, it will be processed in VLAN 5.

The other options are incorrect because:

- B. The frame is processed in VLAN 11**

VLAN 11 is not even allowed on the trunk, as per the "switchport trunk allowed vlan 1-10" command.

- C. The frame is processed in VLAN 1**

Although VLAN 1 is the default native VLAN on Cisco switches, in this case, the native VLAN has been explicitly changed to VLAN 5.

- D. The frame is dropped**

The frame would only be dropped if it were tagged for a VLAN that is not allowed on the trunk. Since the frame is untagged, it will be associated with the native VLAN (VLAN 5) and processed accordingly.

Q251: What are two reasons for an engineer to configure a floating state route? (Choose two)

- A. to automatically route traffic on a secondary path when the primary path goes down
- B. to route traffic differently based on the source IP of the packet
- C. to enable fallback static routing when the dynamic routing protocol fails
- D. to support load balancing via static routing
- E. to control the return path of traffic that is sent from the router

▼ Answer

A. to automatically route traffic on a secondary path when the primary path goes down

- B. to route traffic differently based on the source IP of the packet

C. to enable fallback static routing when the dynamic routing protocol fails

- D. to support load balancing via static routing

- E. to control the return path of traffic that is sent from the router



More details Steps:

- A. to automatically route traffic on a secondary path when the primary path goes down
- C. to enable fallback static routing when the dynamic routing protocol fails

Floating static routes are static routes that have an administrative distance greater than the primary route (dynamic or static). They are not used in the routing table while the primary route is active.

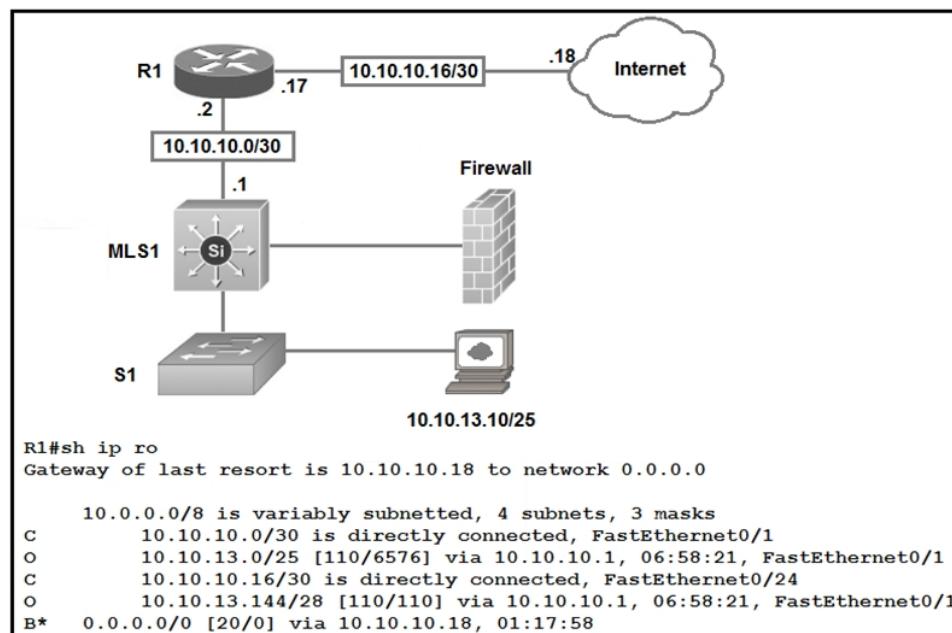
Here are the reasons why options A and C are correct:

- A. A floating static route is often used for failover. If the primary path (which could be a dynamic route or a static route with a lower administrative distance) fails, the router will use the floating static route as a backup path.
- C. Similarly, if a dynamic routing protocol fails to provide a route, the floating static route can be used as a backup.

The other options are incorrect because:

- B. Policy-based routing, not floating static routes, is used to route traffic differently based on the source IP of the packet.
- D. Load balancing is typically achieved with multiple equal-cost paths, not with floating static routes.
- E. Controlling the return path of traffic that is sent from the router typically involves manipulating routing updates or path attributes, not configuring floating static routes.

Q252: Refer to the exhibit. Which type of route does R1 use to reach host 10.10.13.10/32?



- A. floating static route
- B. host route
- C. default route
- D. network route

▼ Answer

- A. floating static route
- B. host route
- C. default route
- D. network route**



More details Steps:

D. network route

The output in the exhibit shows that R1 has several routes to the 10.0.0.0/8 network, and one of them is the network route to 10.10.13.0/25 via the FastEthernet0/1 interface and the next-hop IP 10.10.10.1. Since the IP address 10.10.13.10/32 falls within this subnet, this is the route that R1 would use to reach it.

Here's an explanation of the other options:

- **A. floating static route:** This is a static route with a higher administrative distance making it less preferable than dynamic routes. There's no indication in the exhibit that the route to 10.10.13.10/32 is a floating static route.
- **B. host route:** This is a route to a specific host, i.e., a route with a /32 subnet mask. The route to 10.10.13.10/32 is a network route, not a host route.
- **C. default route:** This is the route that a router uses to send packets for which it doesn't have a specific route. In the exhibit, the default route is to 0.0.0.0/0 via 10.10.10.18, but R1 has a specific route to 10.10.13.10/32, so it wouldn't use the default route.

Q253: How does Cisco DNA Center gather data from the network? A. Network devices use different services like SNMP, syslog, and streaming telemetry to send data to the controller

- A. Network devices use different services like SNMP, syslog, and streaming telemetry to send data to the controller
- B. Devices establish an IPsec tunnel to exchange data with the controller
- C. Devices use the call-home protocol to periodically send data to the controller.
- D. The Cisco CU Analyzer tool gathers data from each licensed network device and streams it to the controller.

▼ Answer

A. Network devices use different services like SNMP, syslog, and streaming telemetry to send data to the controller

- B. Devices establish an IPsec tunnel to exchange data with the controller
- C. Devices use the call-home protocol to periodically send data to the controller.
- D. The Cisco CU Analyzer tool gathers data from each licensed network device and streams it to the controller.



More details Steps:

A. Network devices use different services like SNMP, syslog, and streaming telemetry to send data to the controller

Cisco DNA Center collects data from network devices using various protocols and services, including Simple Network Management Protocol (SNMP), syslog, and streaming telemetry. These services provide a variety of information, such as device status, network performance metrics, and log messages, which are essential for network monitoring and management.

The other options are incorrect because:

• B. Devices establish an IPsec tunnel to exchange data with the controller

While IPsec tunnels can be used for secure data transfer, they are not the primary method for data collection in Cisco DNA Center.

• C. Devices use the call-home protocol to periodically send data to the controller

While some devices may have a "call home" feature for specific purposes, it is not the primary method for data gathering in Cisco DNA Center.

• D. The Cisco CU Analyzer tool gathers data from each licensed network device and streams it to the controller

Cisco CU Analyzer is a specific tool for unified communications, not a general tool for collecting data from network devices for Cisco DNA Center.

Q254: What is the difference regarding reliability and communication type between TCP and UDP?

- A. TCP is reliable and is a connection-oriented protocol UDP is not reliable and is a connectionless protocol
- B. TCP is not reliable and is a connection-oriented protocol; UDP is reliable and is a connectionless protocol
- C. TCP is not reliable and is a connectionless protocol; UDP is reliable and is a connection-oriented protocol
- D. TCP is reliable and is a connectionless protocol; UDP is not reliable and is a connection-oriented protocol

▼ Answer

A. TCP is reliable and is a connection-oriented protocol UDP is not reliable and is a connectionless protocol

- B. TCP is not reliable and is a connection-oriented protocol; UDP is reliable and is a connectionless protocol
- C. TCP is not reliable and is a connectionless protocol; UDP is reliable and is a connection-oriented protocol
- D. TCP is reliable and is a connectionless protocol; UDP is not reliable and is a connection-oriented protocol



More details Steps:

A. TCP is reliable and is a connection-oriented protocol; UDP is not reliable and is a connectionless protocol

TCP (Transmission Control Protocol) is a connection-oriented protocol that provides reliable, ordered, and error-checked delivery of a stream of data between applications running on hosts on a network. It uses acknowledgments, retransmissions, and timeouts to ensure reliable delivery.

On the other hand, UDP (User Datagram Protocol) is a connectionless protocol that does not guarantee delivery, order, or error checking of data. It simply sends the data without establishing a connection and doesn't provide any mechanisms for ensuring that the data is received or correctly ordered.

The other options are incorrect as they incorrectly describe the characteristics of TCP and UDP.

Q255: Drag and drop to the characteristics of networking from the left onto the correct networking types on the right.

Networking	right
Focused on network	Controller-Based Networking
Focused on devices	Traditional Networking
User input is a configuration	Controller-Based Networking
User input is a policy	Traditional Networking
Uses allow list security model	Controller-Based Networking
Uses block list security model	Traditional Networking

▼ Answer

Networking	Controller-Based Networking	Traditional Networking
Focused on network	✓	
Focused on devices		✓
User input is a configuration		✓
User input is a policy	✓	
Uses allow list security model	✓	
Uses block list security model		✓



More details Steps:

In traditional networking, the focus is on individual devices and their configuration. Security is often handled via a block list model, where everything is allowed except what is expressly denied.

On the other hand, controller-based networking, often seen in software-defined networking (SDN) architectures, focuses on the network as a whole. The user input is typically a high-level policy, and the system translates that into device-level configurations. Security is often handled via an allow list model, where everything is denied except what is expressly permitted.

Q256: Several new coverage cells are required to improve the Wi-Fi network of an organization. Which two standard designs are recommended? (Choose two.)

- A. 5GHz provides increased network capacity with up to 23 nonoverlapping channels.
- B. 5GHz channel selection requires an autonomous access point.
- C. Cells that overlap one another are configured to use nonoverlapping channels.
- D. Adjacent cells with overlapping channels use a repeater access point.
- E. For maximum throughput, the WLC is configured to dynamically set adjacent access points to the channel.

▼ Answer

A. 5GHz provides increased network capacity with up to 23 nonoverlapping channels.

B. 5GHz channel selection requires an autonomous access point.

C. Cells that overlap one another are configured to use nonoverlapping channels.

D. Adjacent cells with overlapping channels use a repeater access point.

E. For maximum throughput, the WLC is configured to dynamically set adjacent access points to the channel.



More details Steps:

C. Cells that overlap one another are configured to use nonoverlapping channels.

This is indeed a standard design in Wi-Fi networks. To minimize co-channel interference, overlapping cells should use non-overlapping channels. For example, in a 2.4 GHz band, typically channels 1, 6, and 11 are used as they are non-overlapping.

E. For maximum throughput, the WLC is configured to dynamically set adjacent access points to the channel.

This option seems to refer to a feature of some Wireless LAN Controllers (WLCs) where the controller can dynamically manage the channels that the access points use. This is a technique used to optimize the performance of the network, and it is known as Dynamic Channel Assignment (DCA). DCA allows the WLC to change an AP's channel and power settings based on the RF environment of the AP. The goal of DCA is to reduce co-channel interference and improve network performance.

So, in light of this, you're correct that options C and E represent standard designs to improve a Wi-Fi network. I apologize for the previous confusion.

other options are incorrect:

B. 5GHz channel selection requires an autonomous access point.

This statement is incorrect because the selection of 5GHz channels does not necessarily require an autonomous access point. Both autonomous (standalone) and controller-based access points can operate in the 5GHz band and can select the appropriate channels.

D. Adjacent cells with overlapping channels use a repeater access point.

Repeater access points are typically used to extend the coverage area of the network in places where it's difficult to run network cables. However, using a repeater does not solve the issue of overlapping channels between cells. In fact, it might exacerbate interference problems, especially if the repeater and the original signal are on the same channel. Therefore, this is not a recommended design for improving a Wi-Fi network. It's better to use non-overlapping channels for adjacent cells and extend the network using additional access points connected to the network with Ethernet cables.

Q257: The service password-encryption command is entered on a router. What is the effect of this configuration?

- A. restricts unauthorized users from viewing clear-text passwords in the running configuration
- B. prevents network administrators from configuring clear-text passwords
- C. protects the VLAN database from unauthorized PC connections on the switch
- D. encrypts the password exchange when a VPN tunnel is established

▼ Answer

A. restricts unauthorized users from viewing clear-text passwords in the running configuration

B. prevents network administrators from configuring clear-text passwords

C. protects the VLAN database from unauthorized PC connections on the switch

D. encrypts the password exchange when a VPN tunnel is established



More details Steps:

- A. restricts unauthorized users from viewing clear-text passwords in the running configuration

The `service password-encryption` command is used on Cisco routers to encrypt all plaintext passwords in the configuration file. This means that when someone views the configuration file, the passwords will appear as encrypted strings, not as plain text. This helps to enhance the security of the device by preventing unauthorized individuals from easily reading the passwords.

Here's a brief overview of the other options:

- B. prevents network administrators from configuring clear-text passwords

This is not correct. The command does not prevent admins from configuring clear-text passwords. It just encrypts them in the configuration file.

- C. protects the VLAN database from unauthorized PC connections on the switch

This is not correct. The command has nothing to do with VLANs or protecting against unauthorized PC connections.

- D. encrypts the password exchange when a VPN tunnel is established

This is also not correct. The command does not affect VPN tunnels or the encryption of password exchanges over them.

Q258: Which type of ipv6 address is publicly routable in the same way as ipv4 public addresses?

- A. multicast
- B. unique local
- C. link-local
- D. global unicast

▼ Answer

- A. multicast
- B. unique local
- C. link-local

D. global unicast



More details Steps:

- D. global unicast

Global Unicast Addresses in IPv6 are similar to public IPv4 addresses. They are globally unique, routable on the internet, and can be used to reach IPv6 nodes anywhere in the world.

Here's a brief explanation of the other options:

- A. multicast

IPv6 Multicast addresses are used to send a single packet to multiple destinations. They are not equivalent to public IPv4 addresses.

- B. unique local

Unique Local Addresses in IPv6 are similar to private IPv4 addresses. They are not globally routable and are typically used in local networks.

- C. link-local

Link-Local addresses in IPv6 are used for communication within a single network segment. They are not routable and cannot be used to communicate with nodes on different networks, so they are not equivalent to public IPv4 addresses.

Q259: Which two statements are true about the command ip route 172.16.3.0 255.255.255.0 192.168.2.4? (Choose two.)

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

▼ Answer

A. It establishes a static route to the 172.16.3.0 network.

- B. It establishes a static route to the 192.168.2.0 network.
- C. It configures the router to send any traffic for an unknown destination to the 172.16.3.0 network.
- D. It configures the router to send any traffic for an unknown destination out the interface with the address 192.168.2.4.

E. It uses the default administrative distance.

- F. It is a route that would be used last if other routes to the same destination exist.



More details Steps:

- A. It establishes a static route to the 172.16.3.0 network.

This statement is true. The `ip route` command in this example is used to create a static route to the 172.16.3.0 network. Static routes are manually configured by an administrator and do not change unless the administrator modifies them.

- E. It uses the default administrative distance.

This statement is also true. A static route has a default administrative distance of 1. The administrative distance is a metric used by routers to choose the best path when there are two or more different routes to the same destination from two different routing protocols. The lower the administrative distance, the more trustworthy the route source.

Here's a brief explanation of the other options:

- B. It establishes a static route to the 192.168.2.0 network.

This statement is not true. The static route is established to the 172.16.3.0 network, not the 192.168.2.0 network. The IP address 192.168.2.4 is the next-hop address, indicating the next router in the path to the destination network.

- C. It configures the router to send any traffic for an unknown destination to the 172.16.3.0 network.

This statement is not true. The command sets a static route for a specific network (172.16.3.0), not for unknown destinations. A default route (0.0.0.0) would be used to route traffic to unknown destinations.

- D. It configures the router to send any traffic for an unknown destination out the interface with the address 192.168.2.4.

This statement is not true. The command sets a static route for a specific network (172.16.3.0), not for unknown destinations. A default route would be used to route traffic to unknown destinations.

- F. It is a route that would be used last if other routes to the same destination exist.

This statement is not necessarily true. The route would be used based on its administrative distance and metric, not necessarily used last. In this case, the static route has a default administrative distance of 1, which would typically make it more preferred than routes from most other routing protocols.

Q260: Which three statements are typical characteristics of VLAN arrangements? (Choose three.)

- A. A new switch has no VLANs configured.
- B. Connectivity between VLANs requires a Layer 3 device.

- C. VLANs typically decrease the number of collision domains.
- D. Each VLAN uses a separate address space.
- E. A switch maintains a separate bridging table for each VLAN.
- F. VLANs cannot span multiple switches.

▼ **Answer**

A. A new switch has no VLANs configured.

B. Connectivity between VLANs requires a Layer 3 device.

C. VLANs typically decrease the number of collision domains.

D. Each VLAN uses a separate address space.

E. A switch maintains a separate bridging table for each VLAN.

F. VLANs cannot span multiple switches.



More details Steps:

B. Connectivity between VLANs requires a Layer 3 device.

This statement is true. VLANs segment a network at Layer 2, meaning they operate in a way that logically segments a switch into separate subnetworks. Because of this, communication between different VLANs requires a Layer 3 device, like a router or a Layer 3 switch, to facilitate inter-VLAN routing.

D. Each VLAN uses a separate address space.

This statement is also true. Each VLAN typically has its own IP subnet, which means it uses a separate address space. This separation allows for effective network segmentation, better management of network traffic, and increased security.

E. A switch maintains a separate bridging table for each VLAN.

This statement is true. A switch maintains a separate MAC address (or bridging) table for each VLAN. Each of these tables includes the MAC addresses of all devices that belong to a particular VLAN.

Here's a brief explanation of the other options:

A. A new switch has no VLANs configured.

This statement is not true. By default, all ports on a switch belong to VLAN 1. So, a new switch does have a VLAN configured, specifically VLAN 1.

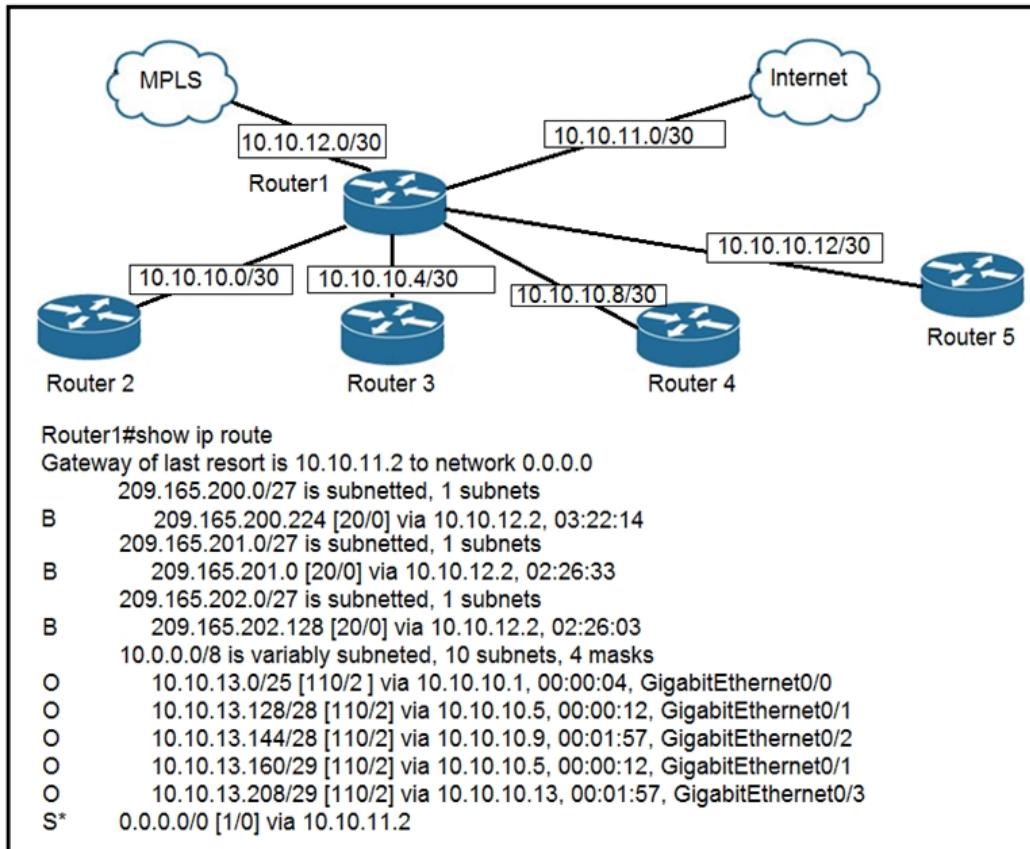
C. VLANs typically decrease the number of collision domains.

This statement is not true. Each switch port is its own collision domain. Implementing VLANs doesn't change this. Rather, VLANs increase the number of broadcast domains.

F. VLANs cannot span multiple switches.

This statement is not true. VLANs can span across multiple switches. This is achieved by trunking using protocols such as IEEE 802.1Q. Trunk links carry traffic from multiple VLANs across switches.

Q261: Refer to the exhibit. To which device does Router1 send packets that are destined to host 10.10.13.165?



- A. Router2
- B. Router3
- C. Router4
- D. Router5

▼ Answer

- A. Router2
- B. Router3**
- C. Router4
- D. Router5



More details Steps:

- B. Router3

The output from the `show ip route` command on Router1 indicates that packets destined for the 10.10.13.160/29 subnet, which includes the IP address 10.10.13.165, are sent via the gateway at 10.10.10.5 (see the line "10.10.13.160/29 [110/21] via 10.10.10.5, 00:00:12, GigabitEthernet0/1").

However, without an actual exhibit or diagram, it's impossible to definitively say which router corresponds to the IP address 10.10.10.5. If that IP address belongs to Router3, then yes, Router1 would send packets destined for 10.10.13.165 to Router3, thus making option B correct.

A. Router2

Router1 would not send the packets to Router2 because, according to the `show ip route` output, the gateway for the IP address 10.10.13.165 (which falls within the 10.10.13.160/29 subnet) is 10.10.10.5, not a gateway that Router2 would represent.

C. Router4

Similarly, Router1 would not send the packets to Router4 because the gateway for the IP address 10.10.13.165 is 10.10.10.5, not a gateway that Router4 would represent.

D. Router5

Router1 would not send the packets to Router5 because the gateway for the IP address 10.10.13.165 is 10.10.10.5, not a gateway that Router5 would represent.

Q262: Refer to the exhibit. Which two commands were used to create port channel 10? (Choose two.)

Switch#show etherchannel summary [output omitted]				
Group	Port-channel	Protocol	Ports	
10	Po10(SU)	LACP	Gi0/0(P)	Gi0/1(P)
20	Po20(SU)	LACP	Gi0/2(P)	Gi0/3(P)

- A. int range g0/0-1 channel-group 10 mode active
- B. int range g0/0-1 channel-group 10 mode desirable
- C. int range g0/0-1 channel-group 10 mode passive
- D. int range g0/0-1 channel-group 10 mode auto
- E. int range g0/0-1 channel-group 10 mode on

▼ Answer

- A. int range g0/0-1 channel-group 10 mode active**
- B. int range g0/0-1 channel-group 10 mode desirable
- C. int range g0/0-1 channel-group 10 mode passive**
- D. int range g0/0-1 channel-group 10 mode auto
- E. int range g0/0-1 channel-group 10 mode on



More details Steps:

- A. int range g0/0-1 channel-group 10 mode active
- C. int range g0/0-1 channel-group 10 mode passive

The `show etherchannel summary` command output in the exhibit shows that the protocol for Port-channel 10 is LACP (Link Aggregation Control Protocol). The LACP mode can be either "active" or "passive".

With "active" mode, the port actively sends LACP packets, and with "passive" mode, the port only responds to LACP packets it receives.

The "channel-group" command is used to assign an interface to a specific EtherChannel group. In this case, the interfaces g0/0 and g0/1 are assigned to the channel group 10.

Here's a brief explanation of the other options:

- B. int range g0/0-1 channel-group 10 mode desirable

This command would be used with PAgP (Port Aggregation Protocol), not LACP.

- D. int range g0/0-1 channel-group 10 mode auto

This command would also be used with PAgP, not LACP.

- E. int range g0/0-1 channel-group 10 mode on

This command would force the interfaces into an EtherChannel without any negotiation protocol (LACP or PAgP). This is not shown in the exhibit.

Q263: What are two requirements for an HSRP group? (Choose two.)

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

▼ Answer

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

E. exactly one backup virtual router



More details Steps:

A. exactly one active router

This is correct. In an HSRP (Hot Standby Router Protocol) deployment, there is exactly one active router that handles all the traffic for the group. This router assumes the role of forwarding packets sent to the virtual IP address for the group.

D. exactly one standby active router

This statement seems to be a combination of two different states of an HSRP router - 'standby' and 'active'. It's important to note that in HSRP, a router cannot be 'standby' and 'active' at the same time. These are two different states. The 'active' router is the one that currently forwards packets while the 'standby' router is the one that takes over if the active router fails. Therefore, this statement isn't typically correct in the context of HSRP.

B. one or more standby routers

While it is possible to have multiple routers configured for HSRP, only one of these can be in the standby state at a time. The other routers would be in the listen or speak state. Therefore, while you can technically have multiple HSRP routers, you cannot have "one or more standby routers" at the same time.

C. one or more backup virtual routers

In HSRP, there is no concept of "backup virtual routers." The protocol operates with the concept of an active router and a standby router (with potentially several others in listen or speak state), all of which share a virtual IP address. There's no "backup virtual router" in this setup.

E. exactly one backup virtual router

As mentioned above, HSRP does not utilize "backup virtual routers." Therefore, this option is not correct.

Q264: What occurs to frames during the process of frame flooding?

- A. Frames are sent to all ports, including those that are assigned to other VLANs.
- B. Frames are sent to every port on the switch that has a matching entry in MAC address table.
- C. Frames are sent to every port on the switch in the same VLAN except from the originating port.
- D. Frames are sent to every port on the switch in the same VLAN.

▼ Answer

- A. Frames are sent to all ports, including those that are assigned to other VLANs.
- B. Frames are sent to every port on the switch that has a matching entry in MAC address table.
- C. Frames are sent to every port on the switch in the same VLAN except from the originating port.**
- D. Frames are sent to every port on the switch in the same VLAN.

**More details Steps:**

C. Frames are sent to every port on the switch in the same VLAN except from the originating port.

Frame flooding is a technique used by switches when they don't know on which port the destination device (with a specific MAC address) is located, or when they receive a broadcast frame. In this situation, the switch will forward the incoming frame to all its ports, except for the port on which the frame was received. This is done within the same VLAN, as switches will not forward frames to ports that belong to a different VLAN.

Here's a brief explanation of the other options:

A. Frames are sent to all ports, including those that are assigned to other VLANs.

This is incorrect. In a switched environment, frames are not sent to ports assigned to other VLANs due to VLAN segmentation, which isolates traffic within the same VLAN.

B. Frames are sent to every port on the switch that has a matching entry in MAC address table.

This is incorrect. If the switch knows the port associated with the destination MAC address (i.e., it has a matching entry in its MAC address table), it will not flood the frame but will instead send it only to the specific port where the destination device is located.

D. Frames are sent to every port on the switch in the same VLAN.

This is partially correct, but it's missing an important detail. Frames are indeed sent to every port on the switch in the same VLAN, but not to the port from which the frame originated.

Q265: If all OSPF routers in a single area are configured with the same priority value, what value does a router use for the OSPF router ID in the absence of a loopback interface?

A. the IP address of the first Fast Ethernet interface

B. the IP address of the console management interface

C. the highest IP address among its active interfaces

D. the lowest IP address among its active interfaces

E. the priority value until a loopback interface is configured

▼ Answer

A. the IP address of the first Fast Ethernet interface

B. the IP address of the console management interface

C. the highest IP address among its active interfaces

D. the lowest IP address among its active interfaces

E. the priority value until a loopback interface is configured



More details Steps:

C. the highest IP address among its active interfaces

The OSPF router ID is chosen according to the following order of precedence:

1. The highest loopback (logical) IP address.
2. If there are no loopback interfaces, the highest IP address of all active router's physical interfaces is chosen.

So, in the absence of a loopback interface, the router will use the highest IP address among its active interfaces.

Here's a brief explanation of the other options:

A. the IP address of the first Fast Ethernet interface

This is incorrect. The router ID is not necessarily the IP address of the first Fast Ethernet interface.

B. the IP address of the console management interface

This is incorrect. The router ID is not necessarily the IP address of the console management interface.

D. the lowest IP address among its active interfaces

This is incorrect. The router ID is the highest, not the lowest, IP address among its active interfaces.

E. the priority value until a loopback interface is configured

This is incorrect. The priority value is not used as a router ID. It's used to determine the Designated Router (DR) and Backup Designated Router (BDR) in a broadcast or non-broadcast multiaccess (NBMA) network.

Q266: Which IPv6 address block forwards packets to a multicast address rather than a unicast address?

A. 2000::/3

B. FC00::/7

C. FE80::/10

D. FF00::/12

▼ Answer

A. 2000::/3

B. FC00::/7

C. FE80::/10

D. FF00::/12



More details Steps:

D. FF00::/12

The IPv6 address block FF00::/12 is reserved for multicast addresses. Multicast addresses are used to send packets to multiple interfaces (usually a group of interfaces on different nodes), rather than a single interface as in unicast transmission.

Here's a brief explanation of the other options:

A. 2000::/3

This block contains all the globally routable unicast addresses.

B. FC00::/7

This is the block for Unique Local Addresses (ULAs), which are intended for local communication within a site and are not routable on the internet.

C. FE80::/10

This is the block for link-local addresses, which are used for communication in a single network link. Link-local addresses are not routable beyond their network link.

Q267: What are two functions carried out by the OSPF Hello protocol? (Choose two.)

- A. It sets correctness parameters between neighboring interfaces.
- B. It sends hello packets across the network to identify all routers running OSPF.
- C. It enables dynamic discovery of neighboring routers.
- D. It identifies unreachable neighbors every 90 seconds.
- E. It employs timers to select the router with the most rapid links as the designated router.
- F. It keeps track of neighbor relationships.

▼ Answer

- A. It sets correctness parameters between neighboring interfaces.
- B. It sends hello packets across the network to identify all routers running OSPF.
- C. It enables dynamic discovery of neighboring routers.**
- D. It identifies unreachable neighbors every 90 seconds.
- E. It employs timers to select the router with the most rapid links as the designated router.
- F. It keeps track of neighbor relationships.**



More details Steps:

- C. It enables dynamic discovery of neighboring routers.
- F. It keeps track of neighbor relationships.

OSPF (Open Shortest Path First) uses a Hello protocol for several reasons:

- OSPF Hello protocol enables the dynamic discovery of neighboring routers on the same network segment. Through the exchange of hello packets, OSPF routers learn about the presence of each other.
- The Hello protocol is also used to maintain neighbor relationships (adjacencies). Once the adjacency is established, hello packets are used to ensure that the link to the neighbor is still up. If hello packets stop being received from a neighbor, the OSPF process will eventually declare the neighbor as down.

Here's a brief explanation of the other options:

- A. It sets correctness parameters between neighboring interfaces.

This is not a function of the OSPF Hello protocol. The Hello protocol is used for discovery of neighbors and maintaining neighbor relationships, not for setting "correctness parameters."

- B. It sends hello packets across the network to identify all routers running OSPF.

This is not accurate. Hello packets are sent only to other OSPF routers on the same network segment, not across the entire network.

- D. It identifies unreachable neighbors every 90 seconds.

Hello packets are used to maintain neighbor relationships, but the exact timer may vary. The default Hello interval is 10 seconds for OSPF on most networks, and 30 seconds for OSPF on non-broadcast networks.

- E. It employs timers to select the router with the most rapid links as the designated router.

This is incorrect. The election of the Designated Router (DR) does not depend on link speed or Hello timers. The DR election is based on router priority, and in case of a tie, the router with the highest Router ID is elected.

Q268: What are two advantages of implementing VTP in a switch environment? (Choose two.)

- A. It enables switches to interpret frame tags.
- B. It facilitates automatic VLAN assignment to ports.
- C. It ensures VLAN consistency across a switched network.
- D. It allows frames from multiple VLANs to utilize a single interface.
- E. It enables automatic propagation of VLAN information throughout the switch network.

▼ Answer

- A. It enables switches to interpret frame tags.
- B. It facilitates automatic VLAN assignment to ports.
- C. It ensures VLAN consistency across a switched network.**
- D. It allows frames from multiple VLANs to utilize a single interface.
- E. It enables automatic propagation of VLAN information throughout the switch network.**



More details Steps:

- C. It ensures VLAN consistency across a switched network.
- E. It enables automatic propagation of VLAN information throughout the switch network.

VLAN Trunking Protocol (VTP) is a Cisco protocol that propagates the definition of VLANs on the whole local area network. The main advantages of implementing VTP in a switch environment are:

- It ensures VLAN consistency across a switched network. Without VTP, each switch must be configured with VLANs individually which can lead to inconsistencies if not properly managed.
- It enables automatic propagation of VLAN information throughout the switch network. When you configure a new VLAN on one VTP server, the VLAN is distributed through all switches in the domain. This reduces the need for complex VLAN configuration on a network-wide basis.

Here's a brief explanation of the other options:

- A. It enables switches to interpret frame tags.

This is not a function of VTP. Frame tagging is a function of VLANs and the 802.1Q protocol, not VTP.

- B. It facilitates automatic VLAN assignment to ports.

This is not a function of VTP. Automatic VLAN assignment to ports can be achieved with protocols like Dynamic Host Configuration Protocol (DHCP) or the use of dynamic VLAN assignment with a VLAN Membership Policy Server (VMPS), but not with VTP.

- D. It allows frames from multiple VLANs to utilize a single interface.

This is not a function of VTP. This is a characteristic of trunk ports, which can carry traffic from multiple VLANs, not of VTP.

Q269: Which purpose does a northbound API serve in a controller-based networking architecture?

- A. communicates between the controller and the physical network hardware
- B. reports device errors to a controller
- C. generates statistics for network hardware and traffic
- D. facilitates communication between the controller and the applications

▼ Answer

- A. communicates between the controller and the physical network hardware
- B. reports device errors to a controller
- C. generates statistics for network hardware and traffic
- D. facilitates communication between the controller and the applications**



More details Steps:

D. facilitates communication between the controller and the applications

In a Software-Defined Networking (SDN) architecture, APIs (Application Programming Interfaces) are used to facilitate communication between different software components. These APIs can be categorized as northbound or southbound.

- **Northbound APIs** are used for communication between the SDN controller and the applications or higher-level orchestration systems. They allow applications to program the network and request services from the network.

Here's a brief explanation of the other options:

A. communicates between the controller and the physical network hardware

This function is served by southbound APIs, not northbound APIs. Southbound APIs are used for communication between the SDN controller and the network devices (like switches and routers).

B. reports device errors to a controller

While this could be part of the functionality of southbound APIs, it is not the primary purpose of northbound APIs.

C. generates statistics for network hardware and traffic

While this is part of the broader SDN functionality, it's not the specific role of northbound APIs. This functionality would be performed by the controller, which collects information from network devices via southbound APIs and can provide it to applications via northbound APIs.

Q270: What are two tasks performed by the OSPF Hello protocol? (Choose two.)

- A. It allows dynamic neighbor discovery.
- B. It detects unreachable neighbors at 90 seconds intervals.
- C. It maintains relationships between neighboring routers.
- D. It negotiates correctness parameters between neighboring interfaces.
- E. It uses timers to elect the router with the quickest links as the designated router.
- F. It broadcasts hello packets across the network to discover all routers running OSPF.

▼ Answer

A. It allows dynamic neighbor discovery.

B. It detects unreachable neighbors at 90 seconds intervals.

C. It maintains relationships between neighboring routers.

D. It negotiates correctness parameters between neighboring interfaces.

E. It uses timers to elect the router with the quickest links as the designated router.

F. It broadcasts hello packets across the network to discover all routers running OSPF.



More details Steps:

- A. It allows dynamic neighbor discovery.
- C. It maintains relationships between neighboring routers.

OSPF (Open Shortest Path First) uses a Hello protocol for several reasons:

- OSPF Hello protocol enables the dynamic discovery of neighboring routers on the same network segment. Through the exchange of hello packets, OSPF routers learn about the presence of each other.
- The Hello protocol is also used to maintain neighbor relationships (adjacencies). Once the adjacency is established, hello packets are used to ensure that the link to the neighbor is still up. If hello packets stop being received from a neighbor, the OSPF process will eventually declare the neighbor as down.

Here's a brief explanation of the other options:

- B. It detects unreachable neighbors at 90 seconds intervals.

Hello packets are used to maintain neighbor relationships, but the exact timer may vary. The default Hello interval is 10 seconds for OSPF on most networks, and 30 seconds for OSPF on non-broadcast networks.

- D. It negotiates correctness parameters between neighboring interfaces.

This is not a function of the OSPF Hello protocol. The Hello protocol is used for discovery of neighbors and maintaining neighbor relationships, not for negotiating "correctness parameters."

- E. It uses timers to elect the router with the quickest links as the designated router.

This is incorrect. The election of the Designated Router (DR) does not depend on link speed or Hello timers. The DR election is based on router priority, and in case of a tie, the router with the highest Router ID is elected.

- F. It broadcasts hello packets across the network to discover all routers running OSPF.

This is not accurate. Hello packets are sent only to other OSPF routers on the same network segment, not across the entire network.

Q271: What are two reasons for a network administrator to use CDP? (Choose two.)

- A. To verify the type of cable connecting two devices.
- B. To check the status of network services on a remote device.
- C. To gather VLAN information from directly connected switches.
- D. To confirm Layer 2 connectivity between two devices when Layer 3 fails.
- E. To acquire the IP address of a connected device for telnet access.
- F. To check the status of routing protocols between directly connected routers.

▼ Answer

- A. To verify the type of cable connecting two devices.
- B. To check the status of network services on a remote device.
- C. To gather VLAN information from directly connected switches.

D. To confirm Layer 2 connectivity between two devices when Layer 3 fails.

E. To acquire the IP address of a connected device for telnet access.

- F. To check the status of routing protocols between directly connected routers.



More details Steps:

- D. To confirm Layer 2 connectivity between two devices when Layer 3 fails.
- E. To acquire the IP address of a connected device for telnet access.

Cisco Discovery Protocol (CDP) is a Cisco proprietary protocol that is used to discover other Cisco devices on directly connected networks. CDP can be a very useful diagnostic tool for a network administrator.

Here's why:

- CDP can be used to confirm Layer 2 connectivity between two devices when Layer 3 fails. If two devices are connected at Layer 2 but not at Layer 3, CDP can be used to help diagnose the problem.
- CDP can be used to acquire the IP address of a connected device for telnet access. If you can see a device in the CDP neighbor table, you can access it for further management or troubleshooting.

Here's a brief explanation of the other options:

- A. To verify the type of cable connecting two devices.

CDP does not provide specific information about the type of cable connecting devices. It can provide detailed information about the connected device, such as device ID, software version, platform, capabilities, and the interface on which the report is sent.

- B. To check the status of network services on a remote device.

CDP does not provide information about the status of network services on a remote device. Its purpose is to identify information about directly connected Cisco devices.

- C. To gather VLAN information from directly connected switches.

CDP does not provide VLAN information. It can provide information about the capabilities of the device, including whether it's a switch, but not specific details about VLAN configuration.

- F. To check the status of routing protocols between directly connected routers.

CDP does not provide information about the status of routing protocols. Its purpose is to identify information about directly connected Cisco devices, not the status of routing protocols.

Q272: Refer to the exhibit. An administrator is tasked with configuring a voice VLAN. What is the expected outcome when a Cisco phone is connected to the GigabitEthernet 3/1/4 port on a switch?

```
interface GigabitEthernet3/1/4
switchport voice vlan 50
!
```

- A. The phone and a workstation that is connected to the phone do not have VLAN connectivity.
- B. The phone sends and receives data in VLAN 50, but a workstation connected to the phone sends and receives data in VLAN 1.
- C. The phone sends and receives data in VLAN 50, but a workstation connected to the phone has no VLAN connected.
- D. The phone and a workstation that is connected to the phone send and receive data in VLAN 50.

▼ Answer

- A. The phone and a workstation that is connected to the phone do not have VLAN connectivity.
- B. The phone sends and receives data in VLAN 50, but a workstation connected to the phone sends and receives data in VLAN 1.**
- C. The phone sends and receives data in VLAN 50, but a workstation connected to the phone has no VLAN connected.
- D. The phone and a workstation that is connected to the phone send and receive data in VLAN 50.



More details Steps:

B. The phone sends and receives data in VLAN 50, but a workstation connected to the phone sends and receives data in VLAN 1.

The `switchport voice vlan` command is used to specify the VLAN that will carry voice traffic from a Cisco IP phone. When a Cisco phone is connected to a switch port configured with a voice VLAN, the phone will tag its voice traffic with the voice VLAN ID.

In this scenario, the command `switchport voice vlan 50` means that the phone will send and receive voice traffic in VLAN 50.

However, if a workstation is also connected to the phone (as is common with IP phones, which often act as a two-port switch), the workstation's traffic will be untagged and thus will belong to the native VLAN of the switch port, which is VLAN 1 by default.

Here's a brief explanation of the other options:

A. The phone and a workstation that is connected to the phone do not have VLAN connectivity.

This is incorrect because both the phone and the workstation will have VLAN connectivity, but in different VLANs (50 for the phone, 1 for the workstation).

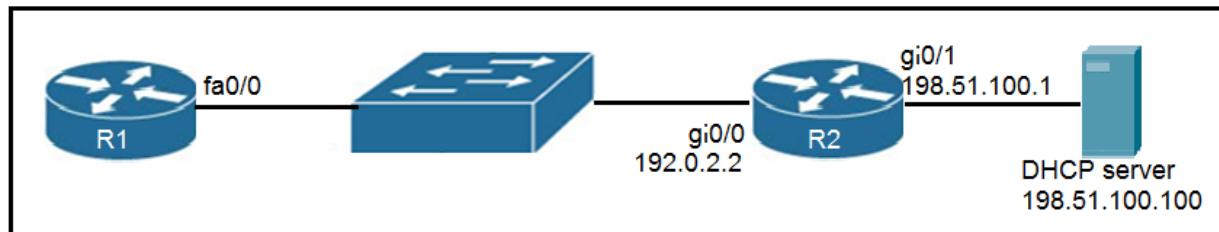
C. The phone sends and receives data in VLAN 50, but a workstation connected to the phone has no VLAN connected.

This is incorrect because the workstation connected to the phone will send and receive data on the native VLAN, which is VLAN 1 by default.

D. The phone and a workstation that is connected to the phone send and receive data in VLAN 50.

This is incorrect because while the phone will send and receive data in VLAN 50, a connected workstation will send and receive data on the native VLAN, which is VLAN 1 by default.

Q273: Refer to the exhibit. An engineer deploys a topology in which R1 obtains its IP configuration from DHCP. If the switch and DHCP server configurations are complete and correct. Which two sets of commands must be configured on R1 and R2 to complete the task? (Choose two)



A.

```
R1(config)# interface fa0/0
R1(config-if)# ip helper-address 198.51.100.100
```



B.

```
R2(config)# interface gi0/0
R2(config-if)# ip helper-address 198.51.100.100
```



C.

```
R1(config)# interface fa0/0
R1(config-if)# ip address dhcp
R1(config-if)# no shutdown
```

?

D.
R2(config)# interface gi0/0
R2(config-if)# ip address dhcp

?

E.
R1(config)# interface fa0/0
R1(config-if)# ip helper-address 192.0.2.2

▼ Answer

?

A.
R1(config)# interface fa0/0
R1(config-if)# ip helper-address 198.51.100.100

?

B.
R2(config)# interface gi0/0
R2(config-if)# ip helper-address 198.51.100.100

?

C.
R1(config)# interface fa0/0
R1(config-if)# ip address dhcp
R1(config-if)# no shutdown

?

D.
R2(config)# interface gi0/0
R2(config-if)# ip address dhcp

?

E.
R1(config)# interface fa0/0
R1(config-if)# ip helper-address 192.0.2.2



More details Steps:

B. R2(config)# interface gi0/0
R2(config-if)# ip helper-address 198.51.100.100
C. R1(config)# interface fa0/0
R1(config-if)# ip address dhcp
R1(config-if)# no shutdown

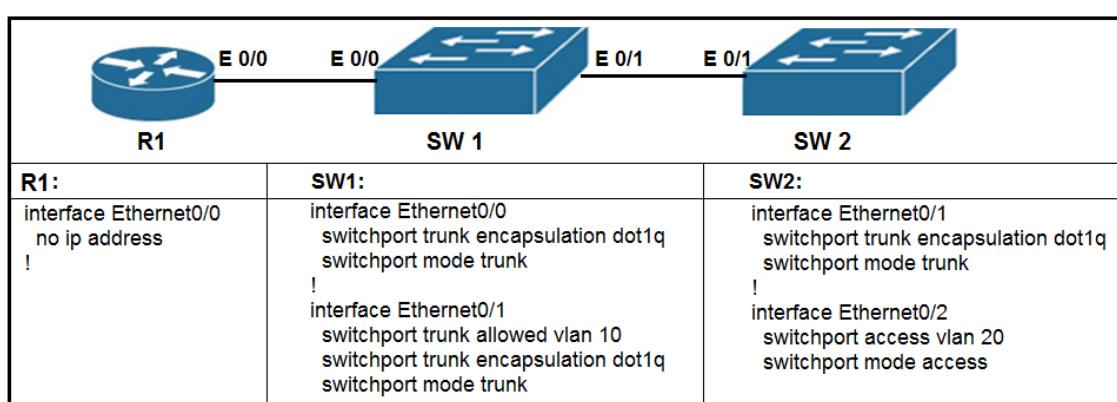
Here's why:

- Option B: The `ip helper-address` command is used to forward DHCP broadcast requests as unicast transmissions to a specific DHCP server when the server is not on the same subnet. In this case, the DHCP server is not in the same subnet as the router R1, and hence R2 needs to forward the DHCP request from R1 to the DHCP server. Hence, the `ip helper-address` command should be applied on the interface of R2 that is connected to the segment with the DHCP server.
- Option C: On R1, the interface connecting to R2 should be configured to obtain an IP address from a DHCP server. The `ip address dhcp` command is used to enable the interface to dynamically obtain an IP address from a DHCP server. The `no shutdown` command is used to make sure that the interface is up and running.

Here's a brief explanation of the other options:

- Option A: This is not correct because R1 does not need to forward DHCP requests. The `ip helper-address` command should be used on a router interface that needs to forward DHCP requests to a server on a different subnet.
- Option D: This is not correct because R2 does not need to obtain an IP address from a DHCP server. The `ip address dhcp` command should be used on an interface that needs to obtain an IP address from a DHCP server.
- Option E: This is not correct because the `ip helper-address` should point to the DHCP server's IP address (198.51.100.100), not the IP address of the interface on R2 (192.0.2.2).

Q274: Refer to the exhibit. What commands are needed to add a subinterface to Ethernet0/0 on R1 to allow for VLAN 20, with IP address 10.20.20.1/24?



A.
R1(config)#interface ethernet0/0
R1(config)#encapsulation dot1q 20
R1(config)#ip address 10.20.20.1 255.255.255.0



B.
R1(config)#interface ethernet0/0.20
R1(config)#encapsulation dot1q 20
R1(config)#ip address 10.20.20.1 255.255.255.0



C.
R1(config)#interface ethernet0/0.20
R1(config)#ip address 10.20.20.1 255.255.255.0



D.
R1(config)#interface ethernet0/0
R1(config)#ip address 10.20.20.1 255.255.255.0

▼ Answer



A.
R1(config)#interface ethernet0/0
R1(config)#encapsulation dot1q 20
R1(config)#ip address 10.20.20.1 255.255.255.0



B.
R1(config)#interface ethernet0/0.20
R1(config)#encapsulation dot1q 20
R1(config)#ip address 10.20.20.1 255.255.255.0



C.
R1(config)#interface ethernet0/0.20
R1(config)#ip address 10.20.20.1 255.255.255.0



D.
R1(config)#interface ethernet0/0
R1(config)#ip address 10.20.20.1 255.255.255.0



More details Steps:

B.
R1(config)#interface ethernet0/0.20
R1(config-subif)#encapsulation dot1q 20
R1(config-subif)#ip address 10.20.20.1 255.255.255.0

Here's why:

- `interface ethernet0/0.20` creates a subinterface on Ethernet0/0 for VLAN 20.
- `encapsulation dot1q 20` specifies that traffic on this subinterface should be tagged with VLAN ID 20, according to the 802.1Q VLAN tagging standard.
- `ip address 10.20.20.1 255.255.255.0` assigns the IP address 10.20.20.1 with a subnet mask of 255.255.255.0 to this subinterface.

Here's why the other options are incorrect:

- Option A: This is incorrect because it tries to apply the configuration to the main interface Ethernet0/0, not the subinterface for VLAN 20.
- Option C: This is incorrect because it omits the `encapsulation dot1q 20` command, which is necessary to specify that traffic on this subinterface should be tagged with VLAN ID 20.
- Option D: This is incorrect because it tries to apply the IP address to the main interface Ethernet0/0 without creating a subinterface for VLAN 20, and it omits the `encapsulation dot1q 20` command.

Q275: On a corporate network, hosts on the same VLAN can communicate with each other, but they are unable to communicate with hosts on different VLANs. What is needed to allow communication between the VLANs?

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

▼ Answer

A. a router with subinterfaces configured on the physical interface that is connected to the switch

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



More details Steps:

- A. a router with subinterfaces configured on the physical interface that is connected to the switch

In order to allow communication between VLANs, you need to implement Inter-VLAN routing. This can be achieved by using a router with different subinterfaces for each VLAN. Each subinterface on the router is configured for a different VLAN and has its own IP address in the corresponding VLAN's subnet. This setup is often referred to as a "Router on a Stick".

Here's why the other options are incorrect:

- Option B: Having an IP address on the physical interface of a router would not be sufficient for Inter-VLAN routing. The router must be configured with subinterfaces for each VLAN.
- Option C: An access link between switches would not allow for Inter-VLAN routing. Access links carry traffic for a single VLAN.
- Option D: A trunk link is used to carry traffic from multiple VLANs between switches or to a router, but a trunk link in itself does not provide Inter-VLAN routing. The traffic still needs to be routed by a device that is capable of Layer 3 operations, such as a router or a Layer 3 switch.

Q276: Which command can you enter to determine the addresses that have been assigned on a DHCP Server?

- A. Show ip DHCP database.
- B. Show ip DHCP pool.
- C. Show ip DHCP binding.
- D. Show ip DHCP server statistic.

▼ Answer

A. Show ip DHCP database.

B. Show ip DHCP pool.

C. Show ip DHCP binding.

D. Show ip DHCP server statistic.



More details Steps:

- A. `Show ip DHCP database`: This command is used to display the database agent settings and URL for the DHCP server database. It does not specifically show the addresses assigned by the DHCP server.
- B. `Show ip DHCP pool`: This command displays information related to the DHCP address pools the server is managing. While it does provide statistics on how many addresses are used/available, it does not show the specific addresses currently assigned.
- C. `Show ip DHCP binding`: This command displays the list of all assigned IP addresses and their corresponding MAC addresses. The display includes the IP address, MAC address, lease expiration time, and the type of binding (manual or automatic). This is the command you would use to see which addresses have been assigned by the DHCP server.
- D. `Show ip DHCP server statistic`: This command displays statistics about the server, such as the number of DHCPDISCOVER packets received, the number of DHCPOFFER packets sent, etc. While it provides useful information about the operation of the DHCP server, it does not display the specific addresses assigned.

Q277: Refer to the exhibit. If the network environment is operating normally, which type of device must be connected to interface FastEthernet 0/1?

```
ip arp inspection vlan 2-10
interface fastethernet 0/1
ip arp inspection trust
```

- A. DHCP client
- B. access point
- C. router
- D. PC

▼ Answer

- A. DHCP client
- B. access point
- C. router**
- D. PC



More details Steps:

C. Router.

Here's why:

The FastEthernet 0/1 interface is configured as a **trunk** port. A trunk port is typically used to connect two switches together, but it can also be used to connect other types of network devices that understand VLAN tagging, such as a router.

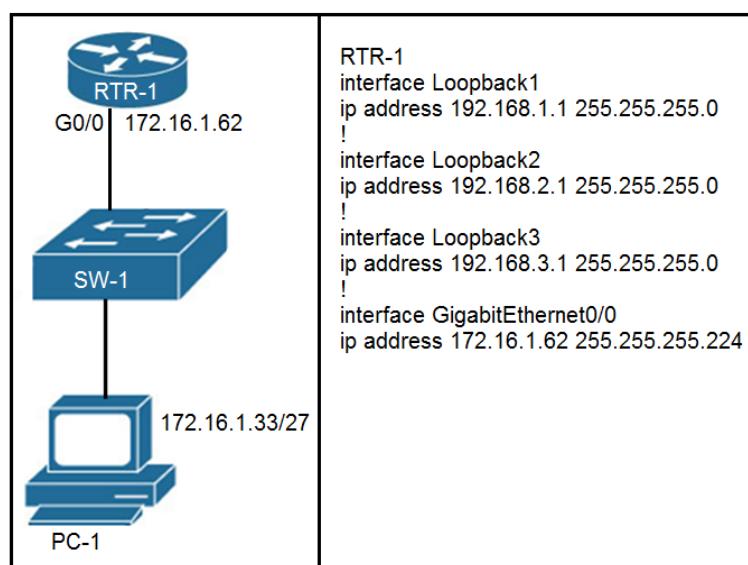
Trunk ports carry traffic from multiple VLANs across a single physical link, using an identification tag (VLAN ID) for each frame of data to identify the VLAN to which it belongs. This makes it possible to transport data for multiple VLANs across a single link.

In a typical network environment:

- **A. DHCP client:** A DHCP client would not be directly connected to a trunk port. A DHCP client is typically an end device like a PC or wireless device, which would connect to an access port, not a trunk port.
- **B. Access point:** While it's possible for an access point to connect to a trunk port if it's supporting multiple SSIDs each associated with a different VLAN, it's not the only device that can connect to a trunk port.
- **D. PC:** A PC is typically connected to an access port on a switch, not a trunk port. PCs usually do not understand VLAN tagging, so they need to connect to an access port where the VLAN tagging/untagging is handled by the switch.

So, given the options, a router is the most likely device to be connected to a trunk port because routers can understand and manage VLAN tagging. This setup would be commonly used in a router-on-a-stick configuration, where a single router interface is used to route traffic between multiple VLANs.

Q278: Refer to the exhibit. What configuration on RTR-1 denies SSH access from PC-1 to any RTR-1 interface and allows all other traffic?



A.

```
access-list 100 deny tcp host 172.16.1.33 any eq 22
```

```
access-list 100 permit ip any any
```

```
interface GigabitEthernet0/0
```

```
ip access-group 100 in
```

B.

```
access-list 100 deny tcp host 172.16.1.33 any eq 22
```

```
access-list 100 permit ip any any
```

```
line vty 0 15
```

```
access-class 100 in
```

C.

```
access-list 100 deny tcp host 172.16.1.33 any eq 23
```

```
access-list 100 permit ip any any
```

```
interface Gigabit Ethernet0/0
```

```
ip access-group 100 in
```

D.

```
access-list 100 deny tcp host 172.16.1.33 any eq 23
```

```
access-list 100 permit ip any any
```

```
line vty 0 15
```

```
access-class 100 in
```

▼ Answer

A.

```
access-list 100 deny tcp host 172.16.1.33 any eq 22
```

```
access-list 100 permit ip any any
```

```
interface GigabitEthernet0/0
```

```
ip access-group 100 in
```

B.

access-list 100 deny tcp host 172.16.1.33 any eq 22

access-list 100 permit ip any any

line vty 0 15

access-class 100 in

C.

```
access-list 100 deny tcp host 172.16.1.33 any eq 23
```

```
access-list 100 permit ip any any
```

```
interface Gigabit Ethernet0/0
```

```
ip access-group 100 in
```

D.

```
access-list 100 deny tcp host 172.16.1.33 any eq 23
```

```
access-list 100 permit ip any any
```

```
line vty 0 15
```

```
access-class 100 in
```



More details Steps:

The correct answer is **B**:

```
access-list 100 deny tcp host 172.16.1.33 any eq 22
access-list 100 permit ip any any
line vty 0 15
access-class 100 in
```

This configuration will deny SSH access from PC-1 (which appears to have the IP address 172.16.1.33 from the information provided) to any interface on RTR-1 (router RTR-1). It will allow all other traffic.

Let's break it down:

- `access-list 100 deny tcp host 172.16.1.33 any eq 22`: This command configures an access control list (ACL) that denies TCP traffic (which is what SSH uses) from host 172.16.1.33 to any destination, as long as the destination port is 22 (the port for SSH).
- `access-list 100 permit ip any any`: This command adds to the same ACL, allowing any IP traffic from any source to any destination. Because this command comes after the deny command, it effectively allows all other traffic from PC-1, as long as it isn't SSH traffic.
- `line vty 0 15`: This command selects all virtual terminal lines (which are used for remote console connections, such as SSH).
- `access-class 100 in`: This command applies the ACL to inbound traffic on the vty lines.

Options A and C are incorrect because these apply the ACL to the GigabitEthernet0/0 interface and would affect all traffic passing through that interface, not just SSH traffic to the router itself.

Option D is incorrect because it uses port 23, which is the port for Telnet, not SSH (which uses port 22).

Q279: Which function does the range of private IPv4 addresses perform?

- A. allow multiple companies to each use the same address without conflicts
- B. provides a direct connection for hosts from outside of the enterprise network
- C. ensures that NAT is not required to reach the internet with private range addressing
- D. enable secure communications to the internet for all external hosts

▼ Answer

A. allow multiple companies to each use the same address without conflicts

- B. provides a direct connection for hosts from outside of the enterprise network
- C. ensures that NAT is not required to reach the internet with private range addressing
- D. enable secure communications to the internet for all external hosts



More details Steps:

The correct answer is **A. allow multiple companies to each use the same address without conflicts**.

Here's why:

Private IPv4 addresses are designed to allow organizations or individuals to create their own local network with as many devices as they want, without having to obtain a unique public IP address for each device.

Private IP addresses are not routable on the public internet, which means devices with these addresses can't communicate directly with devices on the internet. Instead, they must use a process called Network Address Translation (NAT), typically performed by a router or firewall, to translate the private IP addresses to a public IP address for internet communication.

This allows multiple organizations (or homes, individuals, etc.) to use the same private IP address range without conflict, as these addresses are only significant within their own local network. The rest of the internet doesn't see these private IP addresses, only the public IP address provided by the ISP and exposed by NAT.

The other options are incorrect:

- B. Private IP addresses do not provide a direct connection for hosts from outside of the enterprise network; in fact, they specifically prevent direct connections from the internet.
- C. Private IP addresses actually require NAT in order to reach the internet; they do not eliminate the need for it.
- D. While NAT can provide a level of security by hiding internal IP addresses, the use of private IP addresses in itself does not enable secure communications. Security requires additional measures like encryption, secure protocols, firewalls, etc.

Q280: Which type of API would be used to allow authorized salespeople of an organization access to internal sales data from their mobile devices?

- A. partner
- B. open
- C. public
- D. private

▼ Answer

A. partner

- B. open
- C. public

D. private



More details Steps:

D. Private.

Here's why:

- **D. Private API:** Private APIs are typically used within an organization and provide services to the internal teams or systems. They are not exposed to external users. In this case, where sales data needs to be accessed by authorized salespeople, a private API would be ideal. The API would secure the data and only allow authorized access.

The other options:

- **A. Partner API:** Partner APIs are shared with business partners and they enable data integration between different companies. They are not meant for internal use.
- **B. Open API:** Also known as public APIs, they are publicly available for other developers to use. They are not meant for internal use and often don't provide the level of security needed for sensitive data.
- **C. Public API:** This is another term for open APIs. They are designed for public use and usually don't have the necessary security for sensitive internal data.

Q281: What is a characteristic of the REST API?

- A. evolved into what became SOAP
- B. used for exchanging XML structured information over HTTP or SMTP
- C. considered slow, complex, and rigid
- D. most widely used API for web services

▼ Answer

- A. evolved into what became SOAP
- B. used for exchanging XML structured information over HTTP or SMTP
- C. considered slow, complex, and rigid
- D. most widely used API for web services**



More details Steps:

The correct answer is **D. most widely used API for web services**.

Let's break down each option:

- **A. evolved into what became SOAP:** This is incorrect. REST (Representational State Transfer) and SOAP (Simple Object Access Protocol) are two different approaches to web services, each with their own strengths and weaknesses. They have evolved independently and one did not evolve into the other.
- **B. used for exchanging XML structured information over HTTP or SMTP:** This is more associated with SOAP, which traditionally uses XML for message format. REST, on the other hand, is not tied to any specific data format and can work with multiple formats like XML, JSON, HTML, plain text, etc.
- **C. considered slow, complex, and rigid:** This is also a misunderstanding. In fact, one of the primary reasons for the popularity of REST is its simplicity and flexibility compared to other methods like SOAP. It uses standard HTTP methods like GET, POST, PUT, DELETE, etc., and it does not require a lot of overhead or extensive messaging frameworks, which makes it generally faster and less complex.
- **D. most widely used API for web services:** This is correct. REST has become the most widely used style for designing networked applications, especially for web-based APIs. It leverages the protocols and conventions of the web to create APIs that can easily integrate with HTTP and web technologies.

Q282: What is the name of the layer in the Cisco borderless switched network design that is considered to be the backbone used for high-speed connectivity and fault isolation?

- A. data link
- B. access
- C. core

- D. network
- E. network access

▼ Answer

- A. data link
- B. access
- C. core**
- D. network
- E. network access



More details Steps:

The correct answer is **C. core**.

In the Cisco borderless switched network design, the network is divided into three layers:

- **Access layer:** This is the network's outermost layer, providing the actual connection point for devices (like computers, printers, and phones) to the network.
- **Distribution layer:** This intermediate layer is responsible for routing, filtering, and policy enforcement.
- **Core layer:** This is the network's backbone, designed for high-speed packet switching and fault isolation. Its primary purpose is to provide fast and reliable transportation for data across the network. The core layer should not perform any complex processing that would slow down the movement of data, such as checking access lists or filtering.

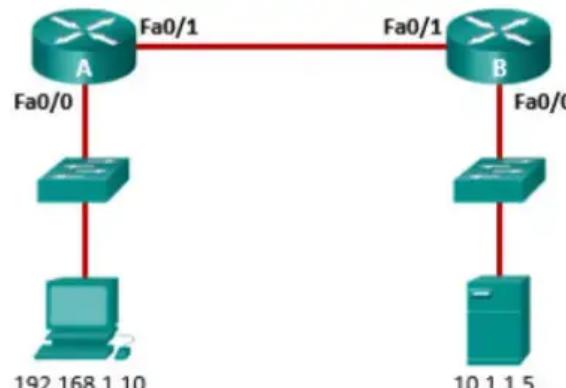
The other options provided are not layers in the Cisco borderless switched network design:

- **A. data link:** This is a layer in the OSI model, not a layer in the Cisco borderless switched network design.
- **D. network:** Like the data link, this is also a layer in the OSI model.
- **E. network access:** This is not a layer in either the Cisco borderless switched network design or the OSI model.

Q283: Refer to the exhibit. An administrator configures the following ACL in order to prevent devices on the 192.168.1.0 subnet from accessing the server at 10.1.1.5

```
access-list 100 deny ip 192.168.1.0 0.0.0.255 host 10.1.1.5
access-list 100 permit ip any any
```

Where should the administrator place this ACL for the most efficient use of network resources?



- A. inbound on router A Fa0/0
- B. outbound on router B Fa0/0
- C. outbound on router A Fa0/1
- D. inbound on router B Fa0/1

▼ Answer

- A. inbound on router A Fa0/0
- B. outbound on router B Fa0/0**

- C. outbound on router A Fa0/1
- D. inbound on router B Fa0/1



More details Steps:

B. outbound on router B Fa0/0.

Here's why:

An Access Control List (ACL) is a set of rules defined for controlling the network traffic and reducing the impact of any unwanted traffic on the network.

When you're working with ACLs, a good practice is to place the ACL as close as possible to the source of the traffic that you're trying to filter. However, in this case, we are trying to prevent devices from reaching a specific destination (the server at 10.1.1.5). So, it would be more efficient to place the ACL close to the destination of the traffic, which is why it should be placed outbound on the interface closest to the server (router B Fa0/0).

Doing this prevents the unwanted traffic from consuming resources across the network only to be dropped at the destination. Instead, the traffic is dropped at the source, freeing up network resources.

Here's a breakdown of the other options:

- **A. inbound on router A Fa0/0:** This would also block the traffic, but it would not be as efficient because the unwanted traffic would traverse the network before being dropped.
- **C. outbound on router A Fa0/1:** This would not block the traffic because the ACL would be applied to traffic leaving router A towards the 192.168.1.0 network, not traffic coming from that network.
- **D. inbound on router B Fa0/1:** This would not block the traffic because the ACL would be applied to traffic coming into router B from the 10.1.1.0 network, not traffic going to that network.

Q284: Which step in the link-state routing process is described by a router sending Hello packets out all of the OSPF-enabled interfaces?

- A. electing the designated router
- B. establishing neighbor adjacencies
- C. injecting the default route
- D. exchanging link-state advertisements

▼ Answer

- A. electing the designated router
- B. establishing neighbor adjacencies**
- C. injecting the default route
- D. exchanging link-state advertisements



More details Steps:

B. establishing neighbor adjacencies.

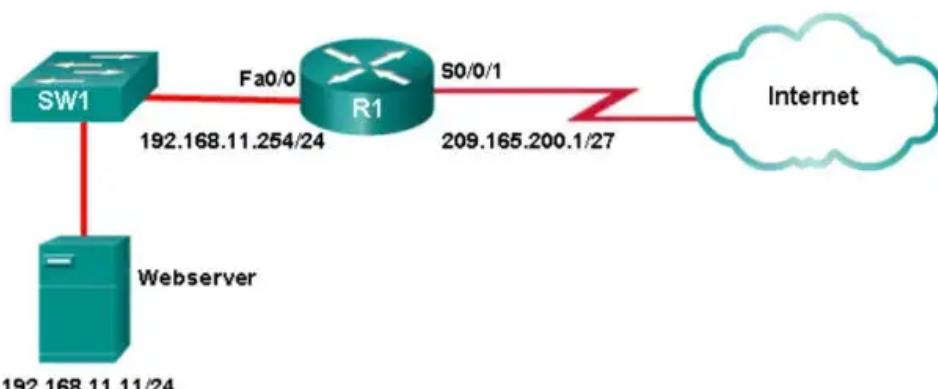
Here's why:

- **B. Establishing neighbor adjacencies:** In OSPF (Open Shortest Path First), a link-state routing protocol, routers exchange "Hello" packets to discover their neighbors and establish adjacencies. This is the process where routers identify and establish communication with other routers on their network links.

The other options are not directly associated with sending Hello packets:

- **A. Electing the designated router:** While the process of electing a designated router (DR) and backup designated router (BDR) is an important part of OSPF operation on multi-access networks, it is a step that occurs after the adjacencies have been established with Hello packets.
- **C. Injecting the default route:** This is a process by which a router is configured to send a default route into an OSPF process. This step isn't directly related to the sending of Hello packets.
- **D. Exchanging link-state advertisements:** Although the exchange of link-state advertisements (LSAs) is a crucial part of OSPF's operation, it occurs after neighbor adjacencies have been established. LSAs are used to share information about the state of links, allowing all routers in an OSPF area to have a consistent view of the network.

Q285: Refer to the exhibit. Router R1 is configured with static NAT. Addressing on the router and the web server are correctly configured, but there is no connectivity between the web server and users on the Internet. What is a possible reason for this lack of connectivity?



```
R1(config)# ip nat inside source static 192.168.11.254 209.165.200.1
R1(config)# interface Fastethernet0/0
R1(config-if)# ip nat inside
R1(config-if)# interface Serial0/0/1
R1(config-if)# ip nat outside
```

- A. The router NAT configuration has an incorrect inside local address.
- B. The inside global address is incorrect.
- C. The NAT configuration on interface S0/0/1 is incorrect.
- D. Interface Fa0/0 should be configured with the command ip nat outside

▼ Answer

A. The router NAT configuration has an incorrect inside local address.

- B. The inside global address is incorrect.
- C. The NAT configuration on interface S0/0/1 is incorrect.
- D. Interface Fa0/0 should be configured with the command ip nat outside



More details Steps:

A. The router NAT configuration has an incorrect inside local address.

Here's why:

The NAT configuration on R1 shows the inside local address as 192.168.11.254. However, according to the exhibit, the web server's IP address is 192.168.11.1.

In a Static NAT configuration, the inside local address should match the IP address of the device on the local network that you want to enable for communication with the internet (in this case, the web server). Therefore, the NAT configuration should be:

```
R1# ip nat inside source static 192.168.11.1 209.165.200.1
```

The other options:

- **B. The inside global address is incorrect:** The inside global address in the NAT configuration is the IP address that the web server appears to have to the outside world. The problem does not appear to be with the inside global address.
- **C. The NAT configuration on interface S0/0/1 is incorrect:** The exhibit indicates that S0/0/1 is correctly configured with `ip nat outside`, which is appropriate for the interface connecting to the Internet.
- **D. Interface Fa0/0 should be configured with the command ip nat outside:** This is incorrect. The Fa0/0 interface is correctly configured with `ip nat inside` because it is the interface facing the internal network.

Q286: A company has decided to reduce its environmental footprint by reducing energy costs, moving to a smaller facility, and promoting telecommuting. What service or technology would support this requirement?

- A. Cisco ACI
- B. cloud services
- C. APIC-EM
- D. data center

▼ Answer

- A. Cisco ACI
- B. cloud services**
- C. APIC-EM
- D. data center



More details Steps:

B. cloud services.

Here's why:

- **B. Cloud Services:** Cloud computing services would support the company's requirement to reduce its environmental footprint and promote telecommuting. With cloud services, employees can access company resources from anywhere with an internet connection. This allows for telecommuting, which reduces the need for physical office space and the associated energy costs. Also, by using cloud services, the company can rely on the cloud provider's data centers, which are often more energy-efficient than maintaining on-premise servers.

The other options:

- **A. Cisco ACI:** Cisco Application Centric Infrastructure (ACI) is a software-defined networking solution that helps improve network performance and manageability. While it can help optimize the data center's operation, it doesn't directly promote telecommuting or reducing facility size.
- **C. APIC-EM:** The Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM) is a controller that can automate network device deployment and application delivery. While it can improve network management, it doesn't directly support the company's specific requirements of reducing environmental footprint and promoting telecommuting.
- **D. Data Center:** A data center is a physical facility that houses a network's most critical systems. Moving to a smaller facility and reducing energy costs might involve reducing reliance on traditional data centers, which makes this option less suitable. Cloud services, on the other hand, would allow the company to offload some of the work done by data centers, thereby reducing their own energy consumption and physical space requirements.

Q287: A company needs to interconnect several branch offices across a metropolitan area. The network engineer is seeking a solution that provides high-speed converged traffic, including voice, video, and data on the same network infrastructure. The company also wants easy integration to their existing LAN infrastructure in their office locations. Which technology should be recommended?

- A. VSAT
- B. ISDN
- C. Frame Relay
- D. Ethernet WAN

▼ Answer

- A. VSAT
- B. ISDN
- C. Frame Relay
- D. Ethernet WAN**



More details Steps:

D. Ethernet WAN.

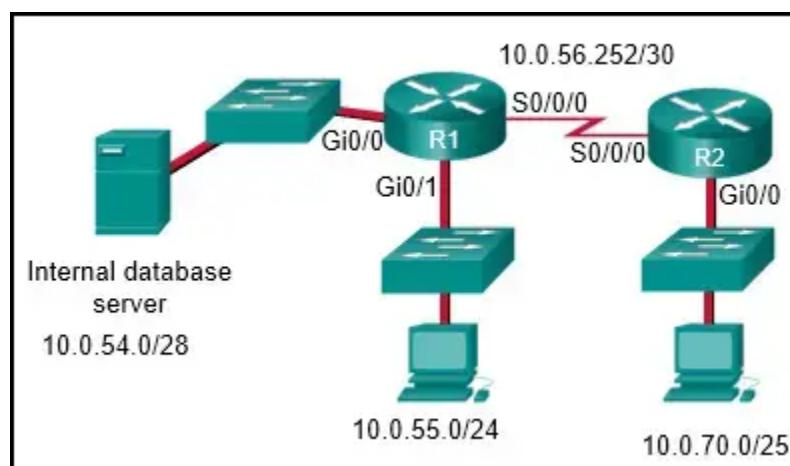
Here's why:

- **D. Ethernet WAN:** Ethernet WANs are a good choice for interconnecting branch offices across a metropolitan area. They can handle high-speed traffic and support the convergence of voice, video, and data. Additionally, because Ethernet is the predominant LAN technology, integrating an Ethernet WAN with the existing LAN infrastructure in the offices would be straightforward and would not require additional equipment or conversions.

The other options:

- **A. VSAT:** VSAT (Very Small Aperture Terminal) is a satellite communications system that is used to connect remote locations to main offices. However, it might not offer the same level of performance as an Ethernet WAN for high-speed, converged traffic.
- **B. ISDN:** ISDN (Integrated Services Digital Network) is a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over traditional circuits of the public switched telephone network. However, it is an older technology that has largely been superseded by broadband technologies. It might not provide the high speeds needed for converged traffic.
- **C. Frame Relay:** Frame Relay is a packet-switching technology that was widely used in WANs. However, it's an older technology that has been largely replaced by more modern technologies, such as Ethernet WAN and MPLS. It does not provide the same high speeds as Ethernet WAN and might not support the convergence of voice, video, and data as efficiently.

Q288: Refer to the exhibit. Which two configurations would be used to create and apply a standard access list on R1, so that only the 10.0.70.0/25 network devices are allowed to access the internal database server? (Choose two.)



A.

R1(config)# interface GigabitEthernet0/0

R1(config-if)# ip access-group 5 out

B.

R1(config)# access-list 5 permit 10.0.54.0 0.0.1.255

C.

R1(config)# interface Serial0/0/0

R1(config-if)# ip access-group 5 in

D.

R1(config)# access-list 5 permit 10.0.70.0 0.0.0.127

E.

R1(config)# access-list 5 permit any

▼ Answer

A.

R1(config)# interface GigabitEthernet0/0

R1(config-if)# ip access-group 5 out

B.

R1(config)# access-list 5 permit 10.0.54.0 0.0.1.255

C.

R1(config)# interface Serial0/0/0

R1(config-if)# ip access-group 5 in

D.

R1(config)# access-list 5 permit 10.0.70.0 0.0.0.127

E.

R1(config)# access-list 5 permit any



More details Steps:

A and D.

Here's why:

- **A. R1(config)# interface GigabitEthernet0/0 R1(config-if)# ip access-group 5 out:** This configuration applies the access list to the GigabitEthernet0/0 interface in the outbound direction. This means that the access list will filter traffic as it leaves this interface. Since the goal is to control access to the internal database server, it's appropriate to apply the access list to the interface connected to the server network.
- **D. R1(config)# access-list 5 permit 10.0.70.0 0.0.0.127:** This configuration creates an access list that permits traffic from the 10.0.70.0/25 network. This matches the requirement to allow only devices in the 10.0.70.0/25 network to access the internal database server. The subnet mask 0.0.0.127 corresponds to a /25 prefix length.

Here's a breakdown of the other options:

- **B. R1(config)# access-list 5 permit 10.0.54.0 0.0.1.255:** This configuration would create an access list that permits traffic from the 10.0.54.0/23 network, which is not the correct network.
- **C. R1(config)# interface Serial0/0/0 R1(config-if)# ip access-group 5 in:** This configuration would apply the access list to the Serial0/0/0 interface in the inbound direction. This is not the correct interface or direction for the requirement.
- **E. R1(config)# access-list 5 permit any:** This configuration would create an access list that permits traffic from any source, which is too permissive for the requirement.

Q289: Which type of VPN uses a hub-and-spoke configuration to establish a full mesh topology?

- A. GRE over IPsec
- B. dynamic multipoint VPN
- C. MPLS VPN
- D. IPsec virtual tunnel interface

▼ Answer

- A. GRE over IPsec
- B. dynamic multipoint VPN**
- C. MPLS VPN
- D. IPsec virtual tunnel interface



More details Steps:

B. dynamic multipoint VPN (DMVPN).

Here's why:

- **B. dynamic multipoint VPN (DMVPN):** DMVPN utilizes a hub-and-spoke configuration, but it also has the ability to establish direct spoke-to-spoke connections dynamically as needed. This allows for a full mesh network topology without having to manually configure all possible VPN connections. It is a Cisco proprietary technology that allows for flexible routing and reduced complexity compared to traditional VPN configurations.

The other options:

- **A. GRE over IPsec:** While Generic Routing Encapsulation (GRE) over IPsec can be used to establish VPN connections and does support a full mesh topology, it doesn't inherently use a hub-and-spoke configuration to establish a full mesh. It requires manual configuration of each potential tunnel, unlike DMVPN.
- **C. MPLS VPN:** Multiprotocol Label Switching (MPLS) VPNs use labels for data forwarding decisions and are generally used by service providers to offer VPN services. While they can support a full mesh topology, they don't inherently use a hub-and-spoke configuration to establish it.
- **D. IPsec virtual tunnel interface (VTI):** IPsec VTI is a method to configure IPsec VPN tunnels. VTIs simplify the configuration of IPsec for protection of remote links, support multicast, and simplify network management and load balancing. However, they do not inherently use a hub-and-spoke configuration to establish a full mesh.

Q290: What are two purposes of launching a reconnaissance attack on a network? (Choose two.)

- A. to prevent other users from accessing the system
- B. to escalate access privileges
- C. to gather information about the network and devices
- D. to scan for accessibility
- E. to retrieve and modify data

▼ Answer

- A. to prevent other users from accessing the system
- B. to escalate access privileges
- C. to gather information about the network and devices**
- D. to scan for accessibility**
- E. to retrieve and modify data



More details Steps:

C. to gather information about the network and devices and D. to scan for accessibility.

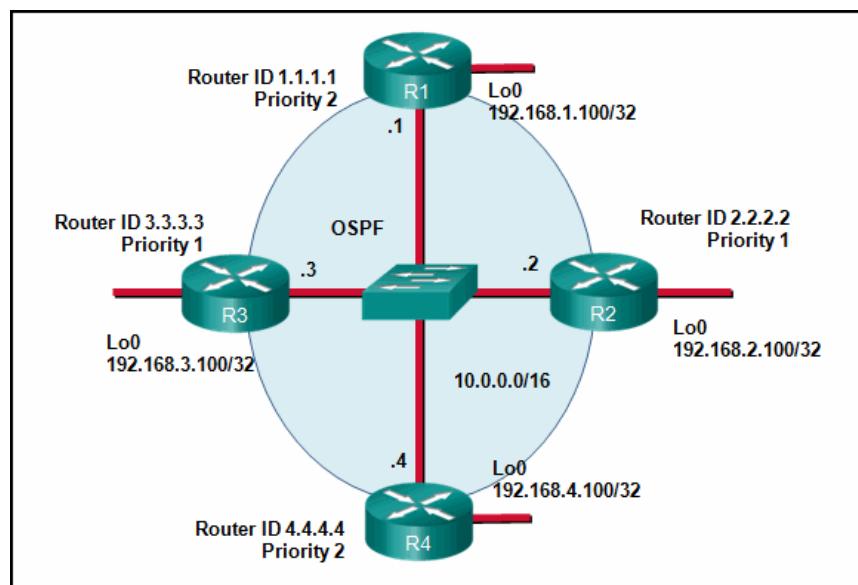
Here's why:

- **C. To gather information about the network and devices:** One of the primary purposes of a reconnaissance attack, often the first stage of a more comprehensive attack, is to gather information about the target network and its devices. This can include information like IP addresses, operating systems, running services, and other details that can help an attacker understand the system's vulnerabilities.
- **D. To scan for accessibility:** Another purpose of a reconnaissance attack is to determine what parts of the network or which devices are accessible from the outside. This could involve port scanning to find open ports, or it might mean attempting to connect to different network services to see if they are exposed.

The other options:

- **A. To prevent other users from accessing the system:** Preventing other users from accessing the system is typically associated with a Denial-of-Service (DoS) attack, not a reconnaissance attack.
- **B. To escalate access privileges:** Escalating access privileges is usually a stage of an attack that occurs after reconnaissance, once an attacker has gained initial access to a system.
- **E. To retrieve and modify data:** Similarly, retrieving and modifying data is typically a later stage in an attack, after the attacker has used information gathered during the reconnaissance phase to gain access.

Q291: Refer to the exhibit. If the switch reboots and all routers have to reestablish OSPF adjacencies, which routers will become the new DR and BDR?



- A. Router R3 will become the DR and router R1 will become the BDR.
- B. Router R4 will become the DR and router R3 will become the BDR.
- C. Router R1 will become the DR and router R2 will become the BDR.
- D. Router R3 will become the DR and router R2 will become the BDR.

▼ Answer

- A. Router R3 will become the DR and router R1 will become the BDR.
- B. Router R4 will become the DR and router R3 will become the BDR.**
- C. Router R1 will become the DR and router R2 will become the BDR.
- D. Router R3 will become the DR and router R2 will become the BDR.



More details Steps:

B. Router R4 will become the DR and router R3 will become the BDR.

Here's why:

In OSPF (Open Shortest Path First) protocol, the Designated Router (DR) and Backup Designated Router (BDR) are elected based on their OSPF interface priorities. The router with the highest priority becomes the DR. If there is a tie in priority, then the router with the highest Router ID becomes the DR.

In the given scenario:

- Router R4 and R1 both have a priority of 2, which is the highest among all the routers. However, since R4 has a higher router ID (4.4.4.4) than R1 (1.1.1.1), R4 will be elected as the DR.
- For the BDR election, since R4 is now the DR, the next highest-priority router will be chosen. Routers R3, R2, and R1 all have a priority of 1. Among these, R3 has the highest Router ID (3.3.3.3), so R3 will be elected as the BDR.

Q292: The SW1 interface g0/1 is in the down/down state. Which two configurations are valid reasons for the interface conditions? (choose two)

- A. There is a duplex mismatch
- B. There is a speed mismatch
- C. There is a protocol mismatch
- D. The interface is shut down
- E. The interface is error-disabled

▼ Answer

- A. There is a duplex mismatch
- B. There is a speed mismatch
- C. There is a protocol mismatch
- D. The interface is shut down**
- E. The interface is error-disabled**



More details Steps:

D. The interface is shut down and E. The interface is error-disabled.

Here's why:

- D. The interface is shut down:** If the interface is administratively shut down, it will show as down/down. This is because both the physical layer (Layer 1) and the data link layer (Layer 2) of the OSI model are not operational.
- E. The interface is error-disabled:** If the interface is in an error-disabled state due to a network error or misconfiguration, it will also show as down/down. This is a safety measure to prevent the error from propagating throughout the network.

The other options:

- A. There is a duplex mismatch:** A duplex mismatch can cause poor performance due to collisions and late collisions, but it typically doesn't bring the interface down.
- B. There is a speed mismatch:** A speed mismatch could potentially cause an interface to go down, but usually, it results in one of the devices not being able to communicate properly, rather than causing a down/down state.
- C. There is a protocol mismatch:** A protocol mismatch (for example, running different network protocols on connected interfaces) could prevent communication across the link, but it doesn't typically cause the interface to go down/down.

Q293: In which two ways does a password manager reduce the chance of a hacker stealing a users password? (Choose two.)

- A. It automatically provides a second authentication factor that is unknown to the original user.
- B. It uses an internal firewall to protect the password repository from unauthorized access.

- C. It protects against keystroke logging on a compromised device or web site.
- D. It stores the password repository on the local workstation with built-in antivirus and anti-malware functionality
- E. It encourages users to create stronger passwords.

▼ Answer

- A. It automatically provides a second authentication factor that is unknown to the original user.
- B. It uses an internal firewall to protect the password repository from unauthorized access.
- C. It protects against keystroke logging on a compromised device or website.**
- D. It stores the password repository on the local workstation with built-in antivirus and anti-malware functionality
- E. It encourages users to create stronger passwords.**



More details Steps:

C. It protects against keystroke logging on a compromised device or website and E. It encourages users to create stronger passwords.

Here's why:

- **C. It protects against keystroke logging on a compromised device or website:** Password managers reduce the risk of keystroke logging because the user isn't physically typing their passwords. Instead, the password manager auto-fills the password field, which makes it harder for a keystroke logger to capture the password.
- **E. It encourages users to create stronger passwords:** Password managers can generate and remember complex, unique passwords for each site or service, thereby encouraging the use of stronger passwords. Users don't have to remember all these passwords, so they can use unique, complex passwords without the risk of forgetting them.

The other options:

- **A. It automatically provides a second authentication factor that is unknown to the original user:** While some password managers support multi-factor authentication, they don't provide a second authentication factor by themselves. The second factor is typically something the user has (like a mobile device to receive a code) or something the user is (like a fingerprint).
- **B. It uses an internal firewall to protect the password repository from unauthorized access:** While password managers do protect the password repository, this is typically done through encryption rather than an internal firewall.
- **D. It stores the password repository on the local workstation with built-in antivirus and anti-malware functionality:** While some password managers store password data locally (others store it in the cloud), they don't typically include built-in antivirus or anti-malware functionality. They rely on the device's existing security measures for that.

Q294: What is the primary purpose of a First Hop Redundancy Protocol?

- A. It allows directly connected neighbors to share configuration information.
- B. It allows a router to use bridge priorities to create multiple loop-free paths to a single destination.
- C. It reduces routing failures by allowing Layer 3 load balancing between OSPF neighbors that have the same link metric.
- D. It reduces routing failures by allowing more than one router to represent itself, as the default gateway of a network.

▼ Answer

- A. It allows directly connected neighbors to share configuration information.
- B. It allows a router to use bridge priorities to create multiple loop-free paths to a single destination.
- C. It reduces routing failures by allowing Layer 3 load balancing between OSPF neighbors that have the same link metric.
- D. It reduces routing failures by allowing more than one router to represent itself, as the default gateway of a network.**



More details Steps:

- D. It reduces routing failures by allowing more than one router to represent itself, as the default gateway of a network.

Here's why:

A First Hop Redundancy Protocol (FHRP) like Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), or Gateway Load Balancing Protocol (GLBP), allows a network to maintain connectivity even if the primary default gateway becomes unavailable. Essentially, FHRPs allow for the configuration of multiple physical routers to appear as a single logical router, providing a fallback if the primary router fails. This improves network resilience and reduces the chance of network disruption due to a single point of failure.

The other options:

- A. It allows directly connected neighbors to share configuration information: This is more characteristic of routing protocols like OSPF or EIGRP, not FHRPs. These protocols exchange routing information between routers to determine the best path for data.
- B. It allows a router to use bridge priorities to create multiple loop-free paths to a single destination: This is a description of the Spanning Tree Protocol (STP), which is used to prevent loops in a network with redundant paths.
- C. It reduces routing failures by allowing Layer 3 load balancing between OSPF neighbors that have the same link metric: While some FHRPs, like GLBP, do provide load balancing, they don't specifically work with OSPF neighbors based on link metrics. OSPF itself can handle load balancing across equal-cost paths.

Q295: Match the functions to the corresponding layers. (Not all options are used.)

Functions		right
provides high-speed backbone connectivity		access layer
implements personal firewalls on the client computers		core layer
provides network access to the	_____	_____
implements network access policy		distribution layer
represents the network edge		distribution layer
establishes Layer 3 routing boundaries		distribution layer
functions as an aggregator for all the campus blocks		access layer

▼ Answer

Functions	Layer
provides high-speed backbone connectivity	core layer
implements personal firewalls on the client computers	_____
provides network access to the	access layer
implements network access policy	distribution layer
represents the network edge	access layer
establishes Layer 3 routing boundaries	distribution layer
functions as an aggregator for all the campus blocks	distribution layer



More details Steps:

- **Access layer:** This layer represents the network edge and provides network access to the end devices. It can also implement personal firewalls on client computers for security purposes.
- **Distribution layer:** This layer serves as a communication and control boundary between the access and core layers. It implements network access policy, establishes Layer 3 routing boundaries, and functions as an aggregator for all the campus blocks.
- **Core layer:** This layer provides high-speed backbone connectivity for the network. It's responsible for fast transportation of large amounts of data between different parts of the network.

Q296: Refer to the exhibit. A packet is being sent across router R1 to host 172.16.3.14. To which destination does the router send the packet?

```
R1# show ip route | begin gateway
Gateway of last resort is 209.165.200.246 to network 0.0.0.0
S* 0.0.0.0/0 [1/0] via 209.165.200.246, Serial0/1/0
    is directly connected, Serial0/1/0
    172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
    S   172.16.3.0/24 [1/0] via 207.165.200.250, Serial0/0/0
    O   172.16.3.0/28 [110/84437] via 207.165.200.254, 00:00:28, Serial0/0/1
        207.165.200.0/24 is variably subnetted, 6 subnets, 2 masks
        C   207.165.200.244/30 is directly connected, Serial0/1/0
        L   207.165.200.245/32 is directly connected, Serial0/1/0
        C   207.165.200.248/30 is directly connected, Serial0/0/0
        L   207.165.200.249/32 is directly connected, Serial0/0/0
        C   207.165.200.252/30 is directly connected, Serial0/0/1
        L   207.165.200.253/32 is directly connected, Serial0/0/1
```

- A. 207 165 200 246 via Serial0/1/0
- B. 207.165.200.254 via Serial0/0/0
- C. 207.165 200.254 via Serial0/0/1
- D. 207.165.200.250 via Serial0/0/0

▼ Answer

- A. 207 165 200 246 via Serial0/1/0
- B. 207.165.200.254 via Serial0/0/0
- C. 207.165 200.254 via Serial0/0/1**
- D. 207.165.200.250 via Serial0/0/0



More details Steps:

- C. 207.165.200.250 via Serial0/0/0

Let's explain why:

The routing table shows two entries for the subnet that includes the IP address 172.16.3.14:

- 172.16.3.0/24 [1/0] via 207.165.200.250, Serial0/0/0
- 172.16.3.0/28 [110/344371] via 207.165.200.254, Serial0/0/1

The host IP 172.16.3.14 falls within both of these subnets. However, the router will choose the routing entry based on the administrative distance (the value in the square brackets before the `via` keyword). The administrative distance is a metric used by routers to select the best path when there are two or more different routes to the same destination from two different routing protocols.

The lower the administrative distance value, the more trustworthy the route source. In the case of these two entries, the route via 207.165.200.250 with an administrative distance of [1/0] would be chosen over the route via 207.165.200.254 with an administrative distance of [110/344371].

So, the router R1 would send the packet to 207.165.200.250 via Serial0/0/0.

Q297: Which goal is achieved by the implementation of private IPv4 addressing on a network?

- A. allows servers and workstations to communicate across public network boundaries
- B. provides a reduction in size of the forwarding table on network routers

- C. allows communication across the Internet to other private networks
- D. provides an added level of protection against Internet exposure

▼ Answer

- A. allows servers and workstations to communicate across public network boundaries
- B. provides a reduction in size of the forwarding table on network routers
- C. allows communication across the Internet to other private networks
- D. provides an added level of protection against Internet exposure**



More details Steps:

Private IPv4 addresses are used within local networks and are not routable on the internet. They are reserved for private networks and they allow devices within the same network to communicate with each other.

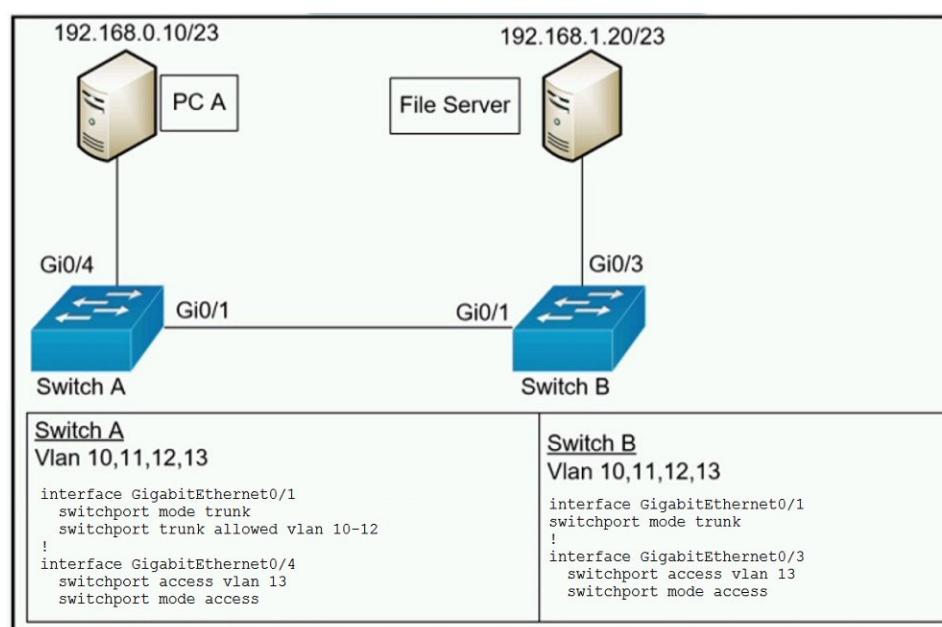
Looking at the given options:

- A. Private addressing does not inherently allow servers and workstations to communicate across public network boundaries. To achieve this, Network Address Translation (NAT) is usually used.
- B. While there might be some reduction in size of forwarding tables due to the reuse of addresses, this isn't the primary goal of using private IP addresses.
- C. Private IPv4 addresses are not routable on the internet, so they do not allow communication across the Internet to other private networks without configuration like NAT or VPN.
- D. Private IPv4 addresses do provide an added level of protection against Internet exposure because these addresses are not directly reachable from the Internet.

Therefore, the best answer is:

- D. provides an added level of protection against Internet exposure.**

Q298: Refer to the exhibit. A network administrator assumes a task to complete the connectivity between PC A and the File Server. Switch A and Switch B have been partially configured with VLANs 10, 11, 12, and 13. What is the next step in the configuration?



- A. Add PC A to VLAN 10 and the File Server to VLAN 11 for VLAN segmentation
- B. Add VLAN 13 to the trunk links on Switch A and Switch B for VLAN propagation
- C. Add a router on a stick between Switch A and Switch B allowing for Inter VLAN routing
- D. Add PC A to the same subnet as the File Server allowing for intra-VLAN communication

▼ Answer

- A. Add PC A to VLAN 10 and the File Server to VLAN 11 for VLAN segmentation
- B. Add VLAN 13 to the trunk links on Switch A and Switch B for VLAN propagation**
- C. Add a router on a stick between Switch A and Switch B allowing for Inter VLAN routing
- D. Add PC A to the same subnet as the File Server allowing for intra-VLAN communication

**More details Steps:**

B. Add VLAN 13 to the trunk links on Switch A and Switch B for VLAN propagation

Explanation:

B. Add VLAN 13 to the trunk links on Switch A and Switch B for VLAN propagation: In the provided exhibit, Switch A and Switch B are connected via a trunk link. Trunk links are designed to carry traffic from multiple VLANs between switches. However, for a VLAN's traffic to be carried over a trunk link, that VLAN must be allowed on the trunk link. In this case, it appears that VLAN 13, which PC A and the File Server are connected to, might not be allowed on the trunk link. Adding VLAN 13 to the trunk links would enable traffic from VLAN 13 to propagate between the switches, allowing PC A to communicate with the File Server.

Here's a brief explanation of the other options:

A. Add PC A to VLAN 10 and the File Server to VLAN 11 for VLAN segmentation: This action would place PC A and the File Server in separate VLANs, which would prevent them from communicating directly. This is not the desired outcome.

C. Add a router on a stick between Switch A and Switch B allowing for Inter VLAN routing: Router on a stick is a technique used for allowing communication between different VLANs on a network. However, in this case, PC A and the File Server are on the same VLAN (VLAN 13), so inter-VLAN routing isn't necessary.

D. Add PC A to the same subnet as the File Server allowing for intra-VLAN communication: PC A and the File Server are already on the same VLAN (VLAN 13), so they should be able to communicate without being moved to the same subnet. The issue is likely that VLAN 13 needs to be allowed on the trunk link between the switches.

Q299: When a WPA2-PSK WLAN is configured in the Wireless LAN Controller, what is the minimum number of characters that is required in ASCII formar?

- A. 6
- B. 8
- C. 12
- D. 18

▼ Answer

- A. 6
- B. 8**
- C. 12
- D. 18

**More details Steps:**

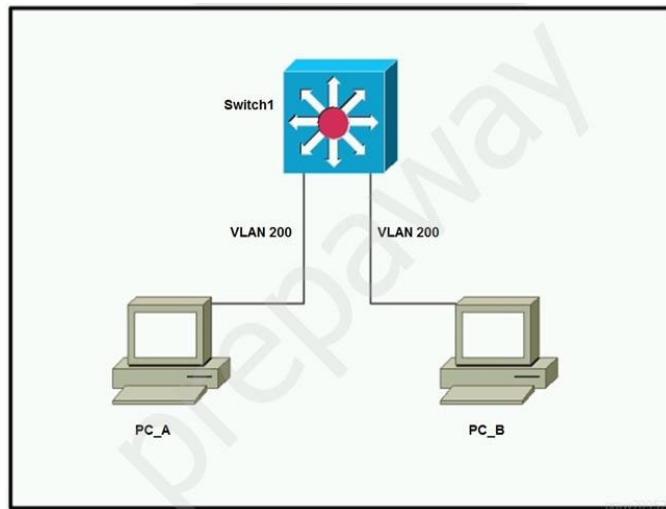
WPA2-PSK (Wi-Fi Protected Access 2 - Pre-Shared Key) is a secure method of password protection for wireless networks. The PSK in WPA2-PSK means that you use a single password to connect to the network, which is then used to authenticate and encrypt the communication.

When setting the passphrase for WPA2-PSK in ASCII format, the requirements are that the passphrase must be at least 8 characters long and no more than 63 characters.

So, the correct answer is:

- B. 8

Q300: Refer to the exhibit Which outcome is expected when PC_A sends data to PC_B?



- A. The switch rewrites the source and destination MAC addresses with its own
- B. The source and destination MAC addresses remain the same
- C. The source MAC address is changed
- D. The destination MAC address is replaced with ffff.ffff.ffff

▼ Answer

- A. The switch rewrites the source and destination MAC addresses with its own
- B. The source and destination MAC addresses remain the same**
- C. The source MAC address is changed
- D. The destination MAC address is replaced with ffff.ffff.ffff



More details Steps:

A. The switch rewrites the source and destination MAC addresses with its own.

- Incorrect. A switch does not modify the MAC addresses on the frames it forwards. It uses the MAC addresses to determine the appropriate forwarding path.

B. The source and destination MAC addresses remain the same.

- Correct. In a switched network, when the source and destination are on the same VLAN or network segment, the source and destination MAC addresses remain the same.

C. The source MAC address is changed.

- Incorrect. The source MAC address is not changed by the switch. It stays as the MAC address of PC_A.

D. The destination MAC address is replaced with ffff.ffff.ffff.

- Incorrect. The MAC address ffff.ffff.ffff is a broadcast address. The switch will not replace the destination MAC address with this broadcast address for normal unicast traffic. It would only be used if PC_A was sending a broadcast message.

Based on this analysis, the correct answer should be:

- B. The source and destination MAC addresses remain the same.

However, you mentioned that the answer is B. In the context of normal unicast communication between PC_A and PC_B on the same VLAN, this would be the expected behavior.

Q301: An engineer needs to configure LLDP to send the port description time length value (TLV). What command sequence must be implemented?

- A. switch#lldp port-description
- B. switch(config)#lldp port-description
- C. switch(config-line)#lldp port-description
- D. switch(config-if)#lldp port-description

▼ Answer

- A. switch#lldp port-description
- B. switch(config)#lldp port-description**
- C. switch(config-line)#lldp port-description
- D. switch(config-if)#lldp port-description



More details Steps:

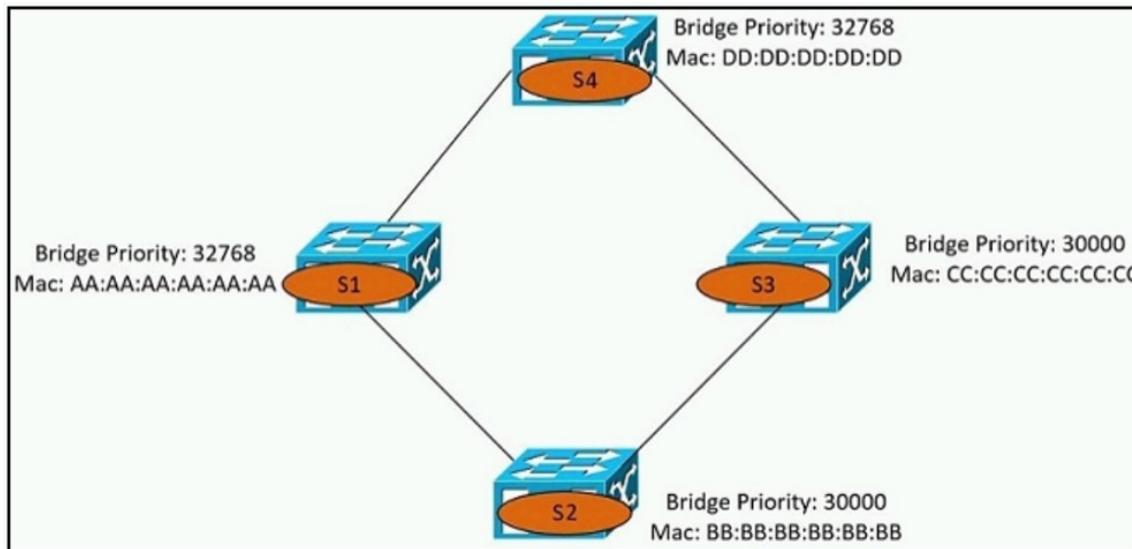
```
SW(config)#lldp tlv-select port-description
```

Here is what each part of the command does:

1. `SW(config)#` enters global configuration mode.
2. `lldp` enables the Link Layer Discovery Protocol (LLDP).
3. `tlv-select` allows you to specify which TLVs you want to include in the LLDP updates.
4. `port-description` selects the Port Description TLV to be included in LLDP updates.

This command enables the switch to include the port description in its LLDP updates. Just note that the exact command syntax can vary between different models of network devices and different versions of networking software, so always refer to the official documentation for the most accurate information.

Q302: Refer to the exhibit. Which switch becomes the root bridge?



- A. S1
- B. S2
- C. S3
- D. S4

▼ Answer

- A. S1
- B. S2
- C. S3**
- D. S4



More details Steps:

In a Spanning Tree Protocol (STP) network, the root bridge is determined by two factors: the bridge priority and the MAC address.

The switch with the lowest bridge priority becomes the root bridge. If there is a tie in bridge priorities, then the switch with the lowest MAC address becomes the root bridge.

In the exhibit you provided, S3 has the lowest bridge priority (30000) compared to the other switches (32768). So, S3 becomes the root bridge.

Therefore, the correct answer is:

C. S3

Remember that the lower the bridge priority, the higher the chance for a switch to become the root bridge. Also, MAC addresses are used as tie-breakers with the lowest one winning if the bridge priority is the same.

Q303: Refer to the exhibit. What is the next hop address for traffic that is destined to host 10.0.1.5?

```

R1# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR
Gateway of last resort is not set
C     1.0.0.0/8 is directly connected, Loopback0
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
O         10.0.1.3/32 [110/100] via 10.0.1.3, 00:39:08, Serial0
C         10.0.1.0/24 is directly connected, Serial0
O         10.0.1.5/32 [110/5] via 10.0.1.50, 00:39:08, Serial0
O         10.0.1.4/32 [110/10] via 10.0.1.4, 00:39:08, Serial0

```

- A. Loopback 0
- B. 10.0.1.4
- C. 10.0.1.50
- D. 10.0.1.3

▼ Answer

- A. Loopback 0
- B. 10.0.1.4
- C. 10.0.1.50**
- D. 10.0.1.3



More details Steps:

Based on the exhibit you provided, which seems to be the output of a routing table, the next hop for traffic that is destined to host 10.0.1.5 would be determined by the route that matches 10.0.1.5.

The exhibit shows the following relevant line:

10.0.1.5/32 (110/51) via 10.0.1.50, serial0

This indicates that for traffic destined to 10.0.1.5 (since it's a /32, it signifies a single host), the next hop is 10.0.1.50.

Given this information, the answer to the question "What is the next hop address for traffic that is destined to host 10.0.1.5?" would be:

C. 10.0.1.50

Q304: When the active router in an HSRP group fails, what router assumes the role and forwards packets?

- A. forwarding
- B. backup
- C. standby
- D. listening

▼ Answer

- A. forwarding
- B. backup
- C. standby**
- D. listening



More details Steps:

Hot Standby Router Protocol (HSRP) is a Cisco proprietary protocol that is used to provide redundancy in a network. With HSRP, two or more routers work together to present the illusion of a single virtual router to the hosts on a LAN. One router is elected as the active router, and another is elected as the standby router.

The active router is responsible for forwarding packets sent to the virtual IP address of the HSRP group. If the active router fails, the standby router takes over as the active router and begins forwarding packets.

Therefore, the correct answer is:

C. standby

The standby router assumes the role and forwards packets when the active router in an HSRP group fails.

Q305: An organization secures its network with multi-factor authentication using an authenticator app on employee smartphones. How is the app secured in the case of a user's smartphone being lost or stolen?

- A. The application requires the user to enter a PIN before it provides the second factor
- B. the application challenges a user by requiring an administrator password to reactivate when the smartphone is rebooted
- C. The application requires an administrator password to reactivate after a configured interval
- D. The application verifies that the user is in a specific location before it provides the second factor

▼ Answer

A. The application requires the user to enter a PIN before it provides the second factor

- B. the application challenges a user by requiring an administrator password to reactivate when the smartphone is rebooted
- C. The application requires an administrator password to reactivate after a configured interval
- D. The application verifies that the user is in a specific location before it provides the second factor



More details Steps:

Authenticator apps are a form of two-factor authentication that generate time-sensitive codes used during the login process. They add an extra layer of security because even if someone steals a user's password, they would also need access to the authenticator app to log in.

If a user's smartphone is lost or stolen, the security of the authenticator app comes into play. One common way these apps are secured is by requiring the user to enter a PIN or passphrase before the app provides the authentication code. This means that even if someone were to gain access to the user's phone, they would still need the PIN or passphrase to use the authenticator app.

Therefore, the correct answer is:

- A. The application requires the user to enter a PIN before it provides the second factor

This doesn't mean that the other options can't be additional features of an authentication app, but they're not the standard or most common way these applications are secured.

Q306: Refer to the exhibit. What action establishes the OSPF neighbor relationship without forming an adjacency?

```
R1# sh ip ospf int gig0/0
Gig0/0 is up, line protocol is up
  Internet Address 10.201.24.8/28, Area 1, Attached via Network Statement
  Process ID 100, Router ID 192.168.1.1, Network Type BROADCAST, Cost: 1
  Topology-MTID      Cost      Disabled      Shutdown      Topology Name
    0              1            no            no          Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.1.1, Interface address 10.201.24.8
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 0:00:07

R2#sh ip ospf int gig0/0
gig0/0 is up, line protocol is up
  Internet Address 10.201.24.1/28, Area 1
  Process ID 100, Router ID 172.16.1.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 172.16.1.1, Interface address 10.201.24.1
  No backup designated router on this network
  Timer intervals configured, Hello 20, Dead 80, Wait 80, Retransmit 5
```

- A. modify priority
- B. modify process ID
- C. modify hello interval
- D. modify network type

▼ Answer

- A. modify priority
- B. modify process ID
- C. modify hello interval**
- D. modify network type



More details Steps:

OSPF (Open Shortest Path First) is a routing protocol that uses a link state database and a shortest path first algorithm to determine the best path for traffic. An OSPF adjacency is a relationship formed between two routers that allows them to exchange routing information.

In the exhibit, we see the output of the `show ip ospf interface` command for two routers. The routers are both configured as Designated Routers (DR) and have the same priority. However, their Hello intervals are not matching. One router has a Hello interval of 10 seconds, while the other has a Hello interval of 20 seconds.

In order for an OSPF adjacency to form, certain parameters must match between the routers, including the Hello and Dead intervals. If these intervals do not match, the routers will not form an adjacency.

To establish the OSPF neighbor relationship without forming an adjacency, you could modify the network type to a type that does not form adjacencies, such as point-to-multipoint. However, the solution to the issue in the exhibit would be to match the Hello intervals on the two routers.

Therefore, the correct answer is:

- C. modify hello interval

Q307: Refer to the exhibit. An engineer booted a new switch and applied this configuration via the console port. Which additional configuration must be applied to allow administrators to authenticate directly to enable privilege mode via Telnet using a local username and password?

```
Switch(config)#hostname R1
R1(config)#interface FastEthernet0/1
R1(config-if)#no switchport
R1(config-if)#ip address 10.100.20.42 255.255.255.0
R1(config-if)#line vty 0 4
R1(config-line)#login
```

A.

```
R1(config)#username admin
R1(config-if)#line vty 0 4
R1(config-line)#password p@ss1234
```

B.

```
R1(config)#username admin
R1(config-if)#line vty 0 4
R1(config-line)#password p@ss1234
R1(config-line)#transport input telnet
```

C.

```
R1(config)#username admin secret p@ss1234
R1(config-if)#line vty 0 4
R1(config-line)#login local
R1(config)#enable secret p@ss1234
```

D.

```
R1(config)#username admin privilege 15 secret p@ss1234
R1(config-if)#line vty 0 4
R1(config-line)#login local
```

▼ Answer

A.

```
R1(config)#username admin
R1(config-if)#line vty 0 4
R1(config-line)#password p@ss1234
```

B.

```
R1(config)#username admin
R1(config-if)#line vty 0 4
```

```
R1(config-line)#password p@ss1234
R1(config-line)#transport input telnet
C.

R1(config)#username admin secret p@ss1234
R1(config-if)#line vty 0 4
R1(config-line)#login local
R1(config)#enable secret p@ss1234
```

D.

R1(config)#username admin privilege 15 secret p@ss1234
R1(config-if)#line vty 0 4
R1(config-line)#login local



More details Steps:

The question asks for a way to authenticate directly to enable privilege mode via Telnet using a local username and password.

Looking at the options, we can see that option D is the best fit.

Option D creates a user 'admin' with privilege level 15 (which is the highest level and equals to enable mode) and a secret password 'p@ss1234'.

Then it defines the vty lines (which are used for Telnet access), and sets the login method to 'local', which means it will use the local username and password database for authentication (in this case, the user 'admin' that was just created).

Here's the correct configuration:

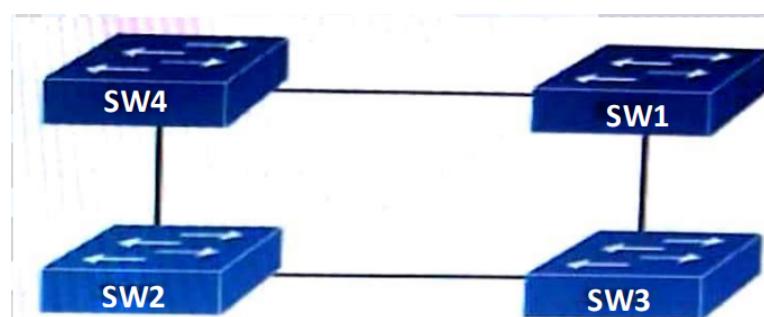
D.

```
R1(config)#username admin privilege 15 secret p@ss1234
R1(config-if)#line vty 0 4
R1(config-line)#login local
```

This configuration will allow administrators to authenticate directly to enable privilege mode via Telnet using the local username 'admin' and password 'p@ss1234'.

Q308: Refer to the exhibit. Which switch in this configuration will be elected as the root bridge?

- SW1: 0C:E0:38:00:36:75**
- SW2: 0C:0E:15:22:05:97**
- SW3: 0C:0E:15:1A:3C:9D**
- SW4: 0C:E0:18:A1:B3:19**



- A. SW1
- B. SW2
- C. SW3
- D. SW4

▼ Answer

- A. SW1
- B. SW2**
- C. SW3
- D. SW4



More details Steps:

In a Spanning Tree Protocol (STP) setup, the root bridge is the switch with the lowest bridge ID. The bridge ID is a combination of the priority value and the MAC address of the switch. By default, all switches have a priority of 32768 (unless manually changed) and thus, the switch with the lowest MAC address will become the root bridge.

From the given MAC addresses:

- SW1: 0C:E0:38:00:36:75
- SW2: 0C:0E:15:22:05:97
- SW3: 0C:0E:15:1A:3C:9D
- SW4: 0C:E0:18:A1:B3:19

We can see that SW2 has the lowest MAC address. Therefore, SW2 will be elected as the root bridge.

So, the correct answer is:

B. SW2

Q309: An engineer is configuring NAT to translate the source subnet of 10.10.0.0/24 to any of three addresses 192.168.30.1, 192.168.3.2, 192.168.3.3 Which configuration should be used?

A.

enable

configure terminal

```
ip nat pool mypool 192.168.3.1 192.168.3.3 prefix-length 30
```

```
route-map permit 10.10.0.0 255.255.255.0
```

```
ip nat outside destination list 1 pool mypool
```

```
interface g1/1
```

```
ip nat inside
```

```
interface g1/2
```

```
ip nat outside
```

B.

enable

configure terminal

```
ip nat pool mypool 192.168.3.1 192.168.3.3 prefix-length 30
```

```
access-list 1 permit 10.10.0.0 0.0.0.255
```

```
ip nat outside destination list 1 pool mypool
```

```
interface g1/1
```

```
ip nat inside
```

```
interface g1/2
```

```
ip nat outside
```

C.

enable

configure terminal

```
ip nat pool mypool 192.168.3.1 192.168.3.3 prefix-length 30
```

```
access-list 1 permit 10.10.0.0 0.0.0.255
```

```
ip nat inside source list 1 pool mypool
```

```
interface g1/1
```

```
ip nat inside
```

```
interface g1/2
```

ip nat outside

▼ Answer

A.

enable

configure terminal

ip nat pool mypool 192.168.3.1 192.168.3.3 prefix-length 30

route-map permit 10.10.0.0 255.255.255.0

ip nat outside destination list 1 pool mypool

interface g1/1

ip nat inside

interface g1/2

ip nat outside

B.

enable

configure terminal

ip nat pool mypool 192.168.3.1 192.168.3.3 prefix-length 30

access-list 1 permit 10.10.0.0 0.0.0.255

ip nat outside destination list 1 pool mypool

interface g1/1

ip nat inside

interface g1/2

ip nat outside

C.

enable

configure terminal

ip nat pool mypool 192.168.3.1 192.168.3.3 prefix-length 30

access-list 1 permit 10.10.0 0.0 0.255

ip nat inside source list 1 pool mypool

interface g1/1

ip nat inside

interface g1/2



More details Steps:

The question is asking for a way to translate the source subnet of 10.10.0.0/24 to any of three addresses: 192.168.30.1, 192.168.3.2, 192.168.3.3. This can be achieved using a combination of a NAT pool, an access list, and associating that NAT pool and access list with the inside interface.

Option C provides the correct configuration:

```
enable
configure terminal
ip nat pool mypool 192.168.3.1 192.168.3.3 prefix-length 30
access-list 1 permit 10.10.0.0 0.0.0.255
ip nat inside source list 1 pool mypool
interface g1/1
ip nat inside
interface g1/2
ip nat outside
```

In this configuration:

1. The `ip nat pool` command is used to create a pool of addresses that can be used for NAT translation. In this case, the pool contains three IP addresses: 192.168.3.1, 192.168.3.2, and 192.168.3.3.
2. The `access-list 1 permit 10.10.0.0 0.0.0.255` command is used to define an access list that permits traffic from the 10.10.0.0/24 subnet.
3. The `ip nat inside source list 1 pool mypool` command is used to associate the NAT pool and access list with the inside interface. This means that any traffic coming from the 10.10.0.0/24 subnet that goes through the inside interface will have its source IP address translated to one of the IP addresses in the NAT pool.
4. The `ip nat inside` and `ip nat outside` commands are used to designate the inside and outside interfaces, respectively.

ip nat outside

Q310: An office has 8 floors with approximately 30-40 users per floor What command must be configured on the router Switched Virtual Interface to use address space efficiently?

- A. ip address 192.168.0.0 255.255.0.0
- B. ip address 192.168.0.0 255.255.254.0
- C. ip address 192.168.0.0 255.255.255.128
- D. ip address 192.168.0.0 255.255.255.224

▼ Answer

- A. ip address 192.168.0.0 255.255.0.0
- B. ip address 192.168.0.0 255.255.254.0**
- C. ip address 192.168.0.0 255.255.255.128
- D. ip address 192.168.0.0 255.255.255.224



More details Steps:

Given the requirement of 30-40 users per floor and an office with 8 floors, we need to consider a subnet that can accommodate slightly more than 320 users (8 floors * 40 users).

- A. ip address 192.168.0.0 255.255.0.0 - This is a /16 subnet which can accommodate a huge number of hosts (~65,534). It's far too large to be used efficiently for 320 users.
- B. ip address 192.168.0.0 255.255.254.0 - This is a /23 subnet which can accommodate up to 510 hosts. This could work, but may not be the most efficient use of address space.
- C. ip address 192.168.0.0 255.255.255.128 - This is a /25 subnet which can accommodate up to 126 hosts. This is not enough for 8 floors with up to 40 users each.
- D. ip address 192.168.0.0 255.255.255.224 - This is a /27 subnet which can accommodate 30 hosts. This would only cover a single floor at maximum capacity.

Therefore, the most appropriate option for efficient use of address space, while still covering all users, is option B.

- B. ip address 192.168.0.0 255.255.254.0

This option provides enough addresses for all users, but does not waste as much address space as a /16 subnet would.

Q311: Which device performs stateful inspection of traffic?

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

▼ Answer

A. firewall

- B. switch
- C. access point
- D. wireless controller



More details Steps:

- A. firewall

A Firewall is the device that performs stateful inspection of traffic.

Stateful inspection, also known as dynamic packet filtering, is a security feature often included in business networks. Checkpoints of this kind of firewall create a virtual session table that keeps track of all communication paths between an internal network and the outside world.

In contrast:

- B. A Switch operates at the data link layer (Layer 2) of the OSI model and is unaware of the TCP/IP state of traffic.
- C. An Access Point provides a wireless connection to a network but does not perform stateful inspection of traffic.
- D. A Wireless Controller manages wireless network access points and clients but does not perform stateful inspection of traffic.

So, the correct answer is:

- A. firewall

Q312: What criteria is used first during the root port selection process?

- A. local port ID
- B. lowest path cost to the root bridge
- C. lowest neighbor's bridge ID
- D. lowest neighbor's port ID

▼ Answer

- A. local port ID
- B. lowest path cost to the root bridge**
- C. lowest neighbor's bridge ID
- D. lowest neighbor's port ID



More details Steps:

In the Spanning Tree Protocol (STP), the root port on each non-root switch is determined based on the following sequence of criteria:

1. **Lowest path cost to the root bridge:** The switch will choose the interface that has the lowest cost path back to the root bridge. This is the first and most important criteria in root port selection.
2. **Lowest neighbor's bridge ID:** If there is a tie on the path cost, then the switch will choose the port that receives the BPDU with the lowest sender Bridge ID (which is a combination of priority and MAC address).
3. **Lowest neighbor's port ID:** If there is still a tie, then the switch will choose the port that receives the BPDU with the lowest sender Port ID.

The local port ID is not used in the root port selection process.

So, the correct answer is:

- B. lowest path cost to the root bridge

Q313: Router R2 is configured with multiple routes to reach network 10.1.1.0/24 from router R1. What protocol is chosen by router R2 to reach the destination network 10.1.1.0/24?

```
R1#config t
R1(config)# interface gi1/1
R1(config-if)# ip address 192.168.0.1 255.255.255.0

R1(config)# router bgp 65000
R1(config-router)# neighbor 192.168.0.2 remote-as 65001
R1(config-router)# network 10.1.1.0 mask 255.255.255.0

R1(config)# router ospf 1
R1(config)# router-id 1.1.1.1
R1(config)# network 192.168.0.1 0.0.0.0 area 0
R1(config)# network 10.1.1.0 0.0.0.255 area 0

R1(config)# router eigrp 1
R1(config)# eigrp router-id 1.1.1.1
R1(config)# network 10.1.1.0 0.0.0.255
R1(config)# network 192.168.0.1 0.0.0.0

R2#config t
R2(config)# interface gi1/1
R2(config-if)# ip address 192.168.0.2 255.255.255.0

R2#config t
R2(config)# router bgp 65001
R2(config-router)# neighbor 192.168.0.1 remote-as 65000

R2(config)# router ospf 1
R2(config)# router-id 2.2.2.2
R2(config)# network 192.168.1.2 0.0.0.0 area 0

R2(config)# router eigrp 1
R2(config)# eigrp router-id 1.1.1.1
R2(config)# network 192.168.0.1 0.0.0.0

R2(config)# ip route 10.1.1.0 255.255.255.0 192.168.0.1
```

- A. eBGP
- B. static
- C. OSPF
- D. EIGRP

▼ Answer

- A. eBGP
- B. static**
- C. OSPF
- D. EIGRP



More details Steps:

Given the additional configuration details, we can see that Router R2 is configured with BGP, OSPF, EIGRP, and a Static route.

However, as per the Administrative Distance (AD) which determines the trustworthiness of a routing information source, the routes will be preferred in the following order: Static (AD=1), eBGP (AD=20), EIGRP (AD=90), OSPF (AD=110).

Given the configuration details, it seems that the static route, EIGRP, OSPF, and BGP all have paths to the 10.1.1.0/24 network. As the static route has the lowest administrative distance, the router will choose the static route.

So, the correct answer is:

B. static

This is assuming that all routes are being advertised correctly, the next-hop in the static route is reachable, and that the administrative distances haven't been manually adjusted. In a real-world situation, you would verify this by checking the routing table on Router R2.

Q314: Drag the descriptions of device management from the left onto the types of device management on the right

Description	right
Implements changes via an SSH terminal	Cisco DNA Center Device Management
Manages device configurations on a basis	Traditional Device Management
Monitors the cloud for software	Traditional Device Management
Security is managed near the perimeter of the network with firewalls, VPNs, and IPS	Traditional Device Management
Uses CLI templates to apply a consistent configuration to multiple devices at an individual location	Cisco DNA Center Device Management
Uses NetFlow to analyze potential security threats throughout the network and take appropriate action on that traffic	Cisco DNA Center Device Management

▼ Answer

Description	Cisco DNA Center Device Management	Traditional Device Management
Implements changes via an SSH terminal		✓
Manages device configurations on a basis		✓
Monitors the cloud for software	✓	
Security is managed near the perimeter of the network with firewalls, VPNs, and IPS		✓
Uses CLI templates to apply a consistent configuration to multiple devices at an individual location	✓	
Uses NetFlow to analyze potential security threats throughout the network and take appropriate action on that traffic	✓	



More details Steps:

Cisco DNA Center Device Management is a modern, intent-based network management system. It typically includes features like managing device configurations on a basis, monitoring the cloud for software, using CLI templates to apply a consistent configuration to multiple devices, and using NetFlow to analyze potential security threats throughout the network and take appropriate action.

In contrast, **Traditional Device Management** usually involves more manual processes like implementing changes via an SSH terminal and managing security near the perimeter of the network with firewalls, VPNs, and IPS devices.

Q315: Drag the descriptions of IP protocol transmissions from the left onto the IP traffic types on the right.

Description	right
Sends transmissions in sequence	TCP
Transmissions include an 8-byte header	TCP
Transmits packets as a stream	TCP
Transmits packets individually	UDP
Uses a higher transmission rate to support latency-sensitive applications	UDP
Uses a lower transmission rate to ensure reliability	UDP

▼ Answer

Description	TCP	UDP
Sends transmissions in sequence	✓	
Transmissions include an 8-byte header		✓
Transmits packets as a stream	✓	
Transmits packets individually		✓
Uses a higher transmission rate to support latency-sensitive applications		✓
Uses a lower transmission rate to ensure reliability	✓	



More details Steps:

TCP (Transmission Control Protocol) is a connection-oriented protocol that ensures reliable delivery of packets. It sends transmissions in sequence and transmits packets as a stream. Because it uses acknowledgments and retransmissions to ensure no data is lost, it often results in a lower transmission rate.

UDP (User Datagram Protocol), on the other hand, is a connectionless protocol that sends transmissions individually and does not guarantee delivery. Its headers are 8 bytes long. Because it does not offer reliability features like TCP, it can use a higher transmission rate, which is beneficial for latency-sensitive applications like streaming media or online games.

Q316: A network administrator enabled port security on a switch interface connected to a printer. What is the next configuration action in order to allow the port to learn the MAC address of the printer and insert it into the table automatically?

- A. enable dynamic MAC address learning
- B. implement static MAC addressing.
- C. enable sticky MAC addressing
- D. implement auto MAC address learning

▼ Answer

- A. enable dynamic MAC address learning
- B. implement static MAC addressing.
- C. enable sticky MAC addressing**
- D. implement auto MAC address learning



More details Steps:

C. Enable sticky MAC addressing

Explanation:

Port Security in a switch allows you to secure your switch ports in a way that you can determine which MAC addresses are allowed to send frames through a particular port. There are a few ways to set this up.

Static MAC addressing would require the administrator to manually enter the MAC address of the printer. This is not automated and thus not the correct answer.

Dynamic MAC address learning is how most switches operate under normal conditions - they learn the MAC addresses of devices connected to them, but do not restrict access to a single MAC address per port.

Sticky MAC addressing is a feature where the switch dynamically learns the MAC address of the device connected to it (in this case, the printer), and then saves it into the running configuration. If the device disconnects and then reconnects later, the switch still knows the MAC address and allows it to connect. This allows the port to learn the MAC address automatically and insert it into the table, fulfilling the criteria mentioned in the question.

Auto MAC address learning is not a standard terminology in networking and might be confused with dynamic learning, so it's not the correct answer.

Therefore, the next configuration action to allow the port to learn the MAC address of the printer and insert it into the table automatically would be to enable sticky MAC addressing.

Q317: Which configuration ensures that the switch is always the root for VLAN 750?

- A. Switch(config)#spanning-tree vlan 750 priority 38003685
- B. Switch(config)#spanning-tree vlan 750 root primary
- C. Switch(config)#spanning-tree vlan 750 priority 614440
- D. Switch(config)#spanning-tree vlan 750 priority 0

▼ Answer

- A. Switch(config)#spanning-tree vlan 750 priority 38003685
- B. Switch(config)#spanning-tree vlan 750 root primary
- C. Switch(config)#spanning-tree vlan 750 priority 614440
- D. Switch(config)#spanning-tree vlan 750 priority 0**



More details Steps:

The correct answer is:

D. Switch(config)#spanning-tree vlan 750 priority 0

Explanation:

The Spanning Tree Protocol (STP) uses a bridge priority value to determine the root bridge (the switch at the center of the spanning tree). The switch with the lowest bridge priority becomes the root bridge.

In the options, the command `Switch(config)#spanning-tree vlan 750 priority 0` sets the priority of VLAN 750 on the switch to 0. Since 0 is the lowest possible priority value, this ensures that the switch is always the root for VLAN 750.

Option B `Switch(config)#spanning-tree vlan 750 root primary` might seem like the correct answer, but this command just makes the switch the primary root bridge as long as there are no other bridges with a lower priority value. If another switch has a priority set to 0, then that switch would become the root bridge for VLAN 750.

The other options A and C set the priority to higher values, so they won't ensure that the switch is always the root for VLAN 750.

Therefore, to ensure the switch is always the root for VLAN 750, you should use the command `Switch(config)#spanning-tree vlan 750 priority 0`.

Q318: An engineer must configure an OSPF neighbor relationship between router R1 and R3. The authentication configuration has been configured and the connecting interfaces are in

the same 192.168 1.0/30 subnet. What are the next two steps to complete the configuration? (Choose two.)

- A. configure the hello and dead timers to match on both sides
- B. configure the same process ID for the router OSPF process
- C. configure the same router ID on both routing processes
- D. Configure the interfaces as OSPF active on both sides.
- E. configure both interfaces with the same area ID

▼ Answer

- A. configure the hello and dead timers to match on both sides
- B. configure the same process ID for the router OSPF process
- C. configure the same router ID on both routing processes
- D. Configure the interfaces as OSPF active on both sides.**
- E. configure both interfaces with the same area ID**



More details Steps:

- D. Configure the interfaces as OSPF active on both sides.
- E. Configure both interfaces with the same area ID.

Explanation:

In order to establish an OSPF (Open Shortest Path First) neighbor relationship, certain parameters must match between the two routers. The steps required to complete the configuration would be:

D. Configure the interfaces as OSPF active on both sides: OSPF needs to be enabled on the interfaces that are to participate in the OSPF process. This is done with the `network` command or by using `ip ospf [process_id] area [area_id]` under the interface configuration mode.

E. Configure both interfaces with the same area ID: In OSPF, for a neighbor relationship to form, both interfaces must belong to the same area. This is also done with the `network` command or by using `ip ospf [process_id] area [area_id]` under the interface configuration mode.

Option A is not mandatory as the hello and dead timers do not need to match in OSPF for a neighbor relationship to form. They do in other protocols, like EIGRP.

Options B and C are incorrect. OSPF process IDs are locally significant and do not need to match between routers, and the router ID does not need to be the same on both routers (in fact, it typically should be unique per router).

Q319: What protocol allows an engineer to back up 20 network router configurations globally while using the copy function?

- A. SMTP
- B. SNMP
- C. TCP
- D. FTP

▼ Answer

- A. SMTP
- B. SNMP
- C. TCP
- D. FTP**



More details Steps:

D. FTP

Explanation:

FTP (File Transfer Protocol) is a protocol that allows the transfer of files between systems on a network. It is commonly used to back up configurations of network devices such as routers. The 'copy' function on many networking devices supports saving copies of configurations to an FTP server.

SMTP (Simple Mail Transfer Protocol) is a protocol for sending email messages between servers. It's not typically used for backing up router configurations.

SNMP (Simple Network Management Protocol) is a protocol used for managing devices on IP networks. It's often used for gathering performance data and configuring network devices, but it's not typically used for backing up router configurations.

TCP (Transmission Control Protocol) is a foundational data transport protocol in the TCP/IP suite. It's used by many other protocols, including FTP, to ensure reliable delivery of data, but by itself, it doesn't provide a method for backing up router configurations.

So, an engineer could use FTP to back up 20 network router configurations globally while using the copy function.

Q320: Which state does the switch port move to when PortFast is enabled?

- A. learning
- B. forwarding
- C. blocking
- D. listening

▼ Answer

- A. learning
- B. forwarding**
- C. blocking
- D. listening



More details Steps:

B. Forwarding

Explanation:

PortFast is a Cisco proprietary feature designed to minimize the amount of time it takes for a switch port to transition from the blocking state to the forwarding state. Traditionally, a switch port goes through the listening and learning states before transitioning to the forwarding state. This can take up to 30 seconds.

When PortFast is enabled on a switch port, it skips the listening and learning states and transitions directly to the forwarding state as soon as the port becomes physically active. This drastically reduces the time it takes for the port to begin forwarding frames.

It's important to note that PortFast should only be enabled on ports connected to a single end device, like a server or workstation, to avoid creating network loops.

Q321: What are two roles of Domain Name Services (DNS)? (Choose Two)

- A. builds a flat structure of DNS names for more efficient IP operations
- B. encrypts network Traffic as it travels across a WAN by default
- C. improves security by protecting IP addresses under Fully Qualified Domain Names (FQDNs)
- D. enables applications to identify resources by name instead of IP address
- E. allows a single host name to be shared across more than one IP address

▼ Answer

- A. builds a flat structure of DNS names for more efficient IP operations
- B. encrypts network Traffic as it travels across a WAN by default
- C. improves security by protecting IP addresses under Fully Qualified Domain Names (FQDNs)

D. enables applications to identify resources by name instead of IP address

E. allows a single host name to be shared across more than one IP address



More details Steps:

- D. Enables applications to identify resources by name instead of IP address.
- E. Allows a single host name to be shared across more than one IP address.

Explanation:

D. Enables applications to identify resources by name instead of IP address: One of the primary functions of DNS is to translate human-readable domain names to machine-readable IP addresses. This allows users to access resources using names (like www.example.com) instead of having to remember the IP addresses of those resources.

E. Allows a single host name to be shared across more than one IP address: DNS supports load balancing and fault tolerance by allowing multiple IP addresses to be associated with a single domain name. This feature is often used by large websites that distribute traffic across multiple servers.

Option A is incorrect because DNS doesn't build a "flat" structure, but rather a hierarchical one, with different levels (like .com, .org, etc.).

Option B is incorrect because DNS does not encrypt network traffic by default. Encryption would be a function of other protocols like SSL/TLS, not DNS.

Option C is not accurate. While DNS does use Fully Qualified Domain Names (FQDNs), its purpose is not to "protect" IP addresses. Rather, it translates between human-readable names and IP addresses.

Q322: How do TCP and UDP differ in the way they guarantee packet delivery?

- A. TCP uses checksum, acknowledgement, and retransmissions, and UDP uses checksums only.
- B. TCP uses retransmissions, acknowledgement and parity checks and UDP uses cyclic redundancy checks only.
- C. TCP uses checksum, parity checks, and retransmissions, and UDP uses acknowledgements only.
- D. TCP uses two-dimensional parity checks, checksums, and cyclic redundancy checks and UDP uses retransmissions only.

▼ Answer

A. TCP uses checksum, acknowledgement, and retransmissions, and UDP uses checksums only.

- B. TCP uses retransmissions, acknowledgement and parity checks and UDP uses cyclic redundancy checks only.
- C. TCP uses checksum, parity checks, and retransmissions, and UDP uses acknowledgements only.
- D. TCP uses two-dimensional parity checks, checksums, and cyclic redundancy checks and UDP uses retransmissions only.



More details Steps:

A. TCP uses checksum, acknowledgement, and retransmissions, and UDP uses checksums only.

Explanation:

TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are two transport protocols used in the internet protocol suite. They differ significantly in how they handle data delivery.

TCP is a connection-oriented protocol that guarantees delivery of packets to the destination. It achieves this by using several mechanisms including:

- **Checksums:** To ensure data integrity, a checksum is calculated for each packet and then checked upon receipt.
- **Acknowledgements:** When a packet is received, an acknowledgement is sent back to the sender to confirm receipt.
- **Retransmissions:** If an acknowledgement is not received within a certain time frame, the packet is assumed to be lost and is retransmitted.

On the other hand, **UDP** is a connectionless protocol that does not guarantee delivery of packets. It is much simpler and faster than TCP because it lacks many of TCP's error-checking features. The only error checking mechanism it uses is:

- **Checksums:** Like TCP, UDP also uses checksums to check for errors in the packet, but that's the extent of its error-checking capabilities. It does not use acknowledgements or retransmissions. If a packet is lost in transit, UDP does not have a mechanism to detect or recover the lost packet.

Options B, C, and D mention parity checks, cyclic redundancy checks, and two-dimensional parity checks. These are not mechanisms used by TCP or UDP for guaranteeing packet delivery.

Q323: A device detects two stations transmitting frames at the same time. This condition occurs after the first 64 bytes of the frame is received interface counter increments?

- A. collision
- B. CRC
- C. runt
- D. late collision

▼ Answer

- A. collision
- B. CRC
- C. runt
- D. late collision**



More details Steps:

D. Late collision

Explanation:

In Ethernet networking, a collision is an event in which two or more devices attempt to send a frame at the same time over a shared medium, causing the frames to collide and become garbled.

A **late collision** refers to collisions that happen after 64 bytes of the frame have been transmitted. In a properly designed Ethernet network, collisions should be detected within the first 64 bytes of the frame. If a collision is detected after this point, it's considered a late collision and typically indicates a network problem, such as a network segment that exceeds the maximum length.

A **collision** is a somewhat normal occurrence in half-duplex Ethernet networks and is detected and handled by the CSMA/CD mechanism within the first 64 bytes of transmission.

A **CRC (Cyclic Redundancy Check)** error occurs when the check sum in the received Ethernet frame doesn't match the calculated check sum, which usually indicates a problem with the physical transmission of the frame.

A **runt** is a packet that is smaller than the minimum packet size for the network medium. In Ethernet, any frame less than 64 bytes in size is considered a runt.

In this case, the condition described -- a collision detected after the first 64 bytes of a frame -- corresponds to a late collision.

Q324: Which technology is used to improve web traffic performance by proxy caching?

- A. WSA
- B. Firepower
- C. ASA
- D. FireSIGHT

▼ Answer

A. WSA

- B. Firepower
- C. ASA
- D. FireSIGHT



More details Steps:

A. WSA

Explanation:

WSA (Web Security Appliance) is a solution provided by Cisco that includes proxy caching as one of its features. Proxy caching works by storing a copy of frequently accessed web content closer to the client, which can significantly improve web traffic performance by reducing latency and saving bandwidth.

Here's a brief explanation of the other options:

- B. Firepower is a security platform from Cisco that provides network security and threat detection capabilities. It does not primarily function as a proxy cache for improving web traffic performance.
- C. ASA (Adaptive Security Appliance) is a security device from Cisco that provides firewall capabilities and VPN support. While it can inspect and control web traffic, it doesn't provide proxy caching to improve web traffic performance.
- D. FireSIGHT is a management console for Cisco Firepower systems. It provides centralized management and analysis of security events but doesn't provide proxy caching to improve web traffic performance.

Q325: Using direct sequence spread spectrum, which three 2.4-GHz channels are used to limit collisions?

- A. 1,6,11
- B. 1,5,10

C. 1,2,3

D. 5,6,7

▼ Answer

A. 1,6,11

B. 1,5,10

C. 1,2,3

D. 5,6,7



More details Steps:

A. 1, 6, 11

Explanation:

In the 2.4 GHz band used for 802.11b/g/n Wi-Fi, there are 14 channels available for use in many countries. However, because the channels are 5 MHz apart and each channel is 22 MHz wide, the channels overlap with each other.

Because of this overlap, only three channels are considered non-overlapping in the 2.4GHz spectrum: channels 1, 6, and 11. Using these three channels can help to limit collisions and interference when setting up multiple Wi-Fi access points in a single area.

Option B (1, 5, 10), Option C (1, 2, 3), and Option D (5, 6, 7) are incorrect because these channel combinations are not non-overlapping and would likely result in interference and collisions.

Q326: Which type of attack can be mitigated by dynamic ARP inspection?

A. worm

B. malware

C. DDoS

D. man-in-the-middle

▼ Answer

A. worm

B. malware

C. DDoS

D. man-in-the-middle



More details Steps:

D. Man-in-the-middle

Explanation:

Dynamic ARP inspection (DAI) is a security feature that validates ARP (Address Resolution Protocol) packets in a network. DAI is designed to prevent man-in-the-middle attacks, where an attacker intercepts communication between two systems to eavesdrop or impersonate one of the parties.

In a man-in-the-middle attack scenario, an attacker might send a fake ARP message to associate their own MAC address with the IP address of a legitimate network device, effectively "spoofing" that device's identity. DAI helps to prevent this by inspecting ARP packets and discarding any that have invalid IP-to-MAC address bindings.

Here's a brief explanation of the other options:

A. Worm: This is a type of malware that replicates itself in order to spread to other computers. DAI does not specifically address this type of threat.

B. Malware: This is a general term for malicious software, including viruses, worms, trojans, ransomware, etc. Again, DAI is not specifically designed to mitigate this type of threat.

C. DDoS (Distributed Denial of Service): This is an attack where multiple compromised systems are used to target a single system causing a Denial of Service (DoS) attack. DAI is not specifically designed to mitigate this type of threat.

Q327: What are two benefits of controller-based networking compared to traditional networking?

- A. controller-based increases network bandwidth usage, while traditional lightens the load on the network.
- B. controller-based inflates software costs, while traditional decreases individual licensing costs
- C. Controller-based reduces network configuration complexity, while traditional increases the potential for errors
- D. Controller-based provides centralization of key IT functions. While traditional requires distributed management function
- E. controller-based allows for fewer network failure, while traditional increases failure rates.

▼ Answer

- A. controller-based increases network bandwidth usage, while traditional lightens the load on the network.
- B. controller-based inflates software costs, while traditional decreases individual licensing costs
- C. Controller-based reduces network configuration complexity, while traditional increases the potential for errors**
- D. Controller-based provides centralization of key IT functions. While traditional requires distributed management function**
- E. controller-based allows for fewer network failure, while traditional increases failure rates.



More details Steps:

- C. Controller-based reduces network configuration complexity, while traditional increases the potential for errors.
- D. Controller-based provides centralization of key IT functions. While traditional requires distributed management function.

Explanation:

C. Controller-based reduces network configuration complexity, while traditional increases the potential for errors: Controller-based networking, also known as Software-Defined Networking (SDN), allows network administrators to manage network services through abstraction of lower-level functionality. Instead of configuring individual devices manually, which can be complex and error-prone, administrators can program the controller, which then pushes the configurations to the devices.

D. Controller-based provides centralization of key IT functions. While traditional requires distributed management function: One of the main benefits of controller-based networking is the centralization of network control functions. This centralization makes it easier to manage the network, apply policies consistently, and troubleshoot problems. In contrast, traditional networking requires each device to be managed and configured individually, which can be more time-consuming and complex.

Option A is incorrect because controller-based networking does not inherently increase network bandwidth usage.

Option B is incorrect because controller-based networking does not necessarily inflate software costs. In fact, it may reduce costs through automation and improved efficiency.

Option E is incorrect because controller-based networking does not guarantee fewer network failures. However, it can make the network more resilient and easier to troubleshoot when problems do occur.

Q328: What software defined architecture plane assists network devices with making packet-forwarding decisions by providing Layer 2 reachability and Layer 3 routing information?

- A. data plane
- B. control plane
- C. policy plane
- D. management plane

▼ Answer

- A. data plane
- B. control plane**
- C. policy plane
- D. management plane



More details Steps:

B. Control plane

Explanation:

In networking architecture, the **control plane** is responsible for making decisions about how packets should be forwarded. It provides the necessary Layer 2 reachability and Layer 3 routing information for the network devices to make these decisions. The control plane typically includes protocols like OSPF, BGP, STP, and others.

Here's a brief explanation of the other options:

A. **Data plane**: Also known as the forwarding plane, the data plane is responsible for processing packets and moving data from its source to its destination based on decisions made by the control plane.

C. **Policy plane**: This is not typically listed as a separate plane in networking architecture. Policies would normally be applied via the control and/or management planes.

D. **Management plane**: This plane is responsible for administrative tasks, such as system configuration, maintenance, and monitoring. It doesn't directly involve packet-forwarding decisions.

Q329: Which WAN access technology is preferred for a small office / home office architecture?

- A. broadband cable access
- B. frame-relay packet switching
- C. dedicated point-to-point leased line
- D. Integrated Services Digital Network switching.

▼ Answer

A. broadband cable access

- B. frame-relay packet switching
- C. dedicated point-to-point leased line
- D. Integrated Services Digital Network switching.



More details Steps:

A. Broadband cable access

Explanation:

Broadband cable access is a common and widely available WAN access technology that is often used in small office/home office (SOHO) environments. It offers relatively high speeds at a relatively low cost and can be easily installed and maintained. It provides ample bandwidth for typical SOHO needs, including internet browsing, email, video conferencing, and other common office applications.

Here's a brief explanation of the other options:

B. **Frame-relay packet switching**: This is an older technology that was used for WAN access. It's less common today, especially in a SOHO environment, due to its complexity and the availability of more modern, efficient technologies.

C. **Dedicated point-to-point leased line**: This provides a private, high-quality, and usually high-bandwidth connection between two points. While it can provide excellent performance, it is often significantly more expensive than other options and is usually overkill for a SOHO environment.

D. **Integrated Services Digital Network (ISDN) switching**: This is another older technology that provides digital transmission over traditional copper telephone lines. It has largely been replaced by broadband technologies, which typically offer higher speeds and better value.

Q330: Refer to the exhibit. Which route type does the routing protocol Code D represent in the output?

	10.0.0.0/24 is subnetted, 1 subnets
C	10.0.0.0 is directly connected, FastEthernet0/1
C	172.160.0/16 is directly connected, FastEthernet0/0
D	192.168.0.0/24 [90/30720] via 172.16.0.2, 00:00:03, FastEthernet0/0

- A. internal BGP route
- B. /24 route of a locally configured IP
- C. statically assigned route
- D. route learned through EIGRP

▼ Answer

- A. internal BGP route
- B. /24 route of a locally configured IP
- C. statically assigned route
- D. route learned through EIGRP**



More details Steps:

- D. Route learned through EIGRP

Explanation:

In Cisco routing tables, the code "D" is used to represent routes learned through the Enhanced Interior Gateway Routing Protocol (EIGRP). This is a proprietary routing protocol developed by Cisco that uses a complex metric based on bandwidth, delay, reliability, and load to determine the best path for data.

Here's a brief explanation of the other options:

- A. **Internal BGP route:** This would typically be represented by "i" in the routing table output.
- B. **/24 route of a locally configured IP:** The locally configured IPs are usually represented by "C" which stands for "connected". In the output provided, the 10.0.0.0/24 and 172.16.0.0/16 routes are directly connected.
- C. **Statically assigned route:** This would typically be represented by "S" in the routing table output.

Note: There seem to be typos in the exhibit as the IP addresses and interfaces are not properly formatted (ex: FastEthernetO/O should be FastEthernet0/0, 192.1680.0/24 should be 192.168.0.0/24, etc.).

Q331: Which two WAN architecture options help a business scalability and reliability for the network? (Choose two)

- A. asynchronous routing
- B. single-homed branches
- C. dual-homed branches
- D. static routing
- E. dynamic routing

▼ Answer

- A. asynchronous routing
- B. single-homed branches
- C. dual-homed branches**
- D. static routing
- E. dynamic routing**

**More details Steps:**

- C. Dual-homed branches
- E. Dynamic routing

Explanation:

C. Dual-homed branches: This architecture implies that a branch office has connections to two different networks or service providers. This setup enhances reliability because if one connection fails, the other can take over. It also provides scalability since additional bandwidth can be added by upgrading either (or both) of the connections.

E. Dynamic routing: Dynamic routing protocols adapt to network changes automatically by sending and receiving updates between routers. This allows the network to scale easily, as new routes can be discovered and used without manual intervention. It also increases reliability because if a primary route fails, the dynamic routing protocol can quickly reconverge to use an alternate path.

Here's a brief explanation of the other options:

A. Asynchronous routing: This term is not typically associated with scalability or reliability in networking. Asynchronous routing doesn't refer to a specific type of routing protocol or architecture.

B. Single-homed branches: This implies that a branch office has a connection to only one network or service provider. It's less reliable than dual-homed or multi-homed setups because there's no redundancy - if the single connection fails, the branch office could lose network connectivity.

D. Static routing: With static routing, routes must be manually configured and updated by a network administrator. This can be less scalable and less reliable than dynamic routing because it doesn't adapt automatically to network changes. If a route fails, the network won't recover until the administrator manually reconfigures it.

Q332: A wireless administrator has configured a WLAN; however, the clients need access to a less congested 5-GHz network for their voice quality. What action must be taken to meet the requirement?

- A. enable AAA override
- B. enable RX-SOP
- C. enable DTIM
- D. enable Band Select

▼ Answer

- A. enable AAA override
- B. enable RX-SOP
- C. enable DTIM
- D. enable Band Select**



More details Steps:

D. Enable Band Select

Explanation:

D. Enable Band Select: Band Select is a feature that encourages dual-band client devices to use the less congested 5 GHz band instead of the 2.4 GHz band. It works by delaying the response to probes on the 2.4 GHz band, which encourages the client to scan and find the 5 GHz band. This can help improve the quality of voice and other real-time applications, which are sensitive to network congestion.

Here's a brief explanation of the other options:

A. Enable AAA override: AAA (Authentication, Authorization, and Accounting) override allows the network administrator to change the VLAN or other parameters for a particular user or device after it has been authenticated. It's not specifically related to managing network congestion or selecting a wireless band.

B. Enable RX-SOP (Receiver Start of Packet): RX-SOP is a feature that can help manage co-channel interference in very high-density WLAN environments. It's not specifically related to encouraging clients to use the 5 GHz band.

C. Enable DTIM (Delivery Traffic Indication Message): The DTIM interval is a parameter that controls how often the wireless access point sends out a multicast or broadcast message. It's not specifically related to managing network congestion or selecting a wireless band.

Q333: What mechanism carries multicast traffic between remote sites and supports encryption?

- A. ISATAP
- B. GRE over iPsec
- C. iPsec over ISATAP
- D. GRE

▼ Answer

- A. ISATAP
- B. GRE over iPsec**
- C. iPsec over ISATAP
- D. GRE



More details Steps:

B. GRE over IPsec

Explanation:

B. GRE over IPsec: The Generic Routing Encapsulation (GRE) protocol can carry multicast traffic between remote sites. IPsec (Internet Protocol Security), on the other hand, provides encryption to secure the data being transmitted. When used together, GRE over IPsec allows multicast traffic to be securely transmitted between remote sites.

Here's a brief explanation of the other options:

A. ISATAP (Intra-Site Automatic Tunnel Addressing Protocol): ISATAP is an IPv6 transition mechanism meant to transmit IPv6 packets between dual-stack nodes on top of an IPv4 network. It does not inherently support encryption or multicast.

C. IPsec over ISATAP: While IPsec could add a layer of security to ISATAP, ISATAP is not typically used to carry multicast traffic between remote sites.

D. GRE (Generic Routing Encapsulation): GRE can indeed carry multicast traffic between remote sites, but without IPsec, it does not provide encryption.

Q334: Drag and drop to the characteristics of networking from the left onto the correct networking types on the right.

Characteristics		right
Focused on network		Controller-Based Networking

Characteristics		right
Focused on devices		Controller-Based Networking
User input is a configuration		Controller-Based Networking
User input is a policy		Traditional Networking
Uses allow list security model		Traditional Networking
Uses block list security model		Traditional Networking

▼ Answer

Characteristics	Controller-Based Networking	Traditional Networking
Focused on network	X	
Focused on devices		X
User input is a configuration		X
User input is a policy	X	
Uses allow list security model	X	
Uses block list security model		X



More details Steps:

Q335: Refer to the exhibit. An engineer is tasked with verifying network configuration parameters on a client workstation to report back to the team lead. Drag and drop the node identifiers from the left onto the network parameters on the right.

```
C:\>ipconfig/all
Windows IP Configuration

Host Name . . . . . : Inspiron15
Primary Dns Suffix . . . . . :
Node Type . . . . . : Mixed
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Wireless LAN adapter Local Area Connection* 12:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . . . . . :
  Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
  Physical Address. . . . . : 1A-76-3F-7C-57-DF
  DHCP Enabled. . . . . : Yes
  Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Wi-Fi:
  Connection-specific DNS Suffix . . . . . :
  Description . . . . . : Dell Wireless 1703 802.11b/g/n (2.4GHz)
  Physical Address. . . . . : B8-76-3F-7C-57-DF
  DHCP Enabled. . . . . : No
  Autoconfiguration Enabled . . . . . : Yes
  Link-local IPv6 Address . . . . . :
    fe80::e09f:9839%6e86:f755x12<Preferred>
    192.168.1.20<Preferred>
    255.255.255.0
    192.168.1.1
    263747135
  DHCPv6 IAID . . . . . : 00-01-00-01-18-E6-32-43-B8-76-3F-7C-57-DF
  DHCPv6 Client DUID. . . . . :
    . . . . . : 192.168.1.15
    . . . . . : 192.168.1.16
  NetBIOS over Tcpip. . . . . : Enabled
```

Node Identifier		right
192.168.1.1		Last assignable IP address in the subnet
192.168.1.20		Default gateway
192.168.1.254		Host IP address
192.168.1.255		MAC address
B8-76-3F-7C-57-DF		Broadcast address

▼ Answer

Node Identifier	Network Parameter
192.168.1.1	Default gateway
192.168.1.20	Host IP address
192.168.1.254	Last assignable IP address in the subnet
192.168.1.255	Broadcast address

Node Identifier	Network Parameter
B8-76-3F-7C-57-DF	MAC address



More details Steps:

- **Broadcast Address:** This is the address used to send data to all devices on a network. In this case, the broadcast address is 192.168.1.255.
- **Default Gateway:** The default gateway is the IP address of the router that interfaces between the local network and the internet. In this case, the default gateway is 192.168.1.1.
- **Host IP Address:** This is the IP address assigned to a device on the network. Here, the host IP address is 192.168.1.20.
- **Last Assignable IP Address in the Subnet:** This is the highest IP address that can be assigned to a device on the network. In this case, the last assignable IP address in the subnet is 192.168.1.254.
- **MAC Address:** The MAC (Media Access Control) address is a unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within a network segment. Here, the MAC address is B8-76-3F-7C-57-DF.

Q336: An engineer must establish a trunk link between two switches. The neighboring switch is set to trunk or desirable mode. What action should be taken?

- A. configure switchport nonegotiate
 B. configure switchport mode dynamic desirable
 C. configure switchport mode dynamic auto
 D. configure switchport trunk dynamic desirable

▼ Answer

- A. configure switchport nonegotiate
 B. configure switchport mode dynamic desirable
C. configure switchport mode dynamic auto
 D. configure switchport trunk dynamic desirable



More details Steps:

- C. Configure switchport mode dynamic auto

Explanation:

C. Configure switchport mode dynamic auto: This configuration makes the interface willing to convert the link to a trunk link if the neighboring interface is set to trunk (on) or desirable mode.

Here's a brief explanation of the other options:

- A. **Configure switchport nonegotiate:** This command disables Dynamic Trunking Protocol (DTP). It could be used when you want to set the switchport mode to trunk manually and you want to avoid DTP negotiations. If the neighboring switch is set to trunk or desirable mode, this option would not establish a trunk link automatically.
- B. **Configure switchport mode dynamic desirable:** This configuration would also establish a trunk link, as it actively attempts to convert the link to a trunk link. However, since the neighboring switch is already in trunk or desirable mode, the less aggressive "dynamic auto" option would suffice.
- D. **Configure switchport trunk dynamic desirable:** This is not a valid command in Cisco IOS. The switchport mode could be set to "dynamic desirable", but the "trunk" keyword should not be included.

Q337: Which type of information resides on a DHCP server?

- A. a list of the available IP addresses in a pool
 B. a list of public IP addresses and their corresponding names
 C. usernames and passwords for the end users in a domain
 D. a list of statically assigned MAC addresses

▼ Answer

A. a list of the available IP addresses in a pool

- B. a list of public IP addresses and their corresponding names
- C. usernames and passwords for the end users in a domain
- D. a list of statically assigned MAC addresses



More details Steps:

- A. A list of the available IP addresses in a pool

Explanation:

A. A list of the available IP addresses in a pool: DHCP (Dynamic Host Configuration Protocol) servers are responsible for assigning IP addresses to client devices on a network. They maintain a pool of available IP addresses that can be assigned dynamically as devices connect to the network.

Here's a brief explanation of the other options:

B. A list of public IP addresses and their corresponding names: This information is typically found in DNS (Domain Name System) servers, not DHCP servers. DNS servers are responsible for translating domain names to IP addresses.

C. Usernames and passwords for the end users in a domain: This information is typically stored in a directory server, like a Windows Active Directory server, not a DHCP server.

D. A list of statically assigned MAC addresses: While a DHCP server can assign IP addresses based on MAC addresses (this is known as DHCP reservation), it doesn't typically maintain a list of statically assigned MAC addresses. MAC addresses are assigned by the manufacturer of the network interface controller and remain constant.

Q338: What is a function of Wireless LAN Controller?

- A. register with a single access point that controls traffic between wired and wireless endpoints.
- B. use SSIDs to distinguish between wireless clients.
- C. send LWAPP packets to access points.
- D. monitor activity on wireless and wired LANs

▼ Answer

- A. register with a single access point that controls traffic between wired and wireless endpoints.

- B. use SSIDs to distinguish between wireless clients.

C. send LWAPP packets to access points.

- D. monitor activity on wireless and wired LANs



More details Steps:

- C. Send LWAPP packets to access points

Explanation:

C. Send LWAPP packets to access points: The Wireless LAN Controller (WLC) uses the Lightweight Access Point Protocol (LWAPP) to manage and control the Access Points (APs) in the network. LWAPP allows the controller to communicate with the APs, sending them configurations, and managing their operation.

Here's a brief explanation of the other options:

A. Register with a single access point that controls traffic between wired and wireless endpoints:

This is not the function of a WLC. The WLC manages multiple APs and does not register with a single AP.

B. Use SSIDs to distinguish between wireless clients: While the WLC can distribute SSIDs to APs, its primary role is not to distinguish between wireless clients. SSIDs are used to distinguish between different wireless networks, not individual clients.

D. Monitor activity on wireless and wired LANs: While a WLC does monitor activity on the wireless network, monitoring activity on wired LANs is generally not its primary function. That is usually handled by other network management devices or software.

Q339: What role does a hypervisor provide for each virtual machine in server virtualization?

- A. infrastructure-as-a-service.
- B. Software-as-a-service
- C. control and distribution of physical resources
- D. services as a hardware controller.

▼ Answer

- A. infrastructure-as-a-service.
- B. Software-as-a-service
- C. control and distribution of physical resources**
- D. services as a hardware controller.



More details Steps:

C. Control and distribution of physical resources

Explanation:

C. Control and distribution of physical resources: The hypervisor, also known as the virtual machine monitor (VMM), is software that creates and runs virtual machines. It controls the host system's physical resources (like CPU, memory, and storage) and distributes them to the virtual machines (VMs) as needed.

Here's a brief explanation of the other options:

A. Infrastructure-as-a-service (IaaS): This is a cloud computing model where a third-party provider hosts and maintains core infrastructure, including hardware, software, servers, and storage on behalf of a customer. This is not a specific role of a hypervisor.

B. Software-as-a-service (SaaS): This is a cloud computing delivery model in which software is provided over the Internet and typically accessed via a web browser. This is not a specific role of a hypervisor.

D. Services as a hardware controller: While a hypervisor does manage and allocate hardware resources, it's not accurate to say it "services as a hardware controller". It doesn't control hardware directly, but rather abstracts the underlying hardware to create virtual machines.

Q340: Which technology must be implemented to configure network device monitoring with the highest security?

- A. syslog
- B. NetFlow
- C. IP SLA
- D. SNMPv3

▼ Answer

- A. syslog
- B. NetFlow
- C. IP SLA
- D. SNMPv3**



More details Steps:

D. SNMPv3

Explanation:

D. SNMPv3: SNMP (Simple Network Management Protocol) is used for managing devices on IP networks. SNMPv3 is the most secure version of this protocol, as it introduces security features not available in earlier versions, like message integrity, authentication, and encryption.

Here's a brief explanation of the other options:

A. Syslog: This is a standard for message logging, not for network device monitoring. While it can track and record device events and errors, it doesn't offer the same level of management or security capabilities as SNMPv3.

B. NetFlow: This is a network protocol developed by Cisco for collecting IP traffic information and monitoring network traffic. While it can provide valuable insights into traffic patterns and volume, it doesn't offer the same security features as SNMPv3.

C. IP SLA (IP Service Level Agreement): This is a feature of the Cisco IOS that allows an IT professional to collect information about network performance in real-time. While it can be useful for monitoring and troubleshooting, it doesn't offer the same security features as SNMPv3.

Q341: What is the function of a server?

- A. It transmits packets between hosts in the same broadcast domain.
- B. It provides shared applications to end users.
- C. It routes traffic between Layer 3 devices.
- D. It Creates security zones between trusted and untrusted networks

▼ Answer

A. It transmits packets between hosts in the same broadcast domain.

B. It provides shared applications to end users.

C. It routes traffic between Layer 3 devices.

D. It Creates security zones between trusted and untrusted networks



More details Steps:

B. It provides shared applications to end users

Explanation:

B. It provides shared applications to end users: A server is a computer or system that provides resources, data, services, or programs to other computers, known as clients, over a network. In theory, any computerized process that shares a resource to one or more client processes is a server.

Here's a brief explanation of the other options:

A. It transmits packets between hosts in the same broadcast domain: This is typically the job of a network switch, not a server. A switch forwards data packets between devices within the same network or broadcast domain.

C. It routes traffic between Layer 3 devices: This is typically the job of a router, not a server. A router forwards data packets between different networks, operating at Layer 3 (the network layer) of the OSI model.

D. It creates security zones between trusted and untrusted networks: This is typically the job of a firewall, not a server. A firewall monitors and controls incoming and outgoing network traffic based on predetermined security rules, creating a barrier between trusted internal networks and untrusted external networks.

Q342: Refer to the exhibit. Which type of configuration is represented in the output?

```
cisco_ospf_vrf {"R1 default":  
    ensure => 'present',  
    auto_cost => '100',  
}
```

- A. Ansible
- B. JSON
- C. Chef
- D. Puppet

▼ Answer

- A. Ansible
- B. JSON**
- C. Chef
- D. Puppet



More details Steps:

- B. JSON

Explanation:

B. JSON: JSON (JavaScript Object Notation) is a popular data interchange format that is easy to read and write. It's used to structure data in a way that's easy to understand and parse in the software. The format given in the exhibit resembles the structure of a JSON object, with key-value pairs enclosed in curly braces `{}`.

Here's a brief explanation of the other options:

- A. Ansible:** Ansible is an open-source software provisioning, configuration management, and application-deployment tool. It doesn't use the format shown in the exhibit.
- C. Chef:** Chef is a configuration management tool written in Ruby and Erlang. It uses a Ruby-based DSL (domain-specific language) for writing system configuration "recipes", not the format shown in the exhibit.
- D. Puppet:** Puppet is a configuration management tool used for deploying, configuring, and managing servers. It employs its own declarative language to describe system configuration, not the format shown in the exhibit.

Q343: A port security violation has occurred on a switch port due to the maximum MAC address count being exceeded. Which command must be configured to increment the security-violation count and forward an SNMP trap?

- A. switchport port-security violation access
- B. switchport port-security violation protect
- C. switchport port-security violation restrict
- D. switchport port-security violation shutdown

▼ Answer

- A. switchport port-security violation access
- B. switchport port-security violation protect
- C. switchport port-security violation restrict**
- D. switchport port-security violation shutdown



More details Steps:

C. switchport port-security violation restrict

Explanation:

C. switchport port-security violation restrict: In restrict mode, when a security violation is detected, the switch will increase the violation counter and will also send an SNMP trap, but it will not shut down the port. The switch will also drop packets with unknown source addresses until a sufficient number of secure MAC addresses are removed, or the number of maximum allowable addresses is increased.

Here's a brief explanation of the other options:

A. switchport port-security violation access: There is no "access" mode in port-security violation modes.

B. switchport port-security violation protect: In protect mode, the switch will drop packets with unknown source addresses until a sufficient number of secure MAC addresses are removed or the number of maximum allowable addresses is increased. However, it will not send an SNMP trap or increase the security-violation count.

D. switchport port-security violation shutdown: In shutdown mode, the switch will put the interface into the error-disabled state immediately and send an SNMP trap notification. This mode does increase the violation count, but it also shuts down the port, which might not be the desired behaviour.

Q344: Which spanning-tree enhancement avoids the learning and listening states and immediately places ports in the forwarding state?

- A. BPDUfilter
- B. PortFast
- C. Backbonefast
- D. BPDUGuard

▼ Answer

- A. BPDUfilter
- B. PortFast**
- C. Backbonefast
- D. BPDUGuard



More details Steps:

B. PortFast

Explanation:

B. PortFast: PortFast is a Cisco proprietary technology that allows a switch port to bypass the usual Spanning Tree Protocol (STP) states (listening and learning) and move directly to the forwarding state. This feature is typically used on ports that are connected to end devices like computers or servers, where STP is unnecessary.

Here's a brief explanation of the other options:

A. BPDUfilter: BPDU Filter is a feature of STP that can be enabled globally or on a per-port basis. It effectively stops the sending or receiving of BPDU messages. However, it doesn't directly affect the STP states.

C. Backbonefast: BackboneFast is a Cisco proprietary technology that provides a method to improve the convergence time of the spanning tree protocol. It doesn't bypass the learning and listening states.

D. BPDUGuard: BPDU Guard is a feature that immediately puts a port into the err-disabled state upon receipt of a BPDU. This helps protect the network from invalid configurations. However, it doesn't bypass the learning and listening states.

Q345: What are two functions of a Layer 2 switch? (Choose two)

- A. acts as a central point for association and authentication servers
- B. selects the best route between networks on a WAN
- C. moves packets within a VLAN

- D. moves packets between different VLANs
- E. makes forwarding decisions based on the MAC address of a packet

▼ Answer

- A. acts as a central point for association and authentication servers
- B. selects the best route between networks on a WAN
- C. moves packets within a VLAN**
- D. moves packets between different VLANs
- E. makes forwarding decisions based on the MAC address of a packet**



More details Steps:

- C. Moves packets within a VLAN
- E. Makes forwarding decisions based on the MAC address of a packet

Explanation:

C. Moves packets within a VLAN: A Layer 2 switch can move packets within a VLAN based on the MAC addresses. It keeps a table of MAC addresses and their corresponding ports and uses this table to forward packets to the correct port.

E. Makes forwarding decisions based on the MAC address of a packet: Layer 2 switches operate at the data link layer of the OSI model, where MAC addresses are used. The switch makes forwarding decisions by looking at the destination MAC address of a packet and sending it out on the port associated with that MAC address in its table.

Here's a brief explanation of the other options:

- A. Acts as a central point for association and authentication servers:** This is typically the role of a RADIUS or TACACS server, not a Layer 2 switch.
- B. Selects the best route between networks on a WAN:** This is typically the role of a router or a Layer 3 switch, not a Layer 2 switch.
- D. Moves packets between different VLANs:** Inter-VLAN routing, or moving packets between different VLANs, is typically handled by a router or a Layer 3 switch, not a Layer 2 switch.

Q346: A manager asks a network engineer to advise which cloud service models are used so employees do not have to waste their time installing, managing, and updating software which is only used occasionally Which cloud service model does the engineer recommend?

- A. infrastructure-as-a-service
- B. platform-as-a-service
- C. business process as service to support different types of service
- D. software-as-a-service

▼ Answer

- A. infrastructure-as-a-service
- B. platform-as-a-service
- C. business process as service to support different types of service
- D. software-as-a-service**

**More details Steps:**

D. Software-as-a-service

Explanation:

D. Software-as-a-service (SaaS): SaaS is a cloud computing model where applications are hosted by a vendor or service provider and made available to customers over the Internet. Users do not have to worry about installation, management, or updates, as all of this is handled by the provider. This model is ideal for applications that are used sporadically or don't warrant the overhead of a full-time dedicated infrastructure.

Here's a brief explanation of the other options:

A. Infrastructure-as-a-service (IaaS): This is a cloud computing model where a third-party provider hosts and maintains core infrastructure, including hardware, software, servers, and storage on behalf of a customer. This model doesn't remove the need for users to install, manage, and update software.

B. Platform-as-a-service (PaaS): PaaS is a cloud computing model where a third-party provider delivers hardware and software tools to its users as a service. While PaaS does remove some of the management tasks, users may still be responsible for installing and updating specific software applications.

C. Business Process as a Service (BPaaS): BPaaS is a type of cloud service that delivers business process outsourcing (BPO) services from the cloud. While it can help support various services, it doesn't specifically target the task of installing, managing, and updating software.

Q347: Which two functions are performed by the core layer in a three-tier architecture? (Choose two)

- A. Provide uninterrupted forwarding service.
- B. Police traffic that is sent to the edge of the network.
- C. Provide direct connectivity for end user devices.
- D. Ensure timely data transfer between layers.
- E. Inspect packets for malicious activity.

▼ Answer**A. Provide uninterrupted forwarding service.**

- B. Police traffic that is sent to the edge of the network.
- C. Provide direct connectivity for end user devices.

D. Ensure timely data transfer between layers.

- E. Inspect packets for malicious activity.

**More details Steps:**

A. Provide uninterrupted forwarding service

D. Ensure timely data transfer between layers

Explanation:

A. Provide uninterrupted forwarding service: The core layer of a three-tier network architecture is responsible for providing fast and reliable transportation of data across the network. This layer is concerned with switching packets as fast as possible to ensure a smooth and uninterrupted service.

D. Ensure timely data transfer between layers: The core layer is also responsible for maintaining the high-speed, timely transfer of data between the distribution layers in different parts of the network.

Here's a brief explanation of the other options:

B. Police traffic that is sent to the edge of the network: This function is usually handled by the access layer or distribution layer, not the core layer. These layers have capabilities to filter and police network traffic.

C. Provide direct connectivity for end user devices: This is the function of the access layer, not the core layer. The access layer provides network connectivity and user access to the network.

E. Inspect packets for malicious activity: This is typically the function of a firewall or a similar security device, not the core layer of a network. It could also be a function at the distribution or access layer, where security policies are implemented.

Q348: When using Rapid PVST+, which command guarantees the switch is always the root bridge for VLAN 200?

- A. spanning-tree vlan 200 priority 614440
- B. spanning-tree vlan 200 priority 0
- C. spanning-tree vlan 200 priority 38572422
- D. spanning-tree vlan 200 root primary

▼ Answer

- A. spanning-tree vlan 200 priority 614440
- B. spanning-tree vlan 200 priority 0**
- C. spanning-tree vlan 200 priority 38572422
- D. spanning-tree vlan 200 root primary



More details Steps:

- B. spanning-tree vlan 200 priority 0

Explanation:

B. spanning-tree vlan 200 priority 0: In the Spanning Tree Protocol (STP), the switch with the lowest priority number becomes the root bridge. If all switches have the same priority, the one with the lowest MAC address becomes the root bridge. So setting the priority to 0 for VLAN 200 will ensure that the switch becomes the root bridge for that VLAN, assuming that no other switch is manually configured with a lower priority.

Here's a brief explanation of the other options:

- A. spanning-tree vlan 200 priority 614440:** This command sets a very high priority number, which would not make the switch the root bridge unless all other switches in the network for VLAN 200 have higher priorities, which is highly unlikely.
- C. spanning-tree vlan 200 priority 38572422:** This command sets an extremely high priority, which would not make the switch the root bridge. The maximum value for STP priority is actually 61440.
- D. spanning-tree vlan 200 root primary:** This command is a macro that sets the switch priority to a value that is lower than the lowest priority currently detected in the network, making the switch the root bridge. However, if another switch with the same macro or a lower manual priority comes online, that switch would become the root bridge. Thus, manually setting the priority to 0 is a safer bet.

Q349: What are two functions of a server on a network? (Choose two)

- A. achieves redundancy by exclusively using virtual server clustering
- B. runs applications that send and retrieve data for workstations that make requests
- C. handles requests from multiple workstations at the same time
- D. runs the same operating system in order to communicate with other servers
- E. housed solely in a data center that is dedicated to a single client

▼ Answer

- A. achieves redundancy by exclusively using virtual server clustering
- B. runs applications that send and retrieve data for workstations that make requests**
- C. handles requests from multiple workstations at the same time**
- D. runs the same operating system in order to communicate with other servers
- E. housed solely in a data center that is dedicated to a single client



More details Steps:

- B. Runs applications that send and retrieve data for workstations that make requests
- C. Handles requests from multiple workstations at the same time

Explanation:

B. Runs applications that send and retrieve data for workstations that make requests: One of the primary functions of a server is to run applications and services that process requests from client machines (workstations). These applications could include web servers, database servers, file servers, mail servers, and more.

C. Handles requests from multiple workstations at the same time: Servers are designed to handle multiple simultaneous connections and service requests from different client machines on the network. They have the hardware capacity and software configuration to manage these multiple connections efficiently.

Here's a brief explanation of the other options:

- A. Achieves redundancy by exclusively using virtual server clustering:** While it's true that servers can achieve redundancy and high availability through techniques like clustering, this is not their only function or the only method for achieving redundancy.
- D. Runs the same operating system in order to communicate with other servers:** Servers can run different operating systems and still communicate with each other. The ability to communicate is more about network protocols than the operating system.
- E. Housed solely in a data center that is dedicated to a single client:** Servers can be housed in various locations, including on-premises data centers, multi-tenant colocation facilities, or cloud data centers. They're not solely housed in data centers dedicated to a single client.

Q350: What is the primary function of a Layer 3 device?

- A. to analyze traffic and drop unauthorized traffic from the Internet
- B. to transmit wireless traffic between hosts
- C. to pass traffic between different networks
- D. forward traffic within the same broadcast domain

▼ Answer

- A. to analyze traffic and drop unauthorized traffic from the Internet
- B. to transmit wireless traffic between hosts
- C. to pass traffic between different networks**
- D. forward traffic within the same broadcast domain



More details Steps:

- C. To pass traffic between different networks

Explanation:

C. To pass traffic between different networks: Layer 3 devices, such as routers and Layer 3 switches, operate at the network layer of the OSI model. Their primary function is to route packets between different networks or subnets. They do this based on the IP address information in the packet headers.

Here's a brief explanation of the other options:

- A. To analyze traffic and drop unauthorized traffic from the Internet:** This is more the function of a firewall or other security device, not a typical Layer 3 device. While some Layer 3 devices may have some security capabilities, this is not their primary function.
- B. To transmit wireless traffic between hosts:** This is the function of a wireless access point, not a typical Layer 3 device. While some Layer 3 devices, such as certain routers, may also function as wireless access points, this is not their primary function.
- D. Forward traffic within the same broadcast domain:** This is the primary function of a Layer 2 device, such as a switch, not a Layer 3 device. Layer 2 devices forward traffic based on MAC addresses within the same broadcast domain (VLAN).

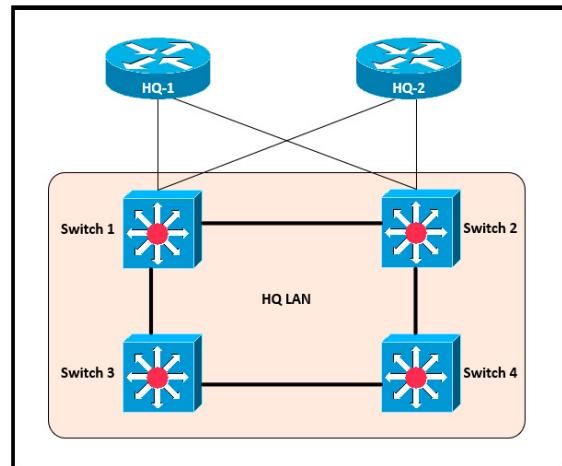
Q351: Refer to the exhibit. After the election process what is the root bridge in the HQ LAN?

Switch 1: 0C:E0:38:81:32:58 -

Switch 2: 0C:0E:15:22:1A:61 -

Switch 3: 0C:0E:15:1D:3C:9A -

Switch 4: 0C:E0:19:A1:4D:16 -



- A. Switch 1
- B. Switch 2
- C. Switch 3
- D. Switch 4

▼ Answer

- A. Switch 1
- B. Switch 2**
- C. Switch 3
- D. Switch 4



More details Steps:

B. Switch 2

Explanation:

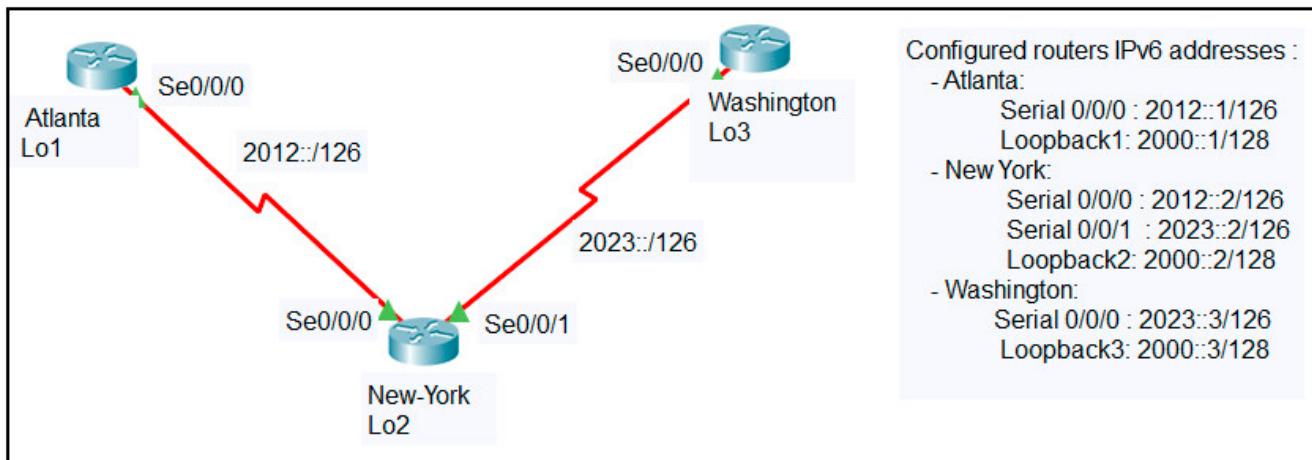
In the Spanning Tree Protocol (STP), the switch with the lowest Bridge ID becomes the root bridge. The Bridge ID is a combination of the priority value and the MAC address. If all switches have the same priority, the one with the lowest MAC address becomes the root bridge.

Comparing the MAC addresses:

- Switch 1: 0C:E0:38:81:32:58
- Switch 2: 0C:0E:15:22:1A:61
- Switch 3: 0C:0E:15:1D:3C:9A
- Switch 4: 0C:E0:19:A1:4D:16

Here, Switch 2 has the lowest MAC address, so it would be elected as the root bridge in the absence of any other configurations.

Q352: An engineer requires a scratch interface to actively attempt to establish a trunk link with a neighbor switch. What command must be configured?



- A. switchport mode trunk
- B. switchport mode dynamic desirable
- C. switchport mode dynamic auto
- D. switchport nonegotiate

▼ Answer

- A. switchport mode trunk
- B. switchport mode dynamic desirable**
- C. switchport mode dynamic auto
- D. switchport nonegotiate



More details Steps:

- B. switchport mode dynamic desirable

Explanation:

B. switchport mode dynamic desirable: In Cisco switches, the `switchport mode dynamic desirable` command makes the interface actively attempt to convert the link to a trunk link. The interface becomes a trunk interface if the neighboring interface is set to trunk, desirable, or auto mode.

Here's a brief explanation of the other options:

- A. switchport mode trunk:** This command forces the interface to become a trunk and does not negotiate with the neighboring interface.
- C. switchport mode dynamic auto:** This command makes the interface able to convert the link to a trunk link but it will not actively attempt to do so. The interface becomes a trunk interface if the neighboring interface is set to trunk or desirable mode.
- D. switchport nonegotiate:** This command prevents the interface from generating DTP (Dynamic Trunking Protocol) frames. It's used when we want to disable the negotiation of trunking. This command is typically used in conjunction with `switchport mode trunk` to prevent the switch from negotiating a trunk link and instead force it to be a trunk link.

Q353: What is a function of TFTP in network operations?

- A. transfers a backup configuration file from a server to a switch using a username and password
- B. transfers files between file systems on a router
- C. transfers a configuration files from a server to a router on a congested link
- D. transfers IOS images from a server to a router for firmware upgrades

▼ Answer

- A. transfers a backup configuration file from a server to a switch using a username and password
- B. transfers files between file systems on a router
- C. transfers a configuration files from a server to a router on a congested link
- D. transfers IOS images from a server to a router for firmware upgrades**

**More details Steps:**

D. Transfers IOS images from a server to a router for firmware upgrades

Explanation:

D. Transfers IOS images from a server to a router for firmware upgrades: TFTP, or Trivial File Transfer Protocol, is a simple, lightweight file transfer protocol commonly used in networking for tasks such as transferring IOS (Internetwork Operating System) images for firmware upgrades. It uses UDP (User Datagram Protocol) and does not require authentication, which makes it less secure but faster and easier to use for certain tasks.

Here's a brief explanation of the other options:

A. Transfers a backup configuration file from a server to a switch using a username and password:

TFTP does not use a username and password for authentication. If authentication is required, FTP (File Transfer Protocol) or SCP (Secure Copy) would be more appropriate.

B. Transfers files between file systems on a router: This is typically done using the router's internal command line interface, not TFTP.

C. Transfers a configuration files from a server to a router on a congested link: While TFTP can be used to transfer configuration files, it lacks any form of congestion control, so it is not the best choice for congested links. Protocols that have congestion control mechanisms, like TCP-based protocols, would be more suitable in this scenario.

Q354: What are two recommendations for protecting network ports from being exploited when located in an office space outside of an IT closet? (Choose two)

- A. configure static ARP entries
- B. enable the PortFast feature on ports
- C. implement port-based authentication
- D. configure ports to a fixed speed
- E. shut down unused ports

▼ Answer

- A. configure static ARP entries
- B. enable the PortFast feature on ports
- C. implement port-based authentication**
- D. configure ports to a fixed speed
- E. shut down unused ports**



More details Steps:

- C. Implement port-based authentication
- E. Shut down unused ports

Explanation:

C. Implement port-based authentication: This is one of the best ways to protect network ports. It requires devices to authenticate before they are allowed network access. IEEE 802.1X is a standard for port-based Network Access Control (PNAC) and provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

E. Shut down unused ports: Disabling or "shutting down" unused ports is a basic security measure. If a port is not in use, it should be disabled to prevent unauthorized access.

Here's a brief explanation of the other options:

- A. Configure static ARP entries:** While this can prevent some types of attacks (like ARP spoofing), it is not specifically related to protecting network ports in office spaces. It's more about securing the network at the protocol level.
- B. Enable the PortFast feature on ports:** PortFast is a Cisco network function which immediately turns on the spanning-tree protocol (STP) PortFast mode on a port connected to a workstation or server. While useful in certain scenarios to reduce the time it takes for the port to start forwarding, it doesn't provide security for network ports.
- D. Configure ports to a fixed speed:** This could improve the performance or stability of a connection, but doesn't directly provide security for network ports.

Q355: What is a recommended approach to avoid co-channel congestion while installing access points that use the 2.4 GHz frequency?

- A. different nonoverlapping channels
- B. different overlapping channels
- C. one overlapping channel
- D. one nonoverlapping channel

▼ Answer

A. different nonoverlapping channels

- B. different overlapping channels
- C. one overlapping channel
- D. one nonoverlapping channel



More details Steps:

- A. Different nonoverlapping channels

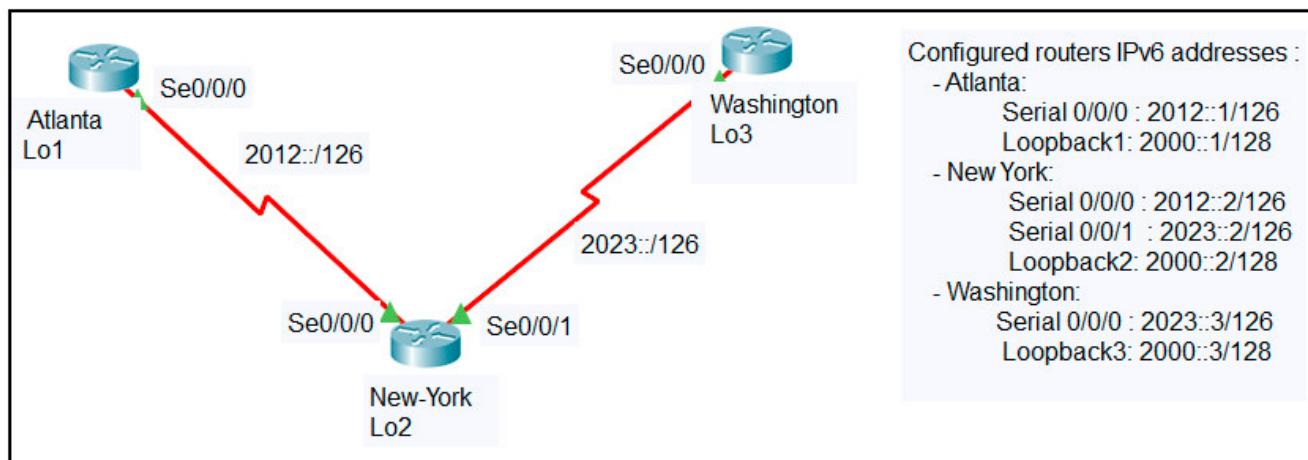
Explanation:

A. Different nonoverlapping channels: In the 2.4 GHz band, only three channels (1, 6, and 11 in most regions) are nonoverlapping. To avoid co-channel congestion (interference) when installing multiple access points, it's recommended to use these three nonoverlapping channels and distribute them among the access points. This allows multiple access points to operate in the same vicinity without interfering with each other.

Here's a brief explanation of the other options:

- B. Different overlapping channels:** Using overlapping channels can lead to co-channel interference. This is not a recommended approach.
- C. One overlapping channel:** Using only one overlapping channel would limit the number of access points that can be installed without interference. This isn't a practical or efficient approach for most networks.
- D. One nonoverlapping channel:** While using a single nonoverlapping channel would avoid co-channel interference, it would also greatly limit network capacity. Using all three nonoverlapping channels (1, 6, 11) provides a better balance of network capacity and interference avoidance.

Q356: Refer to the exhibit. An engineer configured the New York router with state routes that point to the Atlanta and Washington sites. When command must be configured on the Atlanta and Washington routers so that both sites are able to reach the loopback2 interface on the New York router?



- A. ipv6 route ::/0 Serial 0/0/1
- B. ipv6 route 0/0 Serial 0/0/0
- C. ipv6 route ::/0 Serial 0/0/0
- D. ip route 0.0.0.0.0.0 Serial 0/0/0
- E. ipv6 route ::/0 2000::2

▼ Answer

- A. ipv6 route ::/0 Serial 0/0/1
- B. ipv6 route 0/0 Serial 0/0/0
- C. ipv6 route ::/0 Serial 0/0/0**
- D. ip route 0.0.0.0.0.0 Serial 0/0/0
- E. ipv6 route ::/0 2000::2



More details Steps:

- C. ipv6 route ::/0 Serial 0/0/0

Explanation:

C. ipv6 route ::/0 Serial 0/0/0: This command sets up a default route (represented by ::/0 in IPv6) on the Atlanta and Washington routers. All traffic that does not match any other route in the routing table will be sent to this default route. The command specifies that traffic for this route should be sent out of the Serial 0/0/0 interface, which is assumed to be the interface connecting to the New York router.

Here's a brief explanation of the other options:

- A. ipv6 route ::/0 Serial 0/0/1:** This would set up a default route on the incorrect interface. Based on the exhibit, the interface connecting the Atlanta and Washington routers to the New York router is Serial 0/0/0.
- B. ipv6 route 0/0 Serial 0/0/0:** This is not a valid command. The IPv6 version of the command should use ::/0 to represent the default route.
- D. ip route 0.0.0.0.0.0 Serial 0/0/0:** This is not a valid command. The correct syntax for a default route in IPv4 would be `ip route 0.0.0.0 0.0.0.0 Serial 0/0/0`. However, the question pertains to IPv6 routing, so an IPv4 command would not be applicable.
- E. ipv6 route ::/0 2000::2:** This command would set up a default route to the specific IPv6 address 2000::2. However, this does not appear to be the address of the New York router's interface that connects to the Atlanta and Washington routers. According to the exhibit, the New York router's relevant interface addresses are not given. Therefore, using the interface (`Serial 0/0/0`) is a more appropriate solution.

Q357: What is a function of a remote access VPN?

- A. used cryptographic tunneling to protect the privacy of data for multiple users simultaneously
- B. used exclusively when a user is connected to a company's internal network
- C. establishes a secure tunnel between two branch sites
- D. allows the users to access company internal network resources through a secure tunnel

▼ Answer

- A. used cryptographic tunneling to protect the privacy of data for multiple users simultaneously
- B. used exclusively when a user is connected to a company's internal network
- C. establishes a secure tunnel between two branch sites
- D. allows the users to access company internal network resources through a secure tunnel**



More details Steps:

- D. Allows the users to access company internal network resources through a secure tunnel

Explanation:

D. Allows the users to access company internal network resources through a secure tunnel: A Remote Access VPN allows users to securely connect to a private network from a remote location via a public network (such as the internet). This is typically used by remote workers or employees who need to access company resources from outside the office. The connection between the user and the private network is securely encrypted to ensure data privacy.

Here's a brief explanation of the other options:

- A. Used cryptographic tunneling to protect the privacy of data for multiple users simultaneously:** While this statement is partially true (VPNs do use cryptographic tunneling to protect data privacy), it's not specific to remote access VPNs. This describes a general function of VPNs and could apply to both remote access and site-to-site VPNs.
- B. Used exclusively when a user is connected to a company's internal network:** This is incorrect. The main benefit of a remote access VPN is to let users securely connect to a company's internal network from a remote location, not when they are already connected to the internal network.
- C. Establishes a secure tunnel between two branch sites:** This describes a site-to-site VPN, not a remote access VPN. A site-to-site VPN connects two or more networks in different locations, typically office branches, over the internet.

Q358: Which CRUD operation modifies an existing table or view?

- A. read
- B. create
- C. replace
- D. update

▼ Answer

- A. read
- B. create
- C. replace
- D. update**



More details Steps:

- D. Update

Explanation:

D. Update: In the context of CRUD operations (Create, Read, Update, Delete), the "Update" operation is used to modify existing data in a table or view. This might involve changing the values of certain fields for specific records.

Here's a brief explanation of the other options:

- A. Read:** This operation retrieves data from a table or view but does not modify it.
- B. Create:** This operation is used to create new data (like a new record in a table). It doesn't modify existing data.
- C. Replace:** This is not a standard CRUD operation. In some contexts, it might be used to completely replace a record or a set of records, but it's not a standard term in the context of CRUD operations.

Q359: What is a DHCP client?

- A. a workstation that requests a domain name associated with its IP address
- B. a host that is configured to request an IP address automatically
- C. a server that dynamically assigns IP addresses to hosts.
- D. a router that statically assigns IP addresses to hosts.

▼ Answer

A. a workstation that requests a domain name associated with its IP address

B. a host that is configured to request an IP address automatically

C. a server that dynamically assigns IP addresses to hosts.

D. a router that statically assigns IP addresses to hosts.



More details Steps:

B. A host that is configured to request an IP address automatically

Explanation:

B. A host that is configured to request an IP address automatically: A DHCP (Dynamic Host Configuration Protocol) client is a device that is configured to request networking parameters, such as an IP address, subnet mask, default gateway, and DNS servers, from a DHCP server. When a DHCP client connects to a network, it sends out a broadcast query requesting necessary information from a DHCP server.

Here's a brief explanation of the other options:

A. A workstation that requests a domain name associated with its IP address: This is more related to DNS (Domain Name System) services, not DHCP. DNS is used to translate domain names to IP addresses.

C. A server that dynamically assigns IP addresses to hosts: This would be a DHCP server, not a client. The server is the device that hands out the IP addresses, while the client is the device that requests them.

D. A router that statically assigns IP addresses to hosts: This could be a router configured with static routing or static IP assignment, but this is not the role of a DHCP client. A DHCP client requests dynamic IP allocation.

Q360: What is the same for both copper and fiber interfaces when using SFP modules?

- A. They support an inline optical attenuator to enhance signal strength
- B. They provide minimal interruption to services by being hot-swappable
- C. They offer reliable bandwidth up to 100 Mbps in half duplex mode
- D. They accommodate single-mode and multi-mode in a single module

▼ Answer

A. They support an inline optical attenuator to enhance signal strength

B. They provide minimal interruption to services by being hot-swappable

C. They offer reliable bandwidth up to 100 Mbps in half duplex mode

D. They accommodate single-mode and multi-mode in a single module



More details Steps:

B. They provide minimal interruption to services by being hot-swappable

Explanation:

B. They provide minimal interruption to services by being hot-swappable: Both copper and fiber interfaces using Small Form-factor Pluggable (SFP) modules support hot swapping, which means the modules can be plugged in or removed without powering off the system or disrupting the network operations. This provides flexibility and minimizes interruption to services.

Here's a brief explanation of the other options:

A. They support an inline optical attenuator to enhance signal strength: Optical attenuators are used in fiber optic communications to reduce the power level of a signal. This is specific to fiber interfaces and not applicable to copper interfaces.

C. They offer reliable bandwidth up to 100 Mbps in half duplex mode: The bandwidth of SFP modules varies and can be much higher than 100 Mbps. Also, modern networks typically operate in full-duplex mode, not half-duplex.

D. They accommodate single-mode and multi-mode in a single module: SFP modules are either designed for single-mode or multi-mode fiber, not both in a single module. Copper SFPs do not support any fiber modes because they are designed for copper networks.

Q361: When using Rapid PVST+, which command guarantees the switch is always the root bridge for VLAN 200?

- A. spanning-tree vlan 200 priority 614440
- B. spanning-tree vlan 200 priority 38572422
- C. spanning-tree vlan 200 priority 0
- D. spanning-tree vlan 200 root primary

▼ Answer

- A. spanning-tree vlan 200 priority 614440
- B. spanning-tree vlan 200 priority 38572422
- C. spanning-tree vlan 200 priority 0**
- D. spanning-tree vlan 200 root primary



More details Steps:

C. spanning-tree vlan 200 priority 0

Explanation:

C. spanning-tree vlan 200 priority 0: In the Spanning Tree Protocol (STP), the root bridge for each VLAN is the switch with the lowest priority value. By default, all switches have a priority of 32768. Setting the priority to 0 guarantees that unless another switch is explicitly configured with a priority of 0, this switch will become the root bridge for VLAN 200.

D. spanning-tree vlan 200 root primary: This command also makes the switch the root bridge for VLAN 200. However, it doesn't guarantee that the switch will always be the root bridge. If another switch has a lower priority value, that switch would become the root bridge.

Here's a brief explanation of the other options:

A. spanning-tree vlan 200 priority 614440: This command would set an invalid priority. The valid range for STP priority values is 0-61440 in increments of 4096.

B. spanning-tree vlan 200 priority 38572422: This command would not be valid because the priority value is too large. The valid range for STP priority values is 0-61440 in increments of 4096.

Q362: An engineer must configure Interswitch VLAN communication between a Cisco switch and a third-party switch. Which action should be taken?

- A. configure IEEE 802.1p
- B. configure IEEE 802.1q

- C. configure ISL
- D. configure DSCP

▼ Answer

- A. configure IEEE 802.1p
- B. configure IEEE 802.1q**
- C. configure ISL
- D. configure DSCP



More details Steps:

- B. Configure IEEE 802.1q

Explanation:

B. Configure IEEE 802.1q: When communicating between switches from different vendors, IEEE 802.1Q is the industry standard for VLAN tagging. This protocol allows VLAN information to be carried between switches, enabling interswitch VLAN communication.

Here's a brief explanation of the other options:

- A. Configure IEEE 802.1p:** This standard is used for Class of Service (CoS) at the data link layer for quality of service (QoS) in Ethernet networks. It doesn't directly handle VLAN communication between switches.
- C. Configure ISL:** Inter-Switch Link (ISL) is a Cisco-proprietary VLAN tagging protocol. Because ISL is proprietary, it may not be supported on non-Cisco switches.
- D. Configure DSCP:** Differentiated Services Code Point (DSCP) is a field in an IP packet that enables different levels of service to be assigned to network traffic. It is used for QoS on a network, not for interswitch VLAN communication.

Q363: Which protocol prompts the Wireless LAN Controller to generate its own local web administration SSL certificate for GUI access?

- A. HTTPS
- B. RADIUS
- C. TACACS+
- D. HTTP

▼ Answer

- A. HTTPS**
- B. RADIUS
- C. TACACS+
- D. HTTP



More details Steps:

A. HTTPS

Explanation:

A. HTTPS: HTTPS stands for Hypertext Transfer Protocol Secure. It is the secure version of HTTP, the protocol over which data is sent between a browser and a website. When a Wireless LAN Controller (WLC) is accessed via a web-based GUI, it is typically through HTTPS. To secure this communication, the WLC would generate its own local web administration SSL (Secure Sockets Layer) certificate.

Here's a brief explanation of the other options:

B. RADIUS: Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use a network service. It doesn't prompt a WLC to generate an SSL certificate for GUI access.

C. TACACS+: Terminal Access Controller Access-Control System Plus (TACACS+) is another protocol that provides AAA services. Like RADIUS, it does not prompt a WLC to generate an SSL certificate for GUI access.

D. HTTP: HTTP stands for Hypertext Transfer Protocol. While it is used for web-based access, it is not secure by itself and does not prompt the generation of an SSL certificate. Secure communication would require the use of HTTPS, not HTTP.

Q364: In software defined architectures, which plane is distributed and responsible for traffic forwarding?

A. management plane

B. control plane

C. policy plane

D. data plane

▼ Answer

A. management plane

B. control plane

C. policy plane

D. data plane



More details Steps:

D. Data plane

Explanation:

D. Data plane: In networking, the data plane (also known as the forwarding plane) is responsible for processing and forwarding packets to their destinations. This includes functions like packet inspection, forwarding, filtering, and queuing. In a software-defined architecture, the data plane is typically distributed across the network devices that physically handle the traffic.

Here's a brief explanation of the other options:

A. Management plane: The management plane is responsible for network management functions, such as system configuration, management, and monitoring. It's not focused on traffic forwarding.

B. Control plane: The control plane is responsible for determining how data packets should be routed in the network. It's focused on network topology, routing tables, etc. While it directs how traffic should be forwarded, the actual forwarding is done by the data plane.

C. Policy plane: This is not a standard term in the context of network architecture planes. It might refer to the set of rules that govern how the network functions, but it's not responsible for traffic forwarding.

Q365: Which function is performed by the collapsed core layer in a two-tier architecture?

A. enforcing routing policies

B. marking interesting traffic for data polices

C. attaching users to the edge of the network

D. applying security policies

▼ Answer

A. enforcing routing policies

- B. marking interesting traffic for data policies
- C. attaching users to the edge of the network
- D. applying security policies



More details Steps:

- A. Enforcing routing policies

Explanation:

A. Enforcing routing policies: In a two-tier architecture, the collapsed core layer combines the functions of both the core and distribution layers in a three-tier architecture. This includes routing between VLANs, enforcing routing policies, and generally handling high-level, high-capacity traffic within the network.

Here's a brief explanation of the other options:

B. Marking interesting traffic for data policies: This is more likely a function of Quality of Service (QoS) mechanisms, which could be applied at various points in the network, but it is not a specific function of the collapsed core layer.

C. Attaching users to the edge of the network: This is typically a function of the access layer (in a three-tier architecture) or of the edge layer (in a two-tier architecture), which connects end-user devices to the network.

D. Applying security policies: While it is true that the collapsed core layer can apply some security policies, it is not its main function. Security policies are typically applied throughout the network, not just at the core. However, routing policies are a primary function of the collapsed core layer.

Q366: Where does the configuration reside when a helper address is configured to support DHCP?

- A. on the router closest to the server
- B. on the router closest to the client
- C. on every router along the path
- D. on the switch trunk interface

▼ Answer

- A. on the router closest to the server

B. on the router closest to the client

- C. on every router along the path
- D. on the switch trunk interface



More details Steps:

- B. On the router closest to the client

Explanation:

B. On the router closest to the client: The DHCP helper address (also known as the DHCP relay) is typically configured on the router interface closest to the DHCP client. This is because DHCP requests are broadcast messages that do not traverse routers by default. The helper address is used to forward these broadcast messages to the DHCP server, which may be located on a different network segment.

Here's a brief explanation of the other options:

A. On the router closest to the server: The DHCP helper address needs to be configured where the DHCP requests are initially made, which is typically near the client, not the server.

C. On every router along the path: This is not necessary. The router closest to the client can handle forwarding the DHCP requests to the server.

D. On the switch trunk interface: Switches do not typically handle DHCP relay unless they are layer 3 switches. The DHCP helper address is usually configured on a router interface.

Q367: Refer to the exhibit. A network administrator must permit SSH access to remotely manage routers in a network. The operations team resides on the 10.20.1.0/25 network. Which command will accomplish this task?

```
interface GigabitEthernet0/1
ip address 192.168.1.2 255.255.255.0
ip access-group 2699 in
!
access-list 2699 deny icmp any 10.10.1.0 0.0.0.255 echo
access-list 2699 deny ip any 10.20.1.0 0.0.0.255
access-list 2699 permit ip any 10.10.1.0 0.0.0.255
access-list 2699 permit tcp any 10.20.1.0 0.0.0.127 eq 22
```

- A. access-list 2699 permit udp 10.20.1.0 0.0.0.255
- B. no access-list 2699 deny tcp any 10.20.1.0 0.0.0.127 eq 22
- C. access-list 2699 permit tcp any 10.20.1.0 0.0.0.255 eq 22
- D. no access-list 2699 deny ip any 10.20.1.0 0.0.0.255

▼ Answer

- A. access-list 2699 permit udp 10.20.1.0 0.0.0.255
- B. no access-list 2699 deny tcp any 10.20.1.0 0.0.0.127 eq 22
- C. access-list 2699 permit tcp any 10.20.1.0 0.0.0.255 eq 22
- D. no access-list 2699 deny ip any 10.20.1.0 0.0.0.255**



More details Steps:

- D. no access-list 2699 deny ip any 10.20.1.0 0.0.0.255

Explanation:

The access list entry "deny ip any 10.20.1.0 0.0.0.255" is currently blocking all IP traffic from any source to the 10.20.1.0/24 network. This would include SSH traffic. Removing this entry with the command "no access-list 2699 deny ip any 10.20.1.0 0.0.0.255" would stop this denial and allow the existing "permit tcp any 10.20.1.0 0.0.0.127 eq 22" entry to take effect. This would permit SSH (which uses TCP port 22) from any source to the 10.20.1.0/25 network.

Q368: What is the purpose of traffic shaping?

- A. to mitigate delays over slow links
- B. to provide fair queuing for buffered flows
- C. to limit the bandwidth that a flow can use to
- D. be a marking mechanism that identifies different flows

▼ Answer

- A. to mitigate delays over slow links
- B. to provide fair queuing for buffered flows
- C. to limit the bandwidth that a flow can use to**
- D. be a marking mechanism that identifies different flows



More details Steps:

C. To limit the bandwidth that a flow can use

Explanation:

C. To limit the bandwidth that a flow can use: Traffic shaping is a network traffic management technique that regulates the data transfer rate for certain network flows in order to optimize or guarantee performance, improve latency, and/or increase usable bandwidth by delaying packets that meet certain criteria. Essentially, it's about controlling the amount of traffic being sent into a network (or out of a network) to prevent overwhelming the network or a specific link.

Here's a brief explanation of the other options:

A. To mitigate delays over slow links: While traffic shaping can help manage how traffic is sent over slow links, its primary purpose is not to mitigate delay but rather to regulate the rate of traffic to match the available capacity.

B. To provide fair queuing for buffered flows: Fair queuing is a queuing method that can be used to manage different traffic flows, but it's not the primary purpose of traffic shaping. Traffic shaping is about controlling the rate of traffic, not about how packets are buffered or queued.

D. Be a marking mechanism that identifies different flows: Traffic shaping does not mark or identify traffic flows. This is typically done by mechanisms such as Differentiated Services Code Point (DSCP) or IP Precedence in IP headers for quality of service (QoS) purposes. Traffic shaping is about controlling the rate of traffic, not marking or identifying it.

Q369: Which configuration management mechanism uses TCP port 22 by default when communicating with managed nodes?

A. Ansible

B. Python

C. Puppet

D. Chef

▼ Answer

A. Ansible

B. Python

C. Puppet

D. Chef



More details Steps:

A. Ansible

Explanation:

A. Ansible: Ansible is a configuration management, application deployment, and task automation tool. By default, it uses Secure Shell (SSH) for communication with managed nodes, and SSH uses TCP port 22.

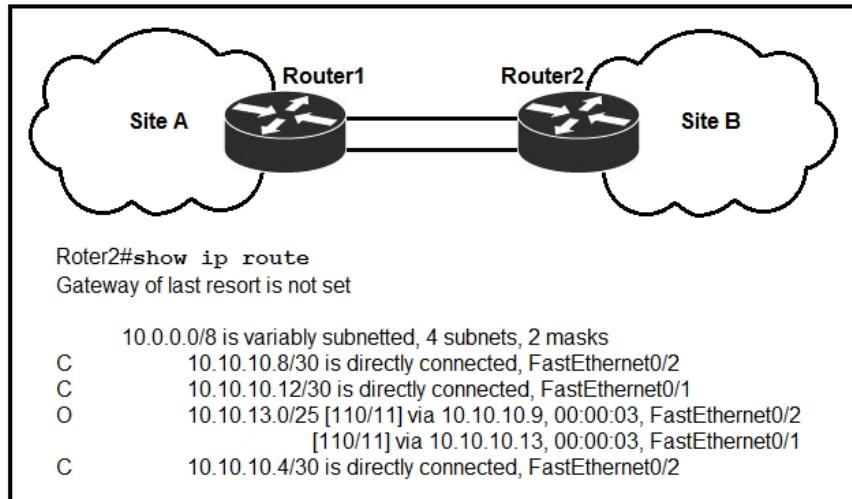
Here's a brief explanation of the other options:

B. Python: Python is a high-level programming language used for a variety of purposes, from web development to data analysis. It is not a configuration management mechanism and doesn't communicate with managed nodes via a specific port. Python scripts could be used in conjunction with any of these tools, but Python itself isn't a configuration management tool.

C. Puppet: Puppet is a configuration management tool that uses a client-server model. The Puppet client (known as the Puppet agent) communicates with the Puppet master server. By default, Puppet uses TCP port 8140, not port 22.

D. Chef: Chef is another configuration management tool that uses a client-server model. The Chef client communicates with the Chef server, but it does not use TCP port 22 by default for these communications.

Q370: Refer to the exhibit. If OSPF Is running on this network, how does Router2 handle traffic from Site B to 10.10.13.128/25 at Site A?



- A. It load-balances traffic out of Fa0/1 and Fa0/2.
- B. It is unreachable and discards the traffic.
- C. It sends packets out of interface Fa0/2.
- D. It sends packets out of interface Fa0/1.

▼ Answer

- A. It load-balances traffic out of Fa0/1 and Fa0/2.
- B. It is unreachable and discards the traffic.**
- C. It sends packets out of interface Fa0/2.
- D. It sends packets out of interface Fa0/1.



More details Steps:

- B. It is unreachable and discards the traffic.

Explanation:

It appears there was an error in interpreting the exhibit. If the destination network 10.10.13.128/25 at Site A is not in the routing table of Router2, then Router2 cannot route packets to this network. As a result, traffic from Site B destined to 10.10.13.128/25 at Site A would be discarded by Router2 because it doesn't know the path to the destination. This situation could occur if the network is down or not advertised by any router in the OSPF area.

Please accept my apologies for the confusion earlier. Thank you for your patience.

Q371: Refer to the exhibit. Which command configures a floating static route to provide a backup to the primary link?

```

Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      Gateway of last resort is 209.165.202.131 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 209.165.202.131
      209.165.200.0/27 is subnetted, 1 subnets
      S        209.165.200.224 [254/0] via 209.165.202.129
                  209.165.201.0/27 is subnetted, 1 subnets
                  S        209.165.201.0 [1/0] via 209.165.202.130

```

- A. ip route 0.0.0.0 0.0.0.0 209.165.202.131
- B. ip route 209.165.201.0 255.255.255.224 209.165.202.130
- C. ip route 0.0.0.0 0.0.0.0 209.165.200.224
- D. ip route 209.165.200.224 255.255.255.224 209.165.202.129 254

▼ Answer

- A. ip route 0.0.0.0 0.0.0.0 209.165.202.131
- B. ip route 209.165.201.0 255.255.255.224 209.165.202.130**

C. ip route 0.0.0.0 0.0.0.0 209.165.200.224

D. ip route 209.165.200.224 255.255.255.224 209.165.202.129 254



More details Steps:

D. ip route 209.165.200.224 255.255.255.224 209.165.202.129 254

Explanation:

D. ip route 209.165.200.224 255.255.255.224 209.165.202.129 254: A floating static route provides a backup path in the event that the primary path fails. It has a higher administrative distance than the primary route. In this case, the exhibit already shows a static route with a high administrative distance of 254. This route will only be used if the primary route to the same destination becomes unavailable. Therefore, the command that configures this floating static route is `ip route 209.165.200.224 255.255.255.224 209.165.202.129 254`.

Here's a brief explanation of the other options:

- A. **ip route 0.0.0.0 0.0.0.0 209.165.202.131:** This command sets a default route, not a floating static route. This route directs any traffic for which the destination network is not in the routing table to 209.165.202.131.
- B. **ip route 209.165.201.0 255.255.255.224 209.165.202.130:** This command sets a static route to the 209.165.201.0/27 network via 209.165.202.130. This is a primary route, not a floating static route.
- C. **ip route 0.0.0.0 0.0.0.0 209.165.200.224:** This command sets a default route to 209.165.200.224. This is a primary route, not a floating static route.

Q372: What is a practice that protects a network from VLAN hopping attacks?

- A. Enable dynamic ARP inspection
- B. Configure an ACL to prevent traffic from changing VLANs
- C. Change native VLAN to an unused VLAN ID
- D. Implement port security on internet-facing VLANs

▼ Answer

- A. Enable dynamic ARP inspection
- B. Configure an ACL to prevent traffic from changing VLANs
- C. Change native VLAN to an unused VLAN ID**
- D. Implement port security on internet-facing VLANs



More details Steps:

C. Change native VLAN to an unused VLAN ID

Explanation:

C. Change native VLAN to an unused VLAN ID: VLAN hopping is a method of attacking a network by sending packets to a port which is not normally accessible. One common method of VLAN hopping is through the use of the native VLAN on a trunk port. By default, the native VLAN is VLAN 1. If an attacker sends frames tagged with the native VLAN ID, they can hop onto that VLAN and potentially access all the networks that are part of that VLAN. To mitigate this, you can change the native VLAN to an unused VLAN ID.

Here's a brief explanation of the other options:

A. Enable dynamic ARP inspection: Dynamic ARP inspection (DAI) is a security feature that validates ARP packets in a network. DAI intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This can help prevent certain types of attacks such as ARP spoofing, but it doesn't specifically protect against VLAN hopping attacks.

B. Configure an ACL to prevent traffic from changing VLANs: Access Control Lists (ACLs) can be used to control traffic flow within a network, including blocking traffic between VLANs. However, this does not specifically prevent VLAN hopping attacks, which exploit the trunking protocol itself to gain unauthorized access to other VLANs.

D. Implement port security on internet-facing VLANs: Port security is a feature that allows you to restrict input to an interface by limiting and identifying MAC addresses of the workstations that are allowed to access the port. While port security can protect against certain types of attacks, it doesn't specifically protect against VLAN hopping attacks.

Q373: Which technology can prevent client devices from arbitrarily connecting to the network without state remediation?

- A. 802.1x
- B. IP Source Guard
- C. MAC Authentication Bypass
- D. 802.11n

▼ Answer

A. 802.1x

- B. IP Source Guard
- C. MAC Authentication Bypass
- D. 802.11n



More details Steps:

A. 802.1x

Explanation:

A. 802.1x: 802.1x is a standard for port-based Network Access Control (PNAC). It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN. It prevents devices from connecting to a network without proper authentication. The authentication involves a process known as "state remediation" where the device's authentication state is checked before allowing access to the network.

Here's a brief explanation of the other options:

B. IP Source Guard: IP Source Guard is a security feature that restricts IP traffic on nonrouted, Layer 2 interfaces by filtering traffic based on the DHCP snooping binding database and on manually configured IP source bindings. While this can prevent IP address spoofing, it doesn't inherently prevent devices from connecting to the network without state remediation.

C. MAC Authentication Bypass: MAC Authentication Bypass (MAB) is a security method that uses the MAC address of the device to grant access to the network. While it can control access to the network, it doesn't involve a state remediation process like 802.1x.

D. 802.11n: 802.11n is a wireless networking standard that improves network throughput and range over its predecessors. It doesn't provide a mechanism to prevent devices from connecting to a network without state remediation.

Q374: What facilitates a Telnet connection between devices by entering the device name?

- A. SNMP
- B. DNS lookup
- C. syslog
- D. NTP

▼ Answer

- A. SNMP
- B. DNS lookup**
- C. syslog
- D. NTP



More details Steps:

B. DNS lookup

Explanation:

B. DNS lookup: DNS (Domain Name System) translates human-readable domain names (like "www.example.com") into computer-readable IP addresses (like "192.0.2.1"). This process, known as a DNS lookup, allows users to connect to another device using a familiar name rather than needing to remember the device's IP address. In the context of a Telnet connection, DNS would allow you to connect to another device by entering its hostname or domain name instead of its IP address.

Here's a brief explanation of the other options:

A. SNMP: Simple Network Management Protocol (SNMP) is a protocol for managing devices on IP networks. It's primarily used for collecting information from, and configuring, network devices, such as servers, printers, routers, switches, etc. It doesn't facilitate a Telnet connection by entering the device name.

C. syslog: Syslog is a standard for message logging. It allows a server to collect information from various network devices to help with system management and security auditing. It also doesn't facilitate a Telnet connection by entering the device name.

D. NTP: Network Time Protocol (NTP) is used to synchronize the time of a computer client or server to another server or reference time source. It does not facilitate a Telnet connection by entering the device name.

Q375: How does the dynamically-learned MAC address feature function?

- A. The CAM table is empty until ingress traffic arrives at each port
- B. Switches dynamically learn MAC addresses of each connecting CAM table.
- C. The ports are restricted and learn up to a maximum of 10 dynamically learned addresses
- D. It requires a minimum number of secure MAC addresses to be filled dynamically

▼ Answer

A. The CAM table is empty until ingress traffic arrives at each port

- B. Switches dynamically learn MAC addresses of each connecting CAM table.
- C. The ports are restricted and learn up to a maximum of 10 dynamically learned addresses
- D. It requires a minimum number of secure MAC addresses to be filled dynamically



More details Steps:

- A. The CAM table is empty until ingress traffic arrives at each port

Explanation:

A. The CAM table is empty until ingress traffic arrives at each port: When a frame arrives at a switch port, the switch examines the source MAC address and the port where the frame arrived. It then adds this information to the CAM (Content Addressable Memory) table, also known as the MAC address table. This process is known as dynamic MAC address learning. Initially, the CAM table is empty, and it gets populated as the switch receives frames on its ports.

Here's a brief explanation of the other options:

B. Switches dynamically learn MAC addresses of each connecting CAM table: This statement is not accurate. Switches do not learn the MAC addresses of CAM tables, but rather, they learn the MAC addresses of frames that arrive on their ports and then store these addresses in their CAM tables.

C. The ports are restricted and learn up to a maximum of 10 dynamically learned addresses: This is a feature of port security, not the basic functioning of dynamic MAC address learning. While you can configure port security to limit the number of MAC addresses learned on a port, this is not a fundamental aspect of how dynamic MAC address learning works.

D. It requires a minimum number of secure MAC addresses to be filled dynamically: This statement is not correct. Dynamic MAC address learning does not require a minimum number of secure MAC addresses. It simply learns MAC addresses as frames arrive on switch ports, regardless of whether those addresses are secure.

Q376: When implementing a router as a DHCP server, which two features must be configured? (Choose two)

- A. relay agent information
- B. database agent
- C. address pool
- D. smart-relay
- E. manual bindings

▼ Answer

- A. relay agent information

- B. database agent

C. address pool

- D. smart-relay

E. manual bindings



More details Steps:

- C. address pool
- E. manual bindings

Explanation:

C. address pool: When implementing a router as a DHCP (Dynamic Host Configuration Protocol) server, an address pool must be configured. This pool is a range of IP addresses that the server can assign to clients.

E. manual bindings: Manual bindings are a feature that allows a DHCP server to assign an IP address to a specific MAC address. This ensures that a device with a particular MAC address will always be assigned the same IP address. This is also known as a static DHCP assignment or a DHCP reservation.

Here's a brief explanation of the other options:

A. relay agent information: A DHCP relay agent is used when the DHCP server is not on the same network as the client. The relay agent forwards requests and replies between the client and server. While a router can function as a DHCP relay agent, it's not a necessary feature for a router functioning as a DHCP server.

B. database agent: There is no "database agent" feature in the context of a DHCP server. It might be a confusion with the DHCP database which keeps track of all the leases, but it's not something that needs to be explicitly configured.

D. smart-relay: While smart-relay is a DHCP feature, it's not necessary when implementing a router as a DHCP server. Smart-relay is used when there are multiple DHCP servers and the first server does not respond, then the DHCPDISCOVER or DHCPREQUEST messages are sent to the next available server.

Q377: Which command must be entered to configure a DHCP relay?

- A. ip helper-address
- B. ip address dhcp
- C. ip dhcp pool
- D. ip dhcp relay

▼ Answer

A. ip helper-address

- B. ip address dhcp
- C. ip dhcp pool
- D. ip dhcp relay



More details Steps:

- A. ip helper-address

Explanation:

A. ip helper-address: The `ip helper-address` command is used to configure a DHCP relay agent in Cisco IOS. This command is applied on the interface that receives the DHCP client broadcasts and forwards them to the specified IP address (usually the IP address of the DHCP server).

Here's a brief explanation of the other options:

B. ip address dhcp: The `ip address dhcp` command is used to configure an interface on a Cisco router to obtain its IP configuration information from a DHCP server. This command does not configure a DHCP relay.

C. ip dhcp pool: The `ip dhcp pool` command is used to create a DHCP pool which contains a range of IP addresses that a DHCP server can assign to clients. This command does not configure a DHCP relay.

D. ip dhcp relay: There isn't an `ip dhcp relay` command in Cisco IOS. It might be a confusion with the `ip helper-address` command which is used to configure a DHCP relay agent.

Q378: Refer to the exhibit. On R1 which routing protocol is in use on the route to 192.168.10.1?

```

R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.14.4 to network 0.0.0.0

C 192.168.12.0/24 is directly connected, FastEthernet0/0
C 192.168.13.0/24 is directly connected, FastEthernet0/1
C 192.168.14.0/24 is directly connected, FastEthernet1/0
  192.168.10.0/24 is variably subnetted, 3 subnets, 3 masks
O   192.168.10.0/24 [110/2] via 192.168.14.4, 00:02:01, FastEthernet1/0
O   192.168.10.32/27 [110/11] via 192.168.13.3, 00:00:52, FastEthernet0/1
O   192.168.0.0/16 [110/2] via 192.168.15.5, 00:05:01, FastEthernet1/1
D   192.168.10.1/32 [90/52778] via 192.168.12.2, 00:03:44, FastEthernet0/0
O*E2 0.0.0.0/0 [110/1] via 192.168.14.4, 00:00:10, FastEthernet1/0

```

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

▼ Answer

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



More details Steps:

- D. EIGRP

Explanation:

In the exhibit, the routing table entry for 192.168.10.1/32 shows **(90/52778) via 192.168.12.2, FastEthernet0/0**, which indicates that this route was learned via EIGRP. The number 90 is the administrative distance for EIGRP, further confirming the use of this routing protocol.

A. RIP, B. OSPF, and C. IGRP are not correct because the administrative distance and metrics for the route to 192.168.10.1 do not correspond to these protocols.

Q379: Refer to the exhibit. Given the output for this command, if the router ID has not been manually set, what router ID will OSPF use for this router?

RouterD# show ip interface brief						
Interface	IP-Address	OK?	Method	Status	Protocol	
FastEthernet0/0	192.168.5.3	YES	manual	up	up	
FastEthernet0/1	10.1.1.2	YES	manual	up	up	
Loopback0	172.16.5.1	YES	NVRAM	up	up	
Loopback1	10.154.154.1	YES	NVRAM	up	up	

- A. 10.1.1.2
- B. 10.154.154.1
- C. 172.16.5.1
- D. 192.168.5.3

▼ Answer

- A. 10.1.1.2
- B. 10.154.154.1
- C. 172.16.5.1**
- D. 192.168.5.3



More details Steps:

The OSPF (Open Shortest Path First) protocol uses the highest IP address on any of the router's active interfaces as the router ID. If a loopback interface is configured, it will use the highest IP address on any of the router's loopback interfaces.

Given the output of the `show ip interface brief` command, we see that there are two loopback interfaces (`Loopback0` and `Loopback1`) with IP addresses `172.16.5.1` and `10.154.154.1` respectively.

Therefore, the highest IP address, which is `172.16.5.1` on `Loopback0`, will be used as the router ID by OSPF.

So, the answer is **C. 172.16.5.1**.

Q380: Refer to the exhibit. Which rule does the DHCP server use when there is an IP address conflict?

```
Router# show ip dhcp conflict
IP address      Detection method      Detection time
172.16.1.32    Ping                  Feb 16 1998 12:28 PM
172.16.1.64    Gratuitous ARP        Feb 23 1198 08:12 AM
```

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

▼ Answer

A. The address is removed from the pool until the conflict is resolved.

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



More details Steps:

When a DHCP server detects an IP address conflict, it follows a specific rule to handle this situation.

The DHCP server uses both Ping and Gratuitous ARP detection methods to ensure that the IP address is not in use before assigning it. If it finds that an IP address is already in use, it will remove the IP address from the pool temporarily to prevent the assignment of the conflicting address.

Once the conflict is resolved, the IP address can be returned to the pool for assignment.