CERT EMPIRE

CISCO CCNA 200-301 Exam Questions

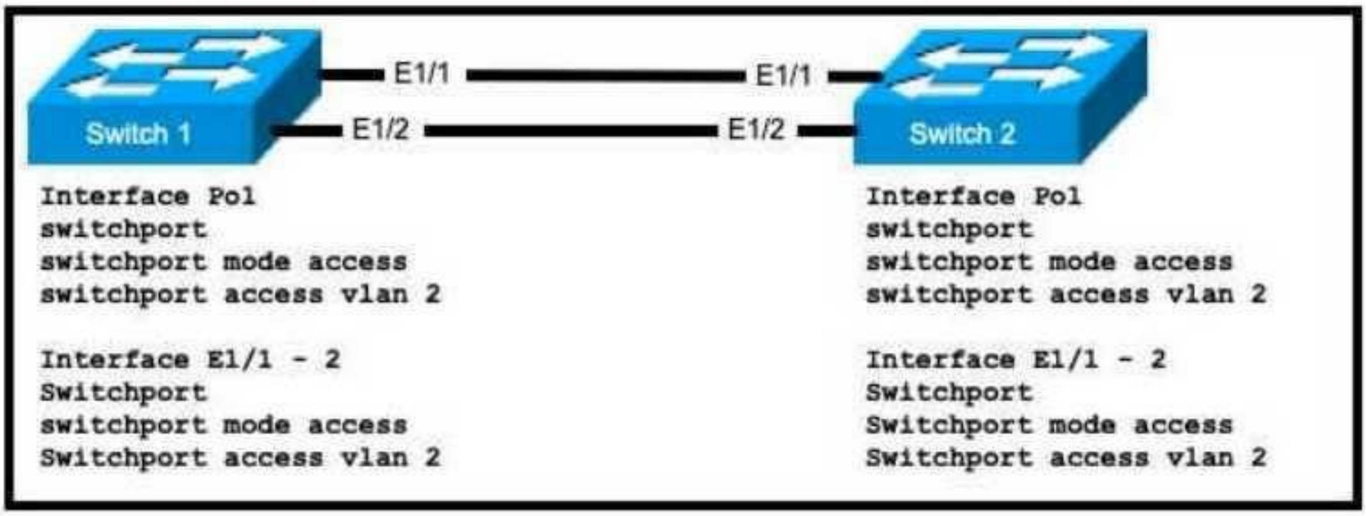
Total Questions: 900+
Demo Questions: 35
Version: Updated for 2025

Prepared and Verified by Cert Empire – Your Trusted IT Certification Partner

For Access to the full set of Updated Questions – Visit:
CCNA 200-301 Exam Dumps by Cert Empire

Question: 1

Refer to the exhibit.



```
Interface Pol
switchport
switchport mode access
switchport access vlan 2

Interface E1/1 - 2
Switchport
switchport mode access
Switchport access vlan 2
```

```
Interface Pol
switchport
switchport mode access
switchport access vlan 2

Interface E1/1 - 2
Switchport
Switchport mode access
Switchport access vlan 2
```

An engineer is configuring an EtherChannel using LACP between Switches 1 and 2 Which configuration must be applied so that only Switch 1 sends LACP initiation packets?

A. Switch 1 (config-if)#channel-group 1 mode on Swrtch2(config-if)#channel-group 1 mode passive

B. Switch1(config-if)#channel-group 1 mode passive Switch2(config-if)#channel-group 1 mode active

C. Switch1config-if)channel-group 1 mode active Switch2(config-if)#channel-group 1 mode passive

D. Switch1(config-if)#channel-group 1 mode on Switch2(config-if)#channel-group 1 mode active

Answer:

C

Explanation:

For an EtherChannel to be formed using LACP (Link Aggregation Control Protocol), ports can be configured in either active or passive mode. Active mode: The port actively sends LACPDU (LACP Data Unit) packets to negotiate the EtherChannel. Passive mode: The port responds to LACPDU packets it receives but does not initiate the LACP negotiation. To ensure that only Switch 1 sends LACP initiation packets, Switch 1 must be configured in active mode, and Switch 2 must be configured in passive mode. This allows Switch 1 to initiate the LACP negotiation, and Switch 2 will respond to form the EtherChannel.

Why Incorrect Options are Wrong:

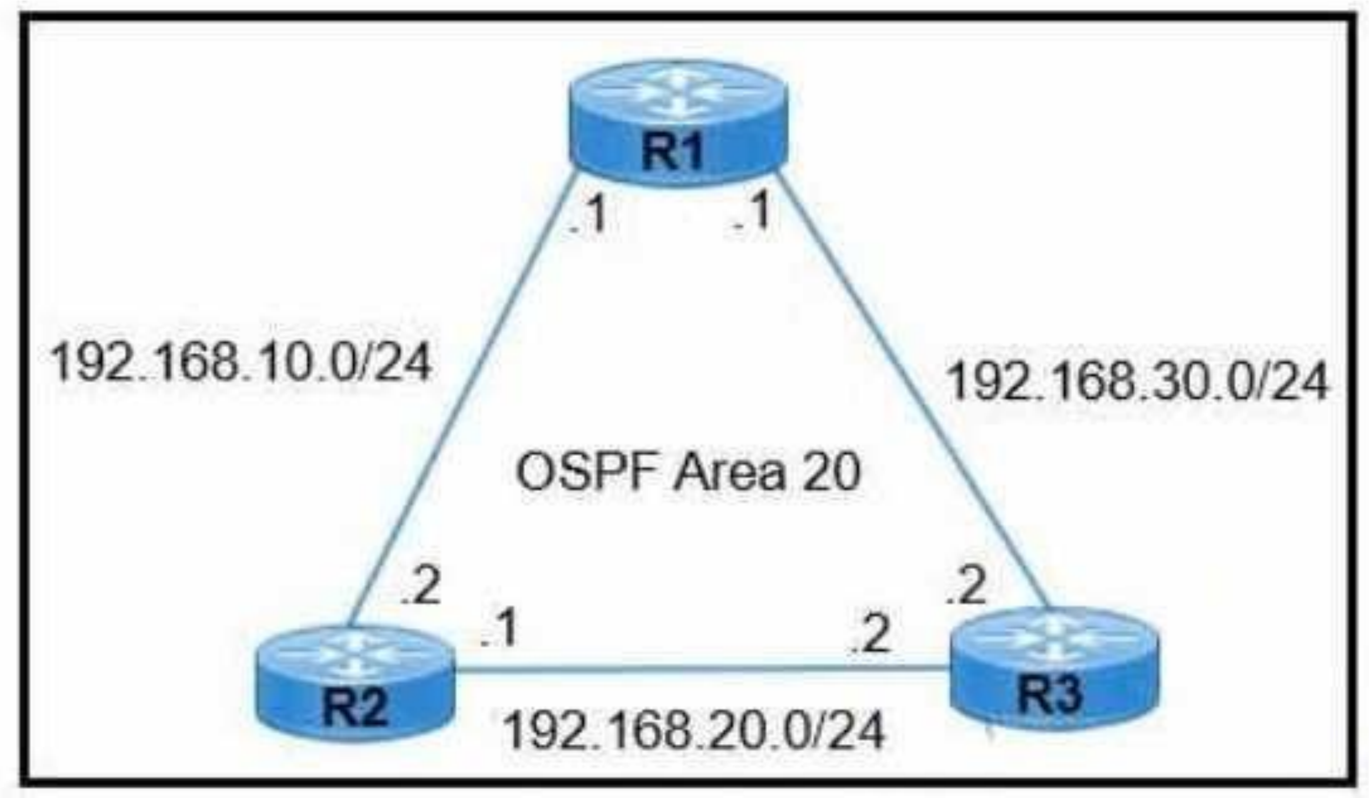
A: mode on on Switch 1 forces the channel without LACP negotiation, which is incompatible with LACP's passive mode on Switch 2. B: Switch 1 in passive mode will not initiate LACP; Switch 2 in active mode will, which contradicts the requirement. D: mode on on Switch 1 forces the channel without LACP, which is incompatible with LACP's active mode on Switch 2.

References:

Cisco IOS Interface and Hardware Component Configuration Guide, Release 15.0SY, "Configuring EtherChannels". (Search for "LACP Modes" or "channel-group mode active passive").
Specifically, the description of LACP modes:
active: "Places a port into an active negotiating state, in which the port initiates negotiations with other ports by sending LACP packets."
passive: "Places a port into a passive negotiating state, in which the port responds to LACP packets that it receives but does not initiate LACP packet negotiation."
Direct URL (example, actual URL may vary based on specific IOS version but content is consistent):
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x3560x/software/release/15-01se/configuration/guide/scg3750x/swethchl.html#wp1114950 (Refer to the section on LACP (802.3ad) EtherChannel Configuration Guidelines and LACP Modes).
IEEE Std 802.3-2018, "IEEE Standard for Ethernet," Clause 43: Link Aggregation. This standard defines LACP behavior.
Section 43.4.2 "LACP functional requirements" describes the active and passive modes.

Question: 2

Refer to the exhibit.



R1 learns all routes via OSPF Which command configures a backup static route on R1 to reach the 192 168.20.0/24 network via R3?

A. R1(config)#ip route 192.168.20.0 255.255.0.0 192.168.30.2

B. R1(config)#ip route 192.168.20.0 255.255.255.0 192.168.30.2 90

C. R1(config)#ip route 192.168.20.0 255.255.255.0 192.168.30.2 111

D. R1(config)#ip route 192.168.20.0 255.255.255.0 192.168.30.2

Answer:

C

Explanation:

To configure a backup static route that is used only when a dynamically learned route (like OSPF) fails, a floating static route is used. This is achieved by setting an administrative distance (AD) for the static route that is higher than the AD of the dynamic routing protocol. OSPF has a default administrative distance of 110. Therefore, the backup static route must have an AD greater than 110. Option C, R1(config)#ip route 192.168.20.0 255.255.255.0 192.168.30.2 111, correctly configures a static route to the 192.168.20.0/24 network via the next-hop 192.168.30.2 (R3's interface) with an administrative distance of 111. Since 111 is greater than OSPF's AD of 110, this route will only be installed in the routing table if the OSPF route to 192.168.20.0/24 is lost.

Why Incorrect Options are Wrong:

/561 A: The subnet mask 255.255.0.0 is incorrect for a /24 network. Also, no AD is specified, defaulting to 1, which would override OSPF. B: The administrative distance of 90 is lower than OSPF's AD (110). This static route would be preferred over the OSPF route, not a backup. D: No administrative distance is specified, so it defaults to 1. This static route would be preferred over the OSPF route, not a backup.

References:

Cisco IOS IP Routing: Protocol-Independent Configuration Guide - "Configuring IP Routing Protocol-Independent Features" - "Administrative Distance" and "Floating Static Routes".
(A general concept covered in Cisco documentation).
"Administrative distance is the feature that routers use in order to select the best path when there are two or more different routes to the same destination from two different routing protocols. Administrative distance defines the reliability of a routing protocol. Each routing protocol is prioritized in order of most to least reliable (believable) with an administrative distance value."
"A floating static route is a static route that is used to back up a dynamically learned route...
A floating static route is configured with a higher administrative distance than the dynamic routing protocol it is backing up."

Default Administrative Distances: OSPF is 110, Static route is 1. (Cisco Press, CCNA 200-301 Official Cert Guide, Volume 1, Chapter 15: Static IPv4 Routing, "Floating Static Routes"; Chapter 18: OSPFv2 Concepts, "OSPFv2 Administrative Distance").
Cisco Command Reference: ip route command.
ip route prefix mask ip-address interface-type interface-number ip-address distance ...
The distance parameter specifies the administrative distance. (Cisco IOS IP Routing: Protocol-Independent Command Reference - ip route).
/561

Question: 3

What is the difference between IPv6 unicast and anycast addressing? A:

A. IPv6 anycast nodes must be explicitly configured to recognize the anycast address, but IPv6 unicast nodes require no special configuration

B. IPv6 unicast nodes must be explicitly configured to recognize the unicast address, but IPv6 anycast

C. An individual IPv6 unicast address is supported on a single interface on one node but an IPv6 anycast address is assigned to a group of interfaces on multiple nodes.

D. Unlike an IPv6 anycast address, an IPv6 unicast address is assigned to a group of interfaces on multiple nodes

Answer:

C

Explanation:

An IPv6 unicast address uniquely identifies a single interface on a single node. Packets sent to a unicast address are delivered to that specific interface. In contrast, an IPv6 anycast address is assigned to a group of interfaces, typically on different nodes. Packets destined for an anycast address are routed to the nearest interface (in terms of routing protocol metrics) that shares that anycast address.

Why Incorrect Options are Wrong:

A: IPv6 anycast addresses are syntactically indistinguishable from unicast addresses; the "anycast" nature comes from configuring the same unicast address on multiple nodes and routing advertisements. B: IPv6 unicast addresses are standard configurations for interfaces; "explicitly configured to recognize" is not a distinguishing feature compared to anycast in this context. D: This statement incorrectly describes IPv6 unicast addresses; unicast addresses are for a single interface, not a group on multiple nodes.

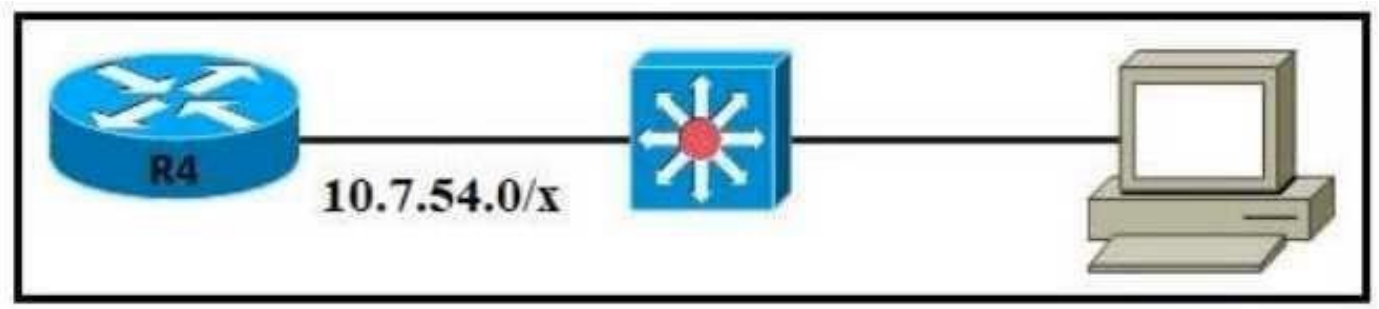
References:

Cisco Press. (2020). CCNA 200-301 Official Cert Guide, Volume 1. Cisco Press.
Chapter 20, "Fundamentals of IP Version 6," section "IPv6 Addressing Formats and Conventions," subsection "Anycast Addresses": "An anycast address is a unicast address that is assigned to more than one interface, typically on different hosts. The routers then determine which host is closest and deliver the packet to that host."
Chapter 20, "Fundamentals of IP Version 6," section "IPv6 Addressing Formats and Conventions," subsection "Unicast Addresses": "A unicast address identifies a single interface on an IPv6 device."

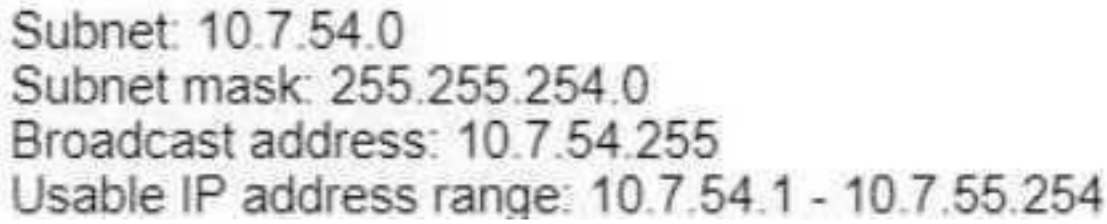
Hinden, R., & Deering, S. (2006). RFC 4291: IP Version 6 Addressing Architecture. IETF.
Section 2.4, "Unicast Addresses": "An identifier for a single interface. A packet sent to a
/561
unicast address is delivered to the interface identified by that address."
Section 2.6, "Anycast Addresses": "An Anycast address is an address that is assigned to more than one interface (typically belonging to different nodes), with the property that a packet sent to an Anycast address is routed to the "nearest" interface having that address..." (Available at: https://www.rfc-editor.org/rfc/rfc4291.html#section-2.6)
Cisco. (n.d.). IPv6 Addressing and Basic Connectivity Configuration Guide, Cisco IOS XE Release 3S. Cisco Systems, Inc.
"IPv6 Unicast Addressing" section: "A unicast address is an identifier for a single interface, on a single node."
"IPv6 Anycast Addresses" section: "An anycast address is an address that is assigned to a set of interfaces that typically belong to different nodes." (Available at: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/xe-3s/ip6-xe-3sbook/ip6-addrg-basic-conn.html - specific page varies by version, search for "IPv6 Anycast Addresses").

Question: 4

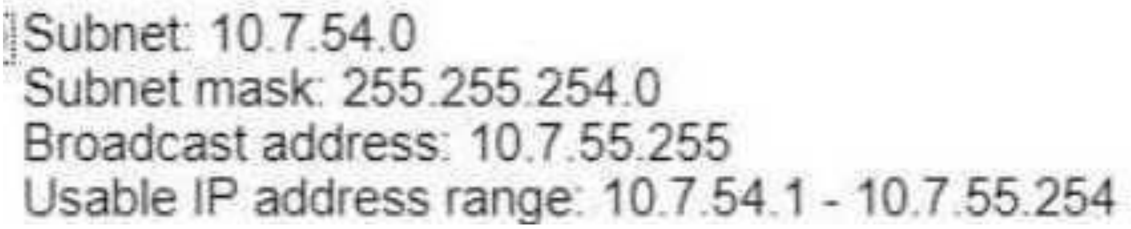
Refer to the exhibit.



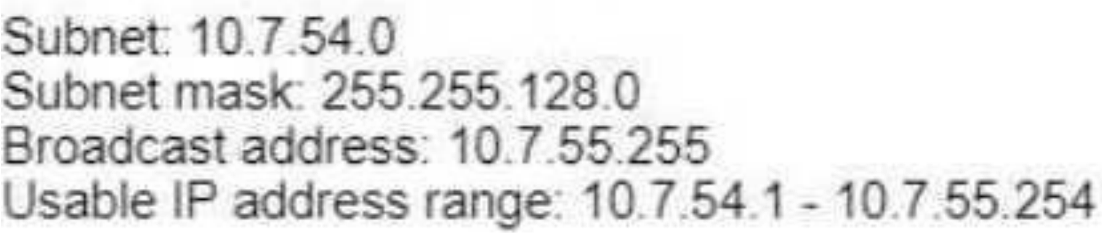
The router has been configured with a supernet to accommodate the requirement for 380 users on a subnet The requirement already considers 30% future growth. Which configuration verifies the IP subnet on router R4? A)


Subnet: 10.7.54.0
Subnet mask: 255.255.254.0
Broadcast address: 10.7.54.255
Usable IP address range: 10.7.54.1 - 10.7.55.254

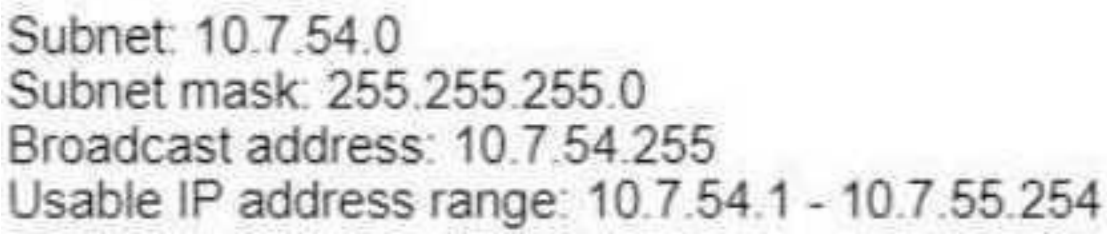
B)


Subnet: 10.7.54.0
Subnet mask: 255.255.254.0
Broadcast address: 10.7.55.255
Usable IP address range: 10.7.54.1 - 10.7.55.254

C)


Subnet: 10.7.54.0
Subnet mask: 255.255.128.0
Broadcast address: 10.7.55.255
Usable IP address range: 10.7.54.1 - 10.7.55.254

D)


Subnet: 10.7.54.0
Subnet mask: 255.255.255.0
Broadcast address: 10.7.54.255
Usable IP address range: 10.7.54.1 - 10.7.55.254

A: Option A B: Option B C: Option C D: Option D

Answer:

B

Explanation:

The question asks to identify the configuration command that verifies the IP subnet on router R4. An "IP subnet" is defined by an IP address and its corresponding subnet mask. The requirement for 380 users, with 30% future growth, means the network must support at least 380 / (1 - 0.30) 543 hosts. This requires 10 host bits (210 - 2 = 1022 hosts), leading to a /22 prefix (32 - 10 = 22 network bits), or a subnet mask of 255.255.252.0. Let's evaluate the options: A) show ip interface brief: This command displays a summary of IP interface information, including the IP address and interface status, but it does not display the subnet mask. Therefore, it cannot fully verify the IP subnet. B) show ip interface GigabitEthernet0/0: This command displays detailed IP information for the specified interface, including its IP address, subnet mask (often shown as a prefix length, e.g., /22), broadcast address, and other IP-specific parameters. The output Internet address is 192.168.0.1/22 directly verifies the IP address and subnet mask. This is a primary command for IP interface verification. C) show running-config interface GigabitEthernet0/0: This command displays the configuration commands currently active for the specified interface, including the ip address command. The output ip address 192.168.0.1 255.255.252.0 verifies the configured IP subnet. D) show interfaces GigabitEthernet0/0: This command provides extensive statistics for an interface, covering Layer 1 and Layer 2 details (like MAC address, errors, duplex, speed) as well as Layer 3 information, including the IP address and subnet mask (Internet address is 192.168.0.1/22). While options B, C, and D all provide the necessary information to verify the IP subnet, the command show ip interface GigabitEthernet0/0 (Option B) is the most precise and directly applicable for verifying the IP-specific operational parameters of an interface. It focuses on IP details without the extensive L1/L2 data of show interfaces or showing the configuration text like show running-config.

Why Incorrect Options are Wrong:

A) show ip interface brief: This command does not display the subnet mask, which is essential for verifying the complete IP subnet. C) show running-config interface GigabitEthernet0/0: While it shows the configured IP subnet, show ip interface is generally preferred for verifying operational IP parameters. D) show interfaces GigabitEthernet0/0: This command is very verbose, providing much L1/L2 information; show ip interface is more focused on IP details.

References:

Cisco IOS IP Addressing Services Command Reference - show ip interface command: "To display the usability status of interfaces configured for IP, use the show ip interface command in privileged EXEC mode. This command displays the IP address, broadcast address, and subnet mask among other IP-related information." (Specific Cisco documentation for this command would confirm its usage for displaying IP address and mask).

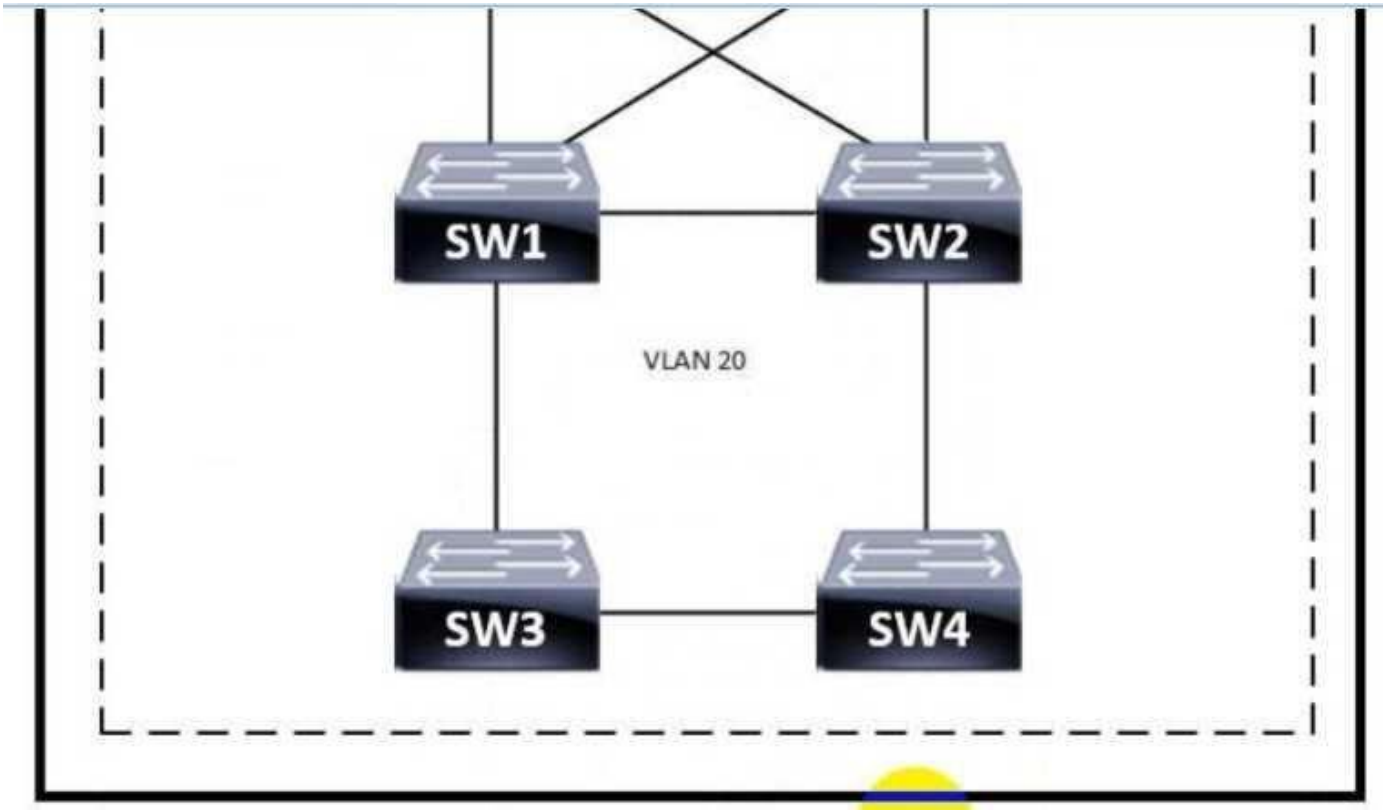
Example: Cisco IOS Interface and Hardware Component Command Reference, show ip interface section. (A general reference as direct URLs to specific internal docs can be transient. The functionality is standard.)

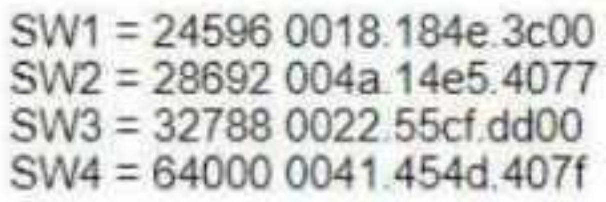
Odom, W. (2019). CCNA 200-301 Official Cert Guide, Volume 1. Cisco Press. Chapter 12, "Verifying IPv4 Addressing and Routing," discusses the use of show ip interface type number as a key command for viewing detailed IPv4 settings, including the IP address and mask. (e.g., page 300).

Cisco IOS Master Command List, Release 15M&T - show ip interface: Describes the command as displaying "IP interface status and configuration." (Available via Cisco's website).

Question: 5

Refer to the exhibit.




SW1 = 24596 0018.184e.3c00
SW2 = 28692 004a.14e5.4077
SW3 = 32788 0022.55cf.dd00
SW4 = 64000 0041.454d.407f

Which switch becomes the root of a spanning tree for VLAN 20 if all li links are of equal speed?

A. SW1

B. SW2

C. SW3

D. SW4

Answer:

C

Explanation:

The root bridge in a Spanning Tree Protocol (STP) topology is elected based on the lowest Bridge ID (BID). The BID consists of a 2-byte Bridge Priority and a 6-byte MAC address. For Per-VLAN Spanning Tree Plus (PVST+), the Bridge Priority field is a combination of a configurable priority value (a multiple of 4096) and the VLAN ID (Extended System ID). For VLAN 20, the STP priorities are calculated as follows: /561 SW1: Configurable Priority 32768 + VLAN ID 20 = 32788. BID: 32788:0000.0C11.1111 SW2: Configurable Priority 32768 + VLAN ID 20 = 32788. BID: 32788:0000.0C22.2222 SW3: Configurable Priority 28672 + VLAN ID 20 = 28692. BID: 28692:0000.0C33.3333 SW4: Configurable Priority 32768 + VLAN ID 20 = 32788. BID: 32788:0000.0C44.4444 Comparing the BIDs, SW3 has the lowest priority value (28692). Therefore, SW3 becomes the root bridge for VLAN 20. The equal speed of links affects path cost calculations for non- root bridges but not the root bridge election itself.

Why Incorrect Options are Wrong:

A (SW1): SW1 has a priority of 32788 for VLAN 20, which is higher than SW3's priority of 28692.
B (SW2): SW2 has a priority of 32788 for VLAN 20, which is higher than SW3's priority of 28692.
D (SW4): SW4 has a priority of 32788 for VLAN 20, which is higher than SW3's priority of 28692.

References:

Cisco Systems, "Understanding and Configuring Spanning Tree Protocol (STP) on Catalyst Switches" - Search on Cisco.com for this document or similar STP configuration guides. Specifically, sections covering Root Bridge Election and Bridge ID (BID) components including priority and extended system ID (VLAN ID).

Example content: The BID is an 8-byte value (2-byte priority + 6-byte MAC). The switch with the numerically lowest BID becomes the root. The priority field includes the extended system ID, which is the VLAN ID for PVST+.

Odom, W. (2019). CCNA 200-301 Official Cert Guide, Volume 1. Cisco Press. Chapter 10: "Spanning Tree Protocol Concepts", Section: "Electing a Root Bridge".

Specifically, the explanation of the Bridge ID (Priority and MAC Address) and how the Extended System ID (VLAN ID) is part of the priority field in PVST+. The default priority is 32768. The switch with the lowest priority value is chosen; if priorities are equal, the lowest MAC address is the tiebreaker. (Approx. pages 268-271 in some editions).

IEEE Std 802.1D-2004, "IEEE Standard for Local and metropolitan area networks--Media Access Control (MAC) Bridges." Section 17.3 "Bridge identifiers" and Section 17.4 "Root Bridge election". (While CCNA focuses on Cisco's implementation, the underlying principles are based on this standard).

Question: 6

Which protocol uses the SSL?

A. HTTP

B. SSH

C. HTTPS

D. Telnet

Answer:

C

Explanation:

HTTPS (Hypertext Transfer Protocol Secure) is the protocol that explicitly uses SSL (Secure Sockets Layer), or its successor TLS (Transport Layer Security), to encrypt the communication channel. This secures data exchanged between a web browser (client) and a web server, ensuring confidentiality and integrity.

Why Incorrect Options are Wrong:

A: HTTP: HTTP (Hypertext Transfer Protocol) is the standard protocol for transmitting hypermedia documents, but it is unencrypted and does not inherently use SSL. B: SSH: SSH (Secure Shell) is a cryptographic network protocol for secure remote login and other secure network services; it uses its own distinct security mechanisms, not SSL/TLS, for its core operations. D: Telnet: Telnet is an older, unsecure protocol for remote terminal access that transmits data, including credentials, in clear text and does not use SSL.

References:

1. Cisco. (n.d.). What Is HTTPS?. Cisco. Retrieved from https://www.cisco.com/c/en/us/products/security/what-is-https.html (This page states: "HTTPS (Hypertext Transfer Protocol Secure) is a secure version of the HTTP protocol that uses the SSL/TLS protocol for encryption and authentication.")

2. Kurose,
J. F., & Ross,
K. W. (2021). Computer Networking: A Top-Down Approach (8th
ed.). Pearson. (Chapter 8, Section 8.6 "Securing TCP Connections: TLS" explains: "HTTP running on top of TLS is often referred to as HTTPS.")

3. Cisco. (n.d.). Transport Layer Security (TLS) Overview. Cisco. Retrieved from https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructurepki/212800-transport-layer-security-tls-overview.html (This document states: "It TLS is
most familiar to users through its use in secure web browsing with HTTPS, which is HTTP

secured by TLS.")

Question: 7

Which two spanning-tree states are bypassed on an interface running PortFast? (Choose two.)

A. disabled

B. listening

C. forwarding

D. learning

E. blocking

Answer:

B, D

Explanation:

PortFast allows an interface to transition directly from the blocking state to the forwarding state, effectively bypassing the listening and learning states. This feature is intended for ports connected to end stations (e.g., PCs, servers) that are not expected to create Layer 2 loops. By skipping the listening and learning states, PortFast minimizes the time it takes for these devices to start communicating on the network after link-up.

Why Incorrect Options are Wrong:

A: disabled: A disabled port is administratively down or not operational; PortFast doesn't bypass this state, it applies to operational ports. C: forwarding: Forwarding is the final operational state that PortFast aims to reach quickly, not bypass. E: blocking: Blocking is the initial state from which PortFast transitions; it is not bypassed.

References:

Cisco, "Understanding and Configuring Spanning Tree Protocol (STP) on Catalyst Switches," (Search for "PortFast" section). While a specific URL changes, this document type is standard. A general search on Cisco's site for "Spanning Tree PortFast" will yield relevant official documentation. For example, the "Spanning Tree Protocol Configuration Guide, Cisco IOS XE Bengaluru 17.6.x (Catalyst 9300 Switches)" discusses PortFast behavior.

Cisco, "Configuring Spanning Tree," Cisco IOS LAN Switching Configuration Guide, Release 12.2. (See section on PortFast). "When you enable PortFast on a switch port, the port immediately changes from the blocking state to the forwarding state, bypassing the usual listening and learning states." (This is a common statement in Cisco STP documentation across various platforms and IOS versions).

IEEE Std 802.1D-2004, "IEEE Standard for Local and metropolitan area networks- Media

Access Control (MAC) Bridges," (See section on Port States and PortFast equivalent concepts like edge ports). While not using the term "PortFast" (a Cisco proprietary feature name), the standard discusses mechanisms for rapid transition for edge ports. Clause 17.19 "Port states" describes the standard states. PortFast is a Cisco implementation that accelerates this for specific port types.

Question: 8

How does Rapid PVST+ create a fast loop-free network topology? A:

A. It requires multiple links between core switches

B. It generates one spanning-tree instance for each VLAN

C. It maps multiple VLANs into the same spanning-tree instance

D. It uses multiple active paths between end stations.

Answer:

B

Explanation:

Rapid PVST+ (Rapid Per-VLAN Spanning Tree Plus) creates a fast, loop-free network topology by running an independent instance of Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w) for each VLAN. This per-VLAN operation allows each VLAN to establish its own optimized, loop-free path. The RSTP mechanisms within each instance ensure rapid convergence to this stable, loop-free state, significantly faster than traditional STP.

Why Incorrect Options are Wrong:

A: It requires multiple links between core switches. RPVST+ manages existing links to prevent loops; multiple links provide redundancy but are not a requirement for its loop- prevention mechanism. C: It maps multiple VLANs into the same spanning-tree instance. This describes the behavior of Multiple Spanning Tree Protocol (MSTP), not RPVST+, which uses one instance per VLAN. D: It uses multiple active paths between end stations. RPVST+, like all STP variants, prevents loops by ensuring only a single active path between any two end stations within a VLAN.

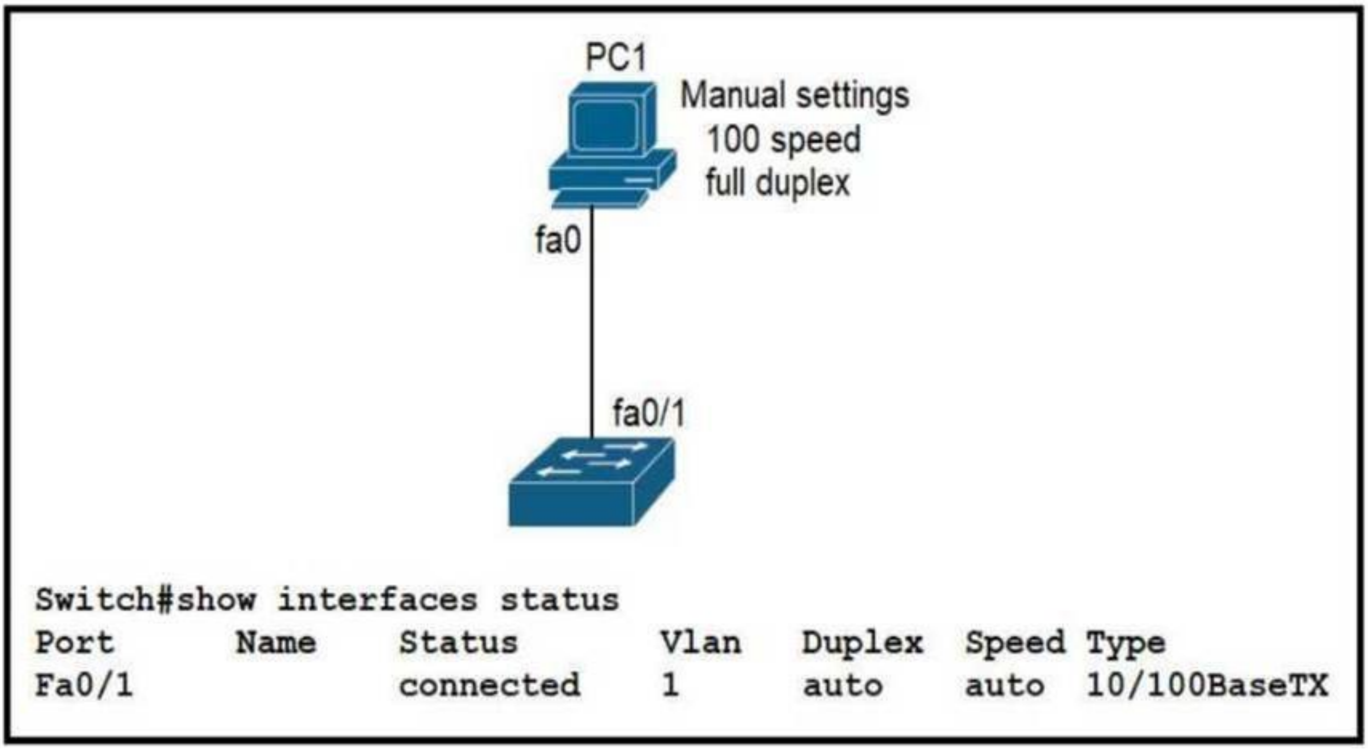
References:

1. Cisco. (n.d.). Spanning Tree Protocol Configuration Guide, Cisco IOS XE Amsterdam 17.3.x (Catalyst 9300 Switches). "Configuring Rapid PVST+". Retrieved from https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/173/configurationguide/lyr23/b173lyr23spanningtree9300cg/configuringspanningtree.html#ID1
08
Relevant text: "Rapid PVST+ is the Cisco implementation of RSTP. It supports PVST+ (one spanning-tree instance for each VLAN)." and "Rapid PVST+ is the IEEE 802.1w (RSTP) standard implemented per VLAN. A single instance of STP runs on each configured VLAN..."
2. Odom, W. (2019). CCNA 200-301 Official Cert Guide, Volume 1. Cisco Press. Chapter 7, "Spanning Tree Protocol Concepts," section "Rapid PVST+ Concepts."
Relevant text: "Rapid PVST+ (RPVST+) is simply Cisco's version of RSTP that provides a

separate instance of 802.1w per VLAN." This highlights that the per-VLAN structure is fundamental to RPVST+, with RSTP providing the fast convergence.

Question: 9

Refer to the exhibit.



```
Switch#show interfaces status
Port      Name      Status        Vlan    Duplex   Speed  Type
Fa0/1               connected     1       auto     auto   10/100BaseTX
```

The link between PC1 and the switch is up. but it is performing poorly. Which interface condition is causing the performance problem?

A. There is a duplex mismatch on the interface

B. There is an issue with the fiber on the switch interface.

C. There is a speed mismatch on the interface.

D. There is an interface type mismatch

Answer:

A

Explanation:

A link that is "up" but "performing poorly" is a classic symptom of a duplex mismatch on an Ethernet interface. When one side of the connection operates in full-duplex mode and the other in half-duplex mode, the full-duplex side may transmit while the half-duplex side is also transmitting or listening. This results in collisions detected by the half-duplex side and often CRC errors or other input errors on the full-duplex side, leading to retransmissions and severely degraded performance. The link itself, however, remains operational.

Why Incorrect Options are Wrong:

B: There is an issue with the fiber on the switch interface. Fiber issues (like dirty connectors or breaks) typically cause the link to be down or flap, not just perform poorly while remaining up. Also, PCs usually connect via copper. C: There is a speed mismatch on the interface. A speed mismatch (e.g., 100 Mbps vs. 1000 Mbps) usually results in the link not coming up at all if autonegotiation fails to find a common speed. D: There is an interface type mismatch. This is vague; if it implies incompatible physical media (e.g., copper to fiber without a converter), the link would not be up.

References:

Cisco IOS LAN Switching Configuration Guide, Release 12.2, "Configuring Interface Characteristics": "A common cause of performance issues on 10/100-Mb Ethernet links is when one port on the link operates at half-duplex while the other port operates at full-duplex." (This general principle is widely documented in Cisco's Ethernet troubleshooting guides).

Note: While a direct URL to a specific page for the 200-301 exam might be from a newer guide, the principle of duplex mismatch causing poor performance is fundamental and consistently documented. A representative modern guide would be:

Cisco, "Troubleshooting Ethernet" (General Cisco documentation often covers this). For example, in many Cisco troubleshooting guides for switches, duplex mismatch is highlighted. Example from a general troubleshooting context: "Symptoms of a Duplex Mismatch: ...The most common symptom of a duplex mismatch is slow throughput..." (Search for "duplex mismatch symptoms cisco" on cisco.com).

IEEE Std 802.3-2018, "IEEE Standard for Ethernet": Clause 28 (Physical Layer link signaling for 10 Mb/s, 100 Mb/s, and 1000 Mb/s Auto-Negotiation) and Clause 30 (Management) describe the auto-negotiation process. Failure in this process, or manual misconfiguration, can lead to duplex mismatches. The standard implies that if duplex modes are mismatched, collisions will occur on the half-duplex link, degrading performance. (e.g., Section 2, Clause 28.2.3.3 "Negotiated ability").

Wendell Odom, "CCNA 200-301 Official Cert Guide, Volume 1", Cisco Press. Chapter 2, "Fundamentals of Ethernet LANs," discusses Ethernet operation, including duplex settings and the impact of mismatches. (While commercial prep, Official Cert Guides are Cisco Press and generally align with official documentation principles). Specific reference to Cisco documentation is preferred over Cert Guides if available for direct citation.

Cisco Learning Network resources often reiterate these concepts. For instance, discussions on Ethernet troubleshooting.

Cisco Support Community, "Troubleshooting Switch Port Problems": This type of document often details duplex mismatch as a primary cause of poor performance on an active link. (e.g., https://community.cisco.com/t5/switching/troubleshooting-switch-port-problems/tap/3106605

- Section on Duplex Mismatch).

Question: 10

Which PoE mode enables powered-device detection and guarantees power when the device is detected?

A. dynamic

B. static

C. active

D. auto

Answer:

B

Explanation:

The static PoE mode on a Cisco switch pre-allocates and reserves the maximum configured power for a port, regardless of whether a powered device (PD) is currently connected. This mode enables PD detection, and crucially, it guarantees that power will be available and supplied to the port once a compatible PD is detected and connected, as the power has already been set aside from the switch's total power budget.

Why Incorrect Options are Wrong:

A: dynamic: "Dynamic" is not a standard Cisco PoE configuration mode keyword. While the auto mode behaves dynamically with power allocation, "dynamic" itself isn't the specific mode that guarantees power. C: active: While PoE operation involves active detection and negotiation, "active" is not a distinct Cisco configuration mode for PoE ports that specifically guarantees power allocation like static mode does. D: auto: The auto mode enables PD detection and supplies power if a PD is detected and if sufficient power is available in the switch's overall budget. It does not guarantee power if the budget is constrained.

References:

Cisco Systems, "Configuring PoE," Catalyst 9300 Series Switches Software Configuration Guide, Cisco IOS XE Bengaluru 17.6.x. Available: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/176/configurationguide/inthw/b176inthw9300cg/configuringpoe.html (See section "PoE Modes" or similar, describing auto and static functionalities).
Specifically, under "PoE Modes": "When you specify static, the switch reserves power for this port even when no device is connected. The switch guarantees that power will be provided to the port when a powered device is connected."
"When you specify auto, the switch automatically detects if the connected device is a powered device and allocates power from the switch power budget. If a device is connected

to a port, the switch turns on power only if it discovers the device and if power is available."

Question: 11

What is an expected outcome when network management automation is deployed?

A. A distributed management plane must be used.

B. Software upgrades are performed from a central controller

C. Complexity increases when new device configurations are added

D. Custom applications are needed to configure network devices

Answer:

B

Explanation:

Network management automation, particularly through centralized controllers like Cisco DNA Center, aims to simplify and streamline network operations. One significant and expected outcome is the ability to perform software upgrades for network devices from a central point. This reduces manual effort, ensures consistency, and allows for scheduled updates across the network, enhancing efficiency and reliability.

Why Incorrect Options are Wrong:

A: A distributed management plane must be used. Automation can utilize centralized management (e.g., a single controller) or distributed models; a distributed plane is not a mandatory outcome. C: Complexity increases when new device configurations are added. Automation typically aims to reduce complexity by using templates and standardized processes, making adding new devices easier. D: Custom applications are needed to configure network devices. While APIs allow for custom solutions, many automation platforms provide built-in tools and interfaces, so custom applications are not always needed.

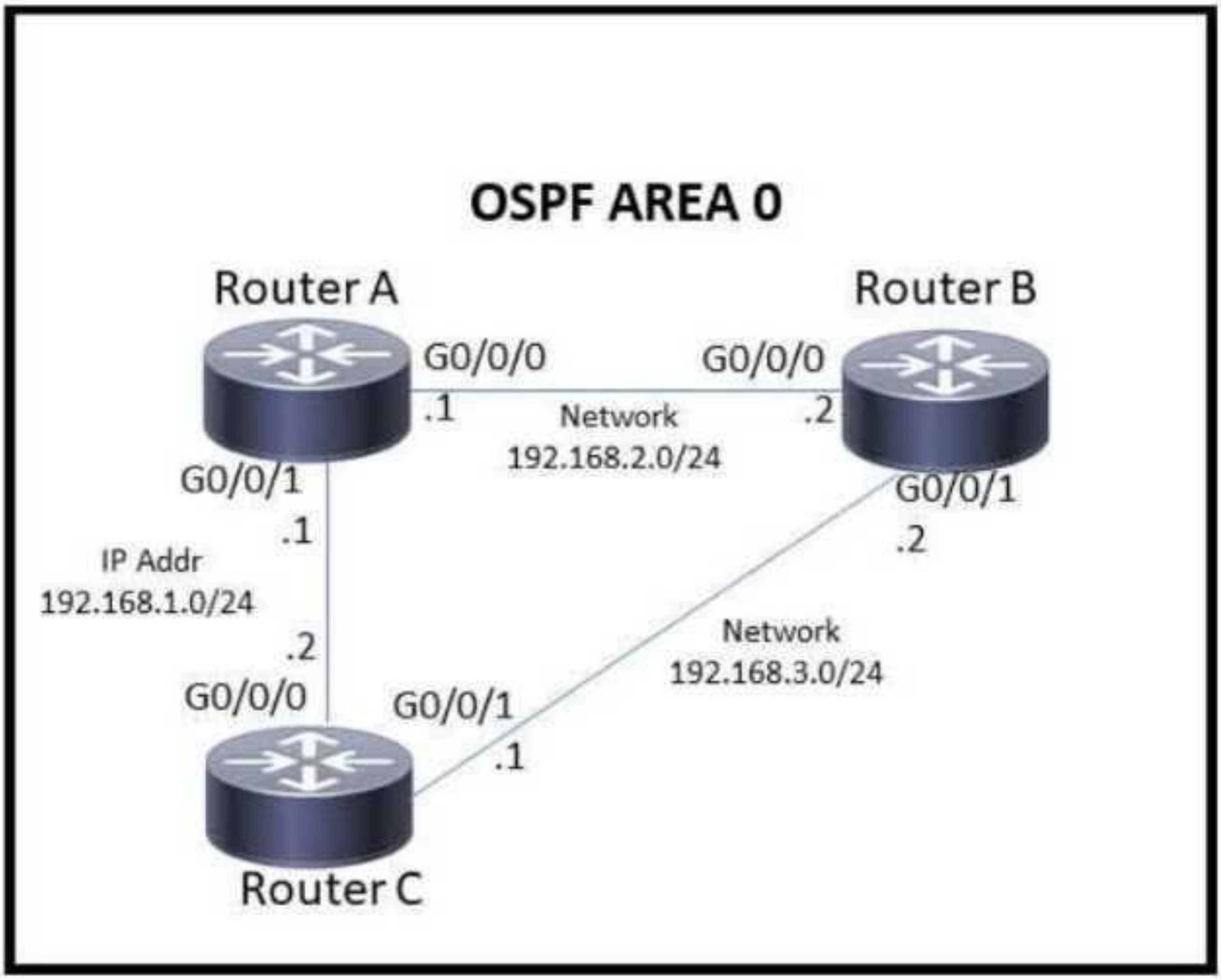
References:

1. Cisco Press, "CCNA 200-301 Official Cert Guide, Volume 2" by Wendell Odom.
Chapter 22, "Introduction to Controller-Based Networking," discusses how controllers centralize network management. Specifically, features like Software Image Management (SWIM) in Cisco DNA Center exemplify centralized software upgrades. (e.g., Section: "Cisco DNA Center Assurance for Network Automation").
"Cisco DNA Center automates several key tasks, including... software image management (SWIM) to upgrade device OS images." (Paraphrased from typical descriptions of DNA Center capabilities).
2. Cisco Learning Network, "CCNA Study Material - Understanding Automation and Programmability."
This resource often highlights the benefits of automation, including centralized management

and simplified operations. The ability to push software updates from a central controller is a
/561
key example of these benefits. (Specific page/section may vary, but the concept is core to Cisco's automation narrative).
URL: (General reference to Cisco's official learning materials for CCNA) e.g., Content on Cisco DNA Center capabilities.
3. Cisco Documentation, "Cisco DNA Center User Guide" or "Cisco DNA Center Solution Overview."
These documents detail the features of Cisco DNA Center, explicitly mentioning Software Image Management (SWIM) as a core function that allows administrators to manage and deploy software images to network devices from a central location.
Example (conceptual, actual URL path may vary):
https://www.cisco.com/c/en/us/products/cloud-systems-management/dna-center/index.html
(See features related to automation and device lifecycle management).

Question: 12

Refer to the exhibit.



Which action must be taken to ensure that router A is elected as the DR for OSPF area 0? A:

A. Configure the OSPF priority on router A with the lowest value between the three routers.

B. Configure router B and router C as OSPF neighbors of router A.

C. Configure the router A interfaces with the highest OSPF priority value within the area.

D. Configure router A with a fixed OSPF router ID

Answer:

C

Explanation:

In OSPF, the Designated Router (DR) election on a multiaccess network segment (like Ethernet, which is implied by the diagram showing multiple routers connected) is determined primarily by the OSPF interface priority. The router with the highest OSPF priority on its interface connected to that segment will be elected as the DR. If priorities are tied, the router with the highest Router ID (RID) wins. To ensure Router A is elected DR, its interface(s) within Area 0 must have the highest OSPF priority among all routers on that segment.

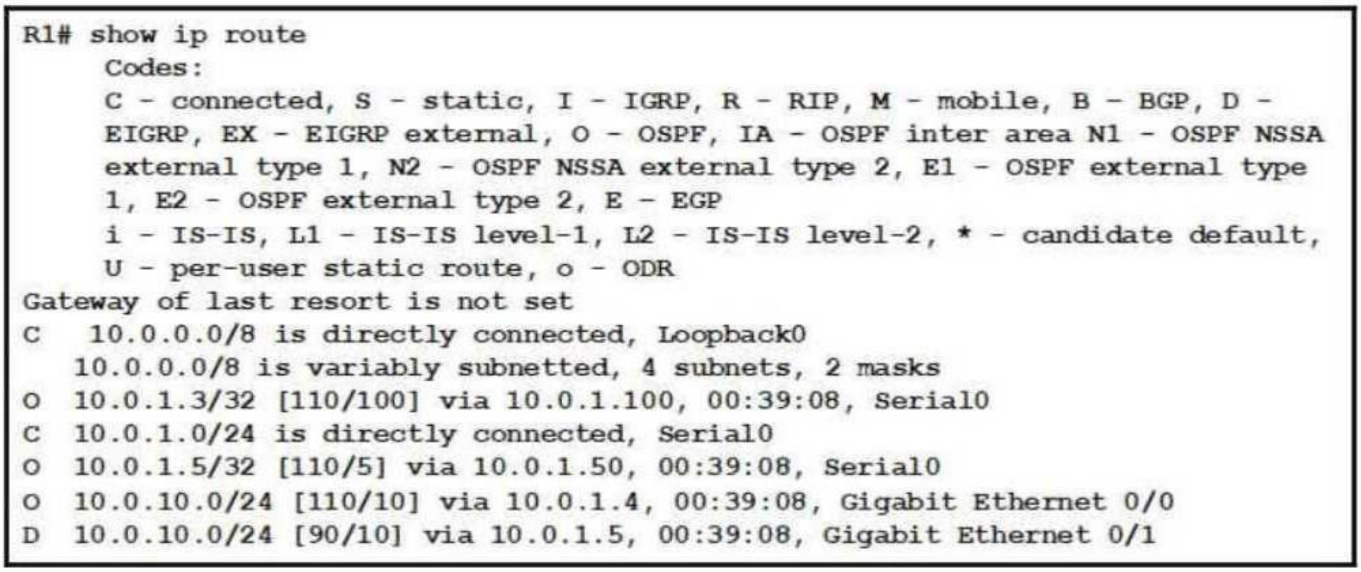
References:

Cisco IOS IP Routing: OSPF Configuration Guide - OSPF Network Design Solutions: Designated Router Election: "OSPF elects a DR and a BDR on every multiaccess network... The router with the highest OSPF priority on a segment will be elected the DR for that segment. The same process is repeated for the BDR. If there is a tie in priority, the router with the higher router ID will be chosen."
URL: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iprouteospf/configuration/15-mt/iro15-mt-book/iro-ospf-overview.html#GUID-70A29167-363F-47F9-959F-263787A396C0
(Refer to the section on DR/BDR election)
Cisco IOS IP Routing: OSPF Command Reference - ip ospf priority: "To set the router priority, which helps determine the designated router (DR) for a network, use the ip ospf priority command in interface configuration mode... The router with the highest priority is elected as the DR."

URL: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iprouteospf/command/iro-crbook/ospf-i1.html#wp1113609037
RFC 2328 - OSPF Version 2, Section 9.4: Electing the Designated Router: "The Designated Router is elected from the set of routers belonging to the network that are eligible to be Designated Router. ....If two routers on the network have the same Router Priority, the one with the highest Router ID is chosen." (This confirms priority is checked first).
URL: https://datatracker.ietf.org/doc/html/rfc2328#section-9.4

Question: 13

Refer to the exhibit.



```
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    10.0.0.0/8 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 10.0.1.100, 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  10.0.10.0/24 [110/10] via 10.0.1.4, 00:39:08, Gigabit Ethernet 0/0
D  10.0.10.0/24 [90/10] via 10.0.1.5, 00:39:08, Gigabit Ethernet 0/1
```

Web traffic is coming in from the WAN interface. Which route takes precedence when the router is processing traffic destined for the LAN network at 10 0.10.0/24?

A. via next-hop 10.0.1.5

B. via next-hop 10 0 1.4

C. via next-hop 10.0 1.50

D. via next-hop 10.0 1 100

Answer:

B

Explanation:

The router selects the best path based on the longest prefix match, then administrative distance (AD), and finally the metric. In this scenario, all listed routes are for the same destination prefix 10.0.10.0/24. Therefore, the selection will be based on the Administrative Distance. The ADs are: Static route (S): 1 EIGRP route (D): 90 OSPF route (O): 110 RIP route (R): 120 The static route S 10.0.10.0/24 1/0 via 10.0.1.4 has the lowest AD (1) and will be chosen.

References:

Cisco Press. CCNA 200-301 Official Cert Guide, Volume 1. Chapter 15: IP Routing. Section: "How Routers Make Forwarding Decisions". (Administrative Distance is a key factor when multiple routes to the same destination prefix exist).
Cisco Systems. IP Routing: Protocol-Independent Configuration Guide, Cisco IOS XE

Release 3S - Route Selection in Cisco IOS Support. (URL: https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocoleigrp/8651-21.html - This document explains route selection, including the role of AD).
"If the prefix length is the same, the router prefers the route with the lower administrative distance."
Cisco Systems. Default Administrative Distances. (URL: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproutepi/configuration/15-mt/iri-15-mtbook/iri-adm-dist.html - Lists default ADs: Static route = 1, EIGRP (internal) = 90, OSPF = 110, RIP = 120).

Question: 14

Which two components comprise part of a PKI? (Choose two.)

A. preshared key that authenticates connections

B. RSA token

C. CA that grants certificates

D. clear-text password that authenticates connections

E. one or more CRLs

Answer:

C, E

Explanation:

A Public Key Infrastructure (PKI) is a framework for managing digital certificates and public- key encryption. Core components include a Certificate Authority (CA), which issues and manages these certificates, binding public keys to entities. Another vital component is the Certificate Revocation List (CRL), published by the CA or a CRL issuer, which lists certificates that are no longer trusted before their official expiry. These elements ensure the integrity and trustworthiness of digital identities and communications within the PKI system.

Why Incorrect Options are Wrong:

A: preshared key that authenticates connections: Preshared keys are symmetric; PKI uses asymmetric cryptography and certificates, not shared secrets. B: RSA token: RSA tokens are authentication devices (e.g., for OTPs), not structural components of the PKI itself. D: clear-text password that authenticates connections: Clear-text passwords offer no cryptographic security and are unrelated to PKI's certificate-based authentication.

References:

1. Cisco Systems, "Public Key Infrastructure Overview" (Part of Cisco IOS Security Configuration Guide).
Direct URL: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/secconnpki/configuration/15mt/sec-pki-15-mt-book/sec-pki-overview.html
Relevant Section: The document lists "Certificate authority (CA)" and "Certificate revocation list (CRL)" as components of a PKI.
2. IETF RFC 5280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".
Direct URL: https://datatracker.ietf.org/doc/html/rfc5280
Relevant Section: Section 3, "PKI Components," explicitly lists "CA: certification authority"

and mentions "CRL issuer" and repositories for CRLs as key parts of a PKI.
3. Odom, W. (2020). CCNA 200-301 Official Cert Guide, Volume 2. Cisco Press.
/561
Relevant Chapter: Chapter 26, "Basic Security Concepts," discusses PKI and its components, including Certificate Authorities and the mechanisms for certificate validation and revocation (like CRLs). (Specific page numbers vary by edition, but the concept is covered in the PKI section).

Question: 15

What are two benefits of FHRPs? (Choose two.)

A. They enable automatic failover of the default gateway.

B. They allow multiple devices to serve as a single virtual gateway for clients in the network.

C. They are able to bundle multiple ports to increase bandwidth.

D. They prevent loops in the Layer 2 network.

E. They allow encrypted traffic.

Answer:

A, B

Explanation:

First Hop Redundancy Protocols (FHRPs) enhance network reliability by providing default gateway redundancy. They enable automatic failover (A) if the primary gateway device fails, ensuring uninterrupted connectivity for end-user devices. FHRPs also allow multiple physical routers to present themselves as a single virtual gateway (B) to hosts on the network, using a shared virtual IP and MAC address. This simplifies host configuration and improves fault tolerance.

Why Incorrect Options are Wrong:

C: Bundling multiple ports to increase bandwidth is a function of EtherChannel (Link Aggregation), not FHRPs. D: Preventing loops in the Layer 2 network is the primary role of Spanning Tree Protocol (STP). E: FHRPs are designed for gateway redundancy and do not inherently provide traffic encryption; other protocols (e.g., IPsec, TLS) handle encryption.

References:

1. Odom, W. (2019). CCNA 200-301 Official Cert Guide, Volume 1. Cisco Press. Chapter 10, "First Hop Redundancy Protocols," states, "The primary benefit of FHRPs is that the end-user devices can continue to send packets to the same default gateway IP address, and the FHRP takes care of the rest, failing over to a working router when the currently active router fails" (supports A) and "FHRPs allow all hosts to use a single default gateway IP address and MAC address, while also allowing the network to have multiple physical routers that can act as that default gateway" (supports B).
2. Cisco. (n.d.). IP Routing: HSRP Configuration Guide, Cisco IOS XE Release 3S - HSRP Overview. Cisco. Retrieved from https://www.cisco.com/c/en/us/td/docs/iosxml/ios/iproutehsrp/configuration/xe-3s/irh-xe-3s-book/irh-hsrp.html. This document explains that HSRP (an FHRP) "provides first-hop routing redundancy" and involves "selecting an

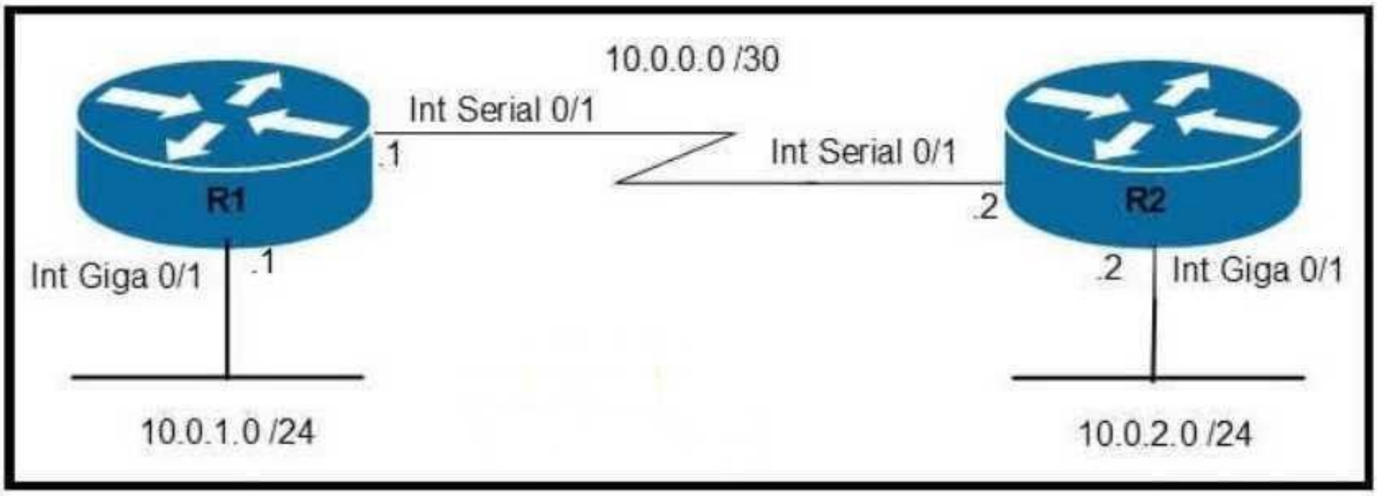
active router and a standby router," which implies automatic failover (supports A) and the
/561
concept of a shared gateway role (supports B).

3. Cisco. (n.d.). Configuring EtherChannels - Understanding EtherChannel. Cisco. Retrieved from https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/173/configurationguide/inthw/b173intandhw9300cg/configuringetherchannels.html. This document describes EtherChannel for bundling links (relevant to why C is incorrect).

4. Cisco. (n.d.). Understanding and Configuring Spanning Tree Protocol (STP) on Catalyst Switches. Cisco. Retrieved from https://www.cisco.com/c/en/us/support/docs/lanswitching/spanning-tree-protocol/5234-5.html. This document explains STP's role in loop prevention (relevant to why D is incorrect).

Question: 16

Refer to the exhibit.



Which command configures OSPF on the point-to-point link between routers R1 and R2?

A. router-id 10.0.0.15

B. neighbor 10.1.2.0 cost 180

C. ipospf priority 100

D. network 10.0.0.0 0.0.0.255 area 0

Answer:

D

Explanation:

The network area command, configured under the OSPF routing process (e.g., router ospf 1), is used to enable OSPF on interfaces whose IP addresses fall within the specified range. In this scenario, the link between R1 (S0/0/0: 10.0.0.1/30) and R2 (S0/0/0: 10.0.0.2/30) uses the 10.0.0.0/30 network. The command network 10.0.0.0 0.0.0.255 area 0 would match these interface IP addresses (10.0.0.1 and 10.0.0.2) and enable OSPF on them, placing them in area 0. This is a fundamental method for activating OSPF on specific network segments.

Why Incorrect Options are Wrong:

A: router-id 10.0.0.15: This command sets the OSPF router ID, which is essential for the OSPF process but does not enable OSPF on any specific interface or link. B: neighbor 10.1.2.0 cost 180: This command is used to manually define OSPF neighbors, typically in Non-Broadcast Multi-Access (NBMA) environments. It's not the standard way to enable OSPF on a point-to-point link. C: ip ospf priority 100: This is an interface-level command that influences the Designated Router (DR) and Backup Designated Router (BDR) election process. DR/BDR elections do not occur on point-to-point links. /561

References:

Cisco Systems, "IP Routing: OSPF Command Reference - network area". (Search for "network area command ospf cisco" on Cisco's official documentation site). A general reference: "The network address wildcard-mask area area-id command defines the interfaces on which OSPF runs and the area ID for those interfaces." (Cisco Press, CCNA 200-301 Official Cert Guide, Volume 1, Chapter 16: OSPF Network Types and Neighbors).

Cisco Systems, "IP Routing: OSPF Command Reference - router-id". (Search for "router-id command ospf cisco").

Cisco Systems, "IP Routing: OSPF Command Reference - neighbor (OSPF)". (Search for "neighbor command ospf cisco").

Cisco Systems, "IP Routing: OSPF Command Reference - ip ospf priority". (Search for "ip ospf priority command cisco").

Cisco Press, CCNA 200-301 Official Cert Guide, Volume 1, by Wendell Odom. Chapter 15, "Implementing OSPF," section "OSPF Configuration," subsection "The network Command." (This typically covers how the network command enables OSPF on interfaces).

Question: 17

What causes a port to be placed in the err-disabled state?

A. nothing plugged into the port

B. link flapping

C. shutdown command issued on the port

D. latency

Answer:

B

Explanation:

The err-disabled state is a feature on Cisco switches that automatically disables a port when specific network errors or misconfigurations are detected. Link flapping, which occurs when a port's physical link repeatedly transitions between up and down states in rapid succession, is a recognized condition that can trigger the err-disabled state. This mechanism helps prevent network instability that might arise from faulty hardware (like a cable or NIC) or other physical layer issues causing the flapping.

Why Incorrect Options are Wrong:

A: nothing plugged into the port: This results in a 'down/down' or 'notconnect' port state, not err-disabled. C: shutdown command issued on the port: This places the port in an 'administratively down' state, which is a deliberate manual action. D: latency: Latency is a measure of network delay; while it can be a symptom of issues that might lead to err-disable (e.g., a loop), it is not a direct trigger itself.

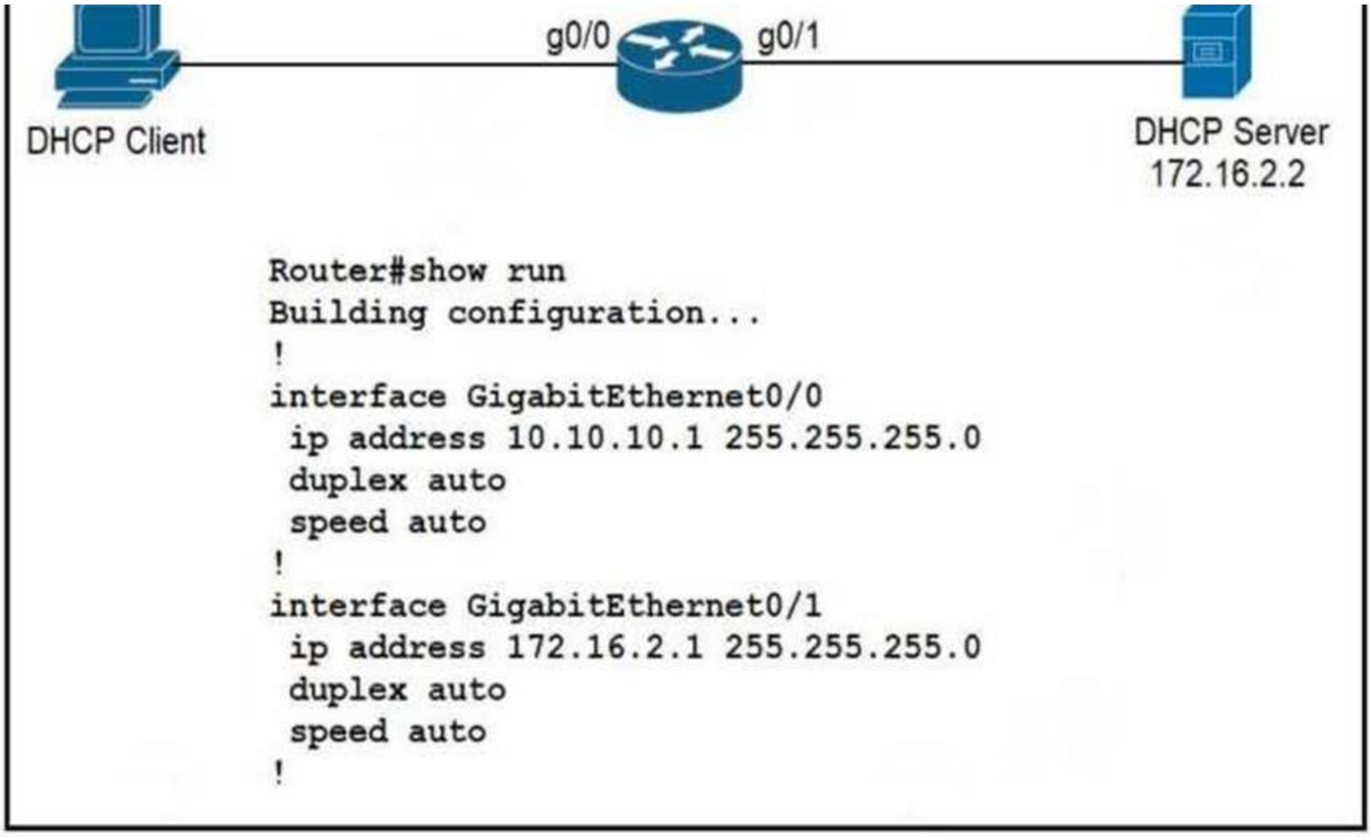
References:

1. Cisco Systems. (n.d.). Errdisable Port State Recovery on the Cisco IOS Platforms. Cisco. Retrieved from https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-treeprotocol/69980-errdisable-recovery.html (See section "Reasons for Ports Going into Errdisable Mode," which lists "link-flap" as a cause: "The port is put into the errdisabled state if it flaps more than five times in 10 seconds.")

2. Odom, W. (2019). CCNA 200-301 Official Cert Guide, Volume 1. Cisco Press. (The concept of err-disabled state and various triggers like port security violations and BPDU Guard are discussed, aligning with the protective nature of the err-disabled state. The specific "link-flap" cause is detailed in the Cisco technical document.)

Question: 18

Refer to the exhibit.



```
Router#show run
Building configuration...
!
interface GigabitEthernet0/0
 ip address 10.10.10.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 172.16.2.1 255.255.255.0
 duplex auto
 speed auto
!
```

An engineer is configuring a new router on the network and applied this configuration. Which additional configuration allows the PC to obtain its IP address from a DHCP server?

A. Configure the ip dhcp relay information command under interface Gi0/1.

B. Configure the ip dhcp smart-relay command globally on the router

C. Configure the ip helper-address 172.16.2.2 command under interface Gi0/0

D. Configure the ip address dhcp command under interface Gi0/0

Answer:

C

Explanation:

DHCP requests from clients are typically broadcast messages. Routers, by default, do not forward these broadcasts between different network segments. To enable a PC on one network segment (connected to Gi0/0) to obtain an IP address from a DHCP server on another segment (172.16.2.2), the router interface connected to the PC must be configured as a DHCP relay agent. The ip helper-address command, applied to the interface receiving the client's DHCP broadcast (Gi0/0), forwards these requests as unicast packets to the specified DHCP server. /561

Why Incorrect Options are Wrong:

A: The ip dhcp relay information command is used to configure DHCP option 82 (Relay Agent Information Option), not the primary relay function. B: The ip dhcp smart-relay command is a global configuration that can simplify relay in some scenarios but ip helper-address is the specific interface-level command required here. D: The ip address dhcp command configures the router interface itself to obtain an IP address from a DHCP server, not to relay requests for other clients.

References:

1. Cisco IOS IP Addressing Services Configuration Guide, Release 15M&T - Configuring DHCP DHCP Relay Agent: "To configure a DHCP relay agent, you must configure the ip helper-address command on the interface that is receiving client DHCP requests."
URL: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddrdhcp/configuration/15mt/dhcp-15-mt-book/dhcp-relay-agent.html (Search for "Configuring the DHCP Relay Agent"
and "ip helper-address")
2. Cisco IOS IP Addressing Services Command Reference - ip helper-address: "To enable the forwarding of UDP broadcasts, including BOOTP and DHCP, use the ip helper-address command in interface configuration mode."
URL: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddrdhcp/command/dhcp-crbook/dhcp-i1.html#wp1017909
3. Cisco CCNA 200-301 Official Cert Guide, Volume 1, Chapter 21: IP Addressing Services DHCP Relay: "The router interface on the subnet with DHCP clients needs one command: ip helper-address server-ip-address."
(Note: While this is a commercial prep material, the concept and command usage are standard and align with official Cisco documentation. The explanation here is based on the Cisco IOS documentation.)
Reference to official Cisco documentation for the command's function: Cisco IOS IP Addressing Services Configuration Guide.
4. IEEE Std 802.11-2016 - IEEE Standard for Information technology- Telecommunications and information exchange between systems Local and metropolitan area networks- Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications (While not directly about DHCP relay on routers, DHCP is a fundamental IP service often discussed in networking standards contexts. The core issue is broadcast forwarding, which ip helper-address solves for DHCP.)
(This source is less direct but establishes the context of IP services. The primary justification comes from Cisco's own documentation for its IOS.)
More direct Cisco documentation is preferred and used above.

Question: 19

Which Layer 2 switch function encapsulates packets for different VLANs so that the packets traverse the same port and maintain traffic separation between the VLANs? A:

A. VLAN numbering

B. VLAN tagging

C. VLAN marking

Answer:

B

Explanation:

VLAN tagging, specifically using the IEEE 802.1Q standard, is the Layer 2 switch function that allows frames from different VLANs to traverse the same physical port (a trunk port). This process involves inserting a 4-byte tag into the Ethernet frame header. This tag includes a VLAN Identifier (VID), which enables switches to distinguish traffic from different VLANs, thereby maintaining traffic separation while using a shared link.

Why Incorrect Options are Wrong:

A: VLAN numbering: This refers to the assignment of a unique numerical ID to a VLAN (e.g., VLAN 10, VLAN 20), not the process of encapsulating frames for transport across a trunk. C: VLAN marking: While sometimes used loosely, "marking" often refers to setting Quality of Service (QoS) bits (like CoS in the 802.1Q tag). "Tagging" is the more precise term for adding the VLAN identification header.

References:

1. Cisco Systems, Inc. (2020). CCNA 200-301 Official Cert Guide, Volume 1. Cisco Press. Chapter 7, "VLANs and VLAN Trunks," Section "VLAN Trunks," subsection "IEEE 802.1Q": "IEEE 802.1Q, often simply called Dot1q, is the most common VLAN trunking protocol today. 802.1Q defines a 4-byte VLAN tag that is inserted into an Ethernet frame." This describes the process of VLAN tagging.
2. Cisco Networking Academy. (Content for CCNAv7). Switching, Routing, and Wireless Essentials Companion Guide. Cisco Press.
Module 3: VLANs, Section 3.2 "VLAN Trunks": "A VLAN trunk is a point-to-point link that carries more than one VLAN. A VLAN trunk extends VLANs across an entire network. Cisco supports IEEE 802.1Q for coordinating trunks on Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces." The mechanism for this is VLAN tagging.
3. IEEE Std 802.1QTM -2018. IEEE Standard for Local and metropolitan area networks-Bridges and Bridged Networks.

Clause 9, "VLAN Tagging": This clause details the format of the VLAN tag (including the
/561
VID) and how it is inserted into frames to identify VLAN membership. This is the authoritative standard for VLAN tagging. (Available via IEEE Xplore) .

Question: 20

Which type of IPv6 address is similar to a unicast address but is assigned to multiple devices on the same network at the same time?

A. global unicast address

B. anycast address

C. multicast address

D. link-local address

Answer:

B

Explanation:

An IPv6 anycast address is assigned to multiple interfaces (typically on different devices). Packets sent to an anycast address are routed to the nearest interface having that address, according to the routing protocol's measure of distance. This means that although multiple devices share the address, only one (the "closest") receives a given packet, making its behavior similar to a unicast address in terms of packet delivery to a single endpoint for a specific communication.

Why Incorrect Options are Wrong:

A: global unicast address: Identifies a single interface, not multiple devices simultaneously for the same address. C: multicast address: Delivers packets to all interfaces in a group, not just one "nearest" device. D: link-local address: A type of unicast address used for communication on a single local link, not typically assigned to multiple devices to provide a service like anycast.

References:

Cisco Press, CCNA 200-301 Official Cert Guide, Volume 1, Chapter 16: IPv6 Addressing and Subnetting. (Specifically, the section on "IPv6 Address Types" which describes unicast, multicast, and anycast addresses.)
"Anycast addresses are syntactically indistinguishable from unicast addresses because anycast addresses are allocated from the unicast address space... An anycast address is assigned to a set of interfaces on different nodes. A packet sent to an anycast address is delivered to only one of the interfaces- the one that is closest to the source, according to the routing protocol's measure of distance."
RFC 4291, "IP Version 6 Addressing Architecture," Section 2.6 "Anycast Addresses." (This is the primary IETF standard defining IPv6 addressing.)
"An anycast address is an address that is assigned to more than one interface (typically belonging to different nodes), with the property that a packet sent to an anycast address is

routed to the "nearest" interface having that address, according to the routing protocols'
/561
measure of distance."
URL: https://datatracker.ietf.org/doc/html/rfc4291#section-2.6
Cisco IOS IPv6 Configuration Guide, "IPv6 Addressing and Basic Connectivity" section.
(Official Cisco documentation often details these address types.)
"An anycast address is a unicast address that is assigned to a set of interfaces (typically on different devices). A packet sent to an anycast address is delivered to the closest interface (identified by the routing protocols) that is assigned the anycast address."
Example URL (may vary by specific IOS version, but concept is consistent):
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/15-mt/ip6-15-mtbook/ip6-addrg-basic-conn.html (Search for "Anycast Addresses")

Question: 21

Which two network actions occur within the data plane? (Choose two.)

A. Add or remove an 802.1Q trunking header.

B. Make a configuration change from an incoming NETCONF RPC.

C. Run routing protocols.

D. Match the destination MAC address to the MAC address table.

E. Reply to an incoming ICMP echo request.

Answer:

A, D

Explanation:

The data plane is responsible for the actual forwarding of data packets based on decisions made by the control plane. Adding or removing an 802.1Q trunking header (A) is a frame modification performed during the forwarding process. Matching the destination MAC address to the MAC address table (D) is a lookup operation that directly determines the outgoing port for a frame. Both are fundamental data plane operations involved in packet/frame processing and forwarding.

References:

1. Odom, W. (2020). CCNA 200-301 Official Cert Guide, Volume 2. Cisco Press.
Chapter 21, "Understanding Controller-Based Networking," section "Control Plane and Data Plane." Specifically, the description of data plane functions: "For example, a router de-encapsulates and re-encapsulates a packet, adds or removes an 802.1Q trunking header, matches the destination MAC address in its MAC address table, matches the destination IP address in its IP routing table..." This directly supports options A and D.
The same chapter describes control plane functions: "...routing protocols that learn routes..." supporting why C is incorrect.
The same chapter describes management plane functions: "...interfaces that allow a network engineer to manage the device (for example, CLI, SNMP, and even APIs like NETCONF...)" supporting why B is incorrect.
2. Cisco. (n.d.). Cisco IOS XE Software Defined Networking: The Controller and the
/561
Network. Cisco. Retrieved from a general understanding of Cisco's architecture documentation (though a direct public URL for this specific phrase in a foundational document is broad, the concept is standard). The principle that packets destined to the device itself (like ICMP replies generated by the device) are handled by the control plane is a core networking concept. For example, see Cisco Live presentations or white papers on

router architecture, e.g., "Router Architecture Overview." A specific document: "Control Plane Policing Implementation Best Practices" on Cisco.com often discusses traffic handled by the route processor (control plane) vs. forwarding hardware (data plane). ICMP destined for the router is typically processed by the route processor.

For instance, the concept is explained in many Cisco technical documents, such as those discussing Control Plane Policing (CoPP), where traffic like ICMP to the device is managed as control plane traffic. While a single URL is hard to pinpoint for such a fundamental concept without a specific document title, it's widely covered in Cisco's technical literature. A relevant section in the CCNA 200-301 Official Cert Guide, Vol 1, Chapter 17, "Basic Router Configuration," implicitly supports this when discussing how a router processes pings to its own interfaces.

Question: 22

Which QoS traffic handling technique retains excess packets in a queue and reschedules these packets for later transmission when the configured maximum bandwidth has been surpassed?

A. weighted random early detection

B. traffic policing

C. traffic shaping

D. traffic prioritization

Answer:

C

Explanation:

Traffic shaping is a QoS mechanism that delays excess packets by storing them in a queue (buffering) when the traffic rate exceeds a configured maximum. These buffered packets are then scheduled for transmission later, smoothing out traffic bursts and ensuring the traffic conforms to the desired rate. This process effectively retains and reschedules packets.

Why Incorrect Options are Wrong:

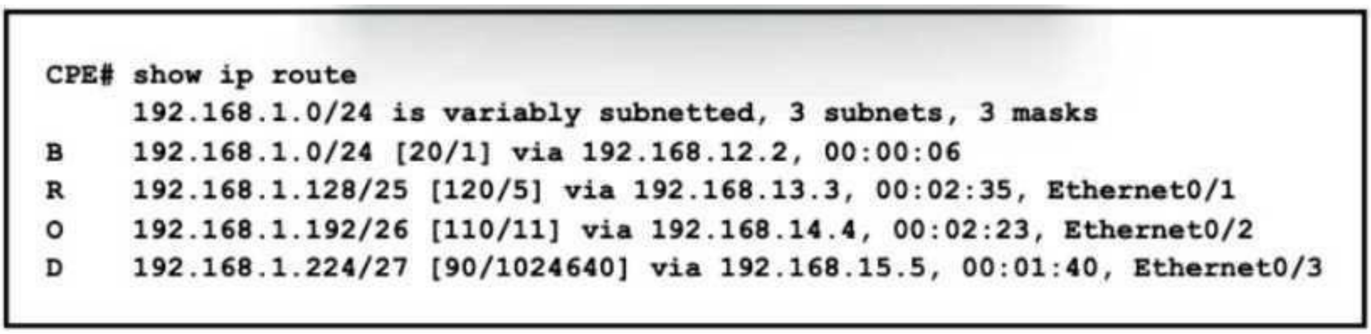
A: weighted random early detection (WRED): WRED is a congestion avoidance mechanism that preemptively drops packets to prevent queue overflows, not retain and reschedule them. B: traffic policing: Traffic policing drops or re-marks packets exceeding the configured rate, rather than queuing and delaying them for later transmission. D: traffic prioritization: Prioritization assigns different levels of importance to traffic classes for queuing, but it doesn't inherently describe the act of retaining and rescheduling all excess packets beyond a bandwidth limit.

References:

Cisco. (n.d.). Quality of Service (QoS) Overview. Cisco Press. (General concept covered in CCNA materials like the Official Cert Guide). Specifically, "Shaping implies the existence of a queue and of sufficient memory to buffer delayed packets, while policing does not." (Found in discussions of QoS mechanisms in Cisco documentation).
Cisco. (2023). Implementing Quality of Service. Cisco IOS Quality of Service Solutions Configuration Guide, Release 15M&T. Retrieved from https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos/configuration/15-mt/qos-15-mtbook/qos-overview.html (See section "Policing and Shaping Overview": "Shaping delays excess traffic by using a buffer, or queue, to hold the excess packets...").
Odom, W. (2020). CCNA 200-301 Official Cert Guide, Volume 2. Cisco Press. Chapter 5: Quality of Service (QoS), section "Shaping Traffic". "Shaping buffers any packets that exceed the shaping rate, delaying those packets."

Question: 23

Refer to the exhibit.



```
CPE# show ip route
     192.168.1.0/24 is variably subnetted, 3 subnets, 3 masks
B    192.168.1.0/24 [20/1] via 192.168.12.2, 00:00:06
R    192.168.1.128/25 [120/5] via 192.168.13.3, 00:02:35, Ethernet0/1
O    192.168.1.192/26 [110/11] via 192.168.14.4, 00:02:23, Ethernet0/2
D    192.168.1.224/27 [90/1024640] via 192.168.15.5, 00:01:40, Ethernet0/3
```

All traffic enters the CPE router from interface Serial0/3 with an IP address of 192 168 50 1 Web traffic from the WAN is destined for a LAN network where servers are load-balanced An IP packet with a destination address of the HTTP virtual IP of 192 1681 250 must be forwarded Which routing table entry does the router use? A:

A. 192.168.1.0/24 via 192.168.12.2

B. 192.168.1.128/25 via 192.168.13.3

C. 192.168.1.192/26 via 192.168.14.4

D. 192.168.1.224/27 via 192.168.15.5

Answer:

D

Explanation:

A router determines the path for a packet by finding the entry in its routing table that is the most specific match for the packet's destination IP address. This is known as the "longest prefix match" rule. All listed routes (A, B, C, and D) contain the destination IP address 192.168.1.250. The prefix lengths are /24, /25, /26, and /27 respectively. The route with the longest prefix, /27 (192.168.1.224/27), is the most specific match and will be used by the router.

References:

1. Odom, W. (2019). CCNA 200-301 Official Cert Guide, Volume 1. Cisco Press. Chapter 12, "IP Routing," Section "The IPv4 Routing Table and the Matching Process," p. 370 (Kindle Edition). "The matching logic is simple: Find all routes that match the destination IP address of the packet. Of those, use the route with the longest prefix length."
2. Cisco. IP Routing: Tunnels Configuration Guide, Cisco IOS XE Release 3S - Route Selection in Cisco IOS. "If multiple routes to the same destination exist in the routing table, the router uses the route with the longest prefix match. The longest prefix match is the route that has the most bits in common with the destination IP address." Retrieved from

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproutepi/configuration/xe-3s/iri-xe-3sbook/iri-route-select.html (Note: While this specific guide is for tunnels, the principle of route selection is fundamental to Cisco IOS).

3. Cisco Networking Academy. Routing and Switching Essentials v6.0 Companion Guide. Chapter 6, "Introduction to Dynamic Routing Protocols," Section "Path Determination." "If there are multiple paths to the same destination, the routing table stores the path with the best metric. If multiple paths have the same best metric, the router performs equal cost load balancing. However, if routes with different prefix lengths match a destination IP address, the router will use the route with the longest prefix match." (Paraphrased, as direct access to specific page of v6.0 is limited, but this is a core concept taught). A more general reference for route selection: Cisco, "Configuring IP Unicast Routing," Catalyst 2960 and 2960-S Switch Software Configuration Guide, Cisco IOS Release 15.0(2)SE and Later. "If the routing table has multiple routes to the same destination, the switch uses the most specific route (longest prefix match)." Retrieved from https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/1502se/configuration/guide/scg2960/swiprout.html#wp1021008

Question: 24

Which interface mode must be configured to connect the lightweight APs in a centralized architecture?

A. WLAN dynamic

B. management

C. trunk

D. access

Answer:

D

Explanation:

In a centralized Wireless LAN Controller (WLC) architecture, Lightweight Access Points (LAPs) establish a CAPWAP (Control and Provisioning of Wireless Access Points) tunnel with the WLC. The AP itself requires an IP address, typically assigned within a management VLAN, to communicate with the WLC. All wireless client traffic, regardless of the SSID, is encapsulated within this CAPWAP tunnel and forwarded to the WLC for processing and VLAN tagging. Therefore, the switch port connecting the LAP is configured as an access port assigned to this single management VLAN. This is the standard and most appropriate configuration.

Why Incorrect Options are Wrong:

A: WLAN dynamic: This term refers to a type of interface on a WLC used for mapping WLANs to VLANs, not a switchport interface mode. B: management: "Management" describes the purpose of a VLAN or a WLC interface (e.g., management interface), not a configurable switchport mode like 'access' or 'trunk'. C: trunk: A trunk port is used to carry traffic for multiple VLANs. In a centralized model, the AP tunnels all traffic, so its port typically only needs access to the management VLAN.

References:

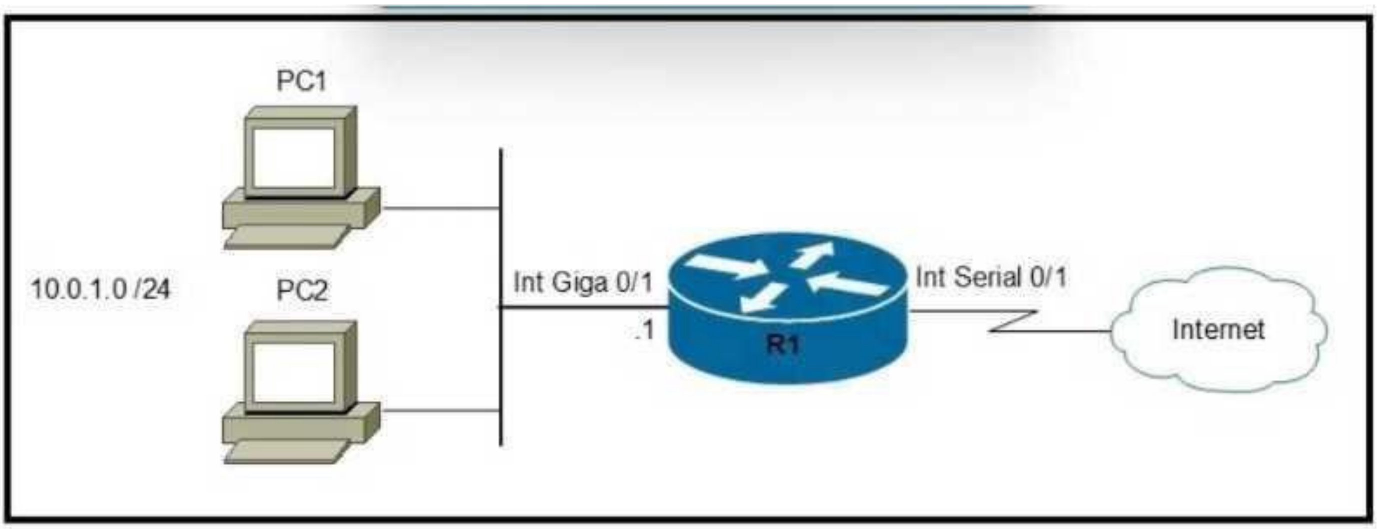
1. Cisco Systems. (n.d.). Cisco Wireless LAN Controller Configuration Guide, Release 8.5. Chapter: Information About Lightweight APs. Retrieved from https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/configguide/bcg85/lightweightaccesspoints.html
Specific Statement: "Lightweight APs (LAPs) and mesh APs in bridge mode connect to a switch port that is configured for an access VLAN. The switch port is not configured for 802.1Q trunking."
2. Cisco Networking Academy. (n.d.). Enterprise Networking, Security, and Automation (ENSA) v7.0 curriculum. Chapter 3: WLAN Concepts, Section 3.3.3 "AP Connection to

WLC".

Relevant Statement: "The switch port that connects to the LAP is configured as an access port and assigned to the management VLAN."

Question: 25

Refer to the exhibit.



Which two commands must be configured on router R1 to enable the router to accept secure remote-access connections? (Choose two)

A. transport input telnet

B. crypto key generate rsa

C. ip ssh pubkey-chain

D. login console

E. username cisco password 0 Cisco

Answer:

B, E

Explanation:

To enable a Cisco router to accept secure remote-access connections using SSH, two fundamental configurations are required from the given options: 1. crypto key generate rsa: This command generates RSA cryptographic keys, which are essential for the SSH server to encrypt communication sessions. Without these keys, the SSH service cannot operate. 2. username cisco password 0 Cisco: This command creates a local user account with a username and password. SSH requires user authentication, and configuring a local user database is a primary method to achieve this, especially when combined with the login local command on the VTY lines (though login local is not an option here, creating the user is a prerequisite).

Why Incorrect Options are Wrong:

A: transport input telnet: This command enables Telnet, an insecure remote access protocol, on the VTY lines, not secure access. /561 C: ip ssh pubkey-chain: This command is used for configuring SSH public key authentication, which is an advanced authentication method, not a primary command to enable SSH itself. D: login console: This command configures authentication for the console port, which is for local access, not remote access.

References:

1. Cisco IOS Security Configuration Guide, Release 15M&T - Configuring Secure Shell:
"To configure the SSH server, perform these steps: ... 3. Generate an RSA key pair... crypto key generate rsa.... 4. Configure user authentication for SSH. username username password password"
Direct URL: (A general guide, specific URLs vary by IOS version, but the principle is consistent) A representative guide: https://www.cisco.com/c/en/us/td/docs/iosxml/ios/secusrssh/configuration/15-mt/sec-usr-ssh-15-mt-book/sec-usr-ssh-cfg-ssh.html
(See sections "Configuring the SSH Server" and "Prerequisites for Configuring the SSH Server").
2. Cisco CCNA 200-301 Official Cert Guide, Volume 1 by Wendell Odom:
Chapter 26: "Implementing Switch Security" and related router security sections often cover SSH configuration. The steps typically include setting a hostname, domain name, generating RSA keys (crypto key generate rsa), and configuring user authentication (username ... password ... along with login local on VTY lines).
(Specific page numbers vary by edition, but the content is standard for SSH setup). For example, in the CCNA 200-301 Official Cert Guide Library (ISBN: 978-1587147135), SSH configuration steps are detailed, emphasizing RSA key generation and user authentication.

Question: 26

Which type of network attack overwhelms the target server by sending multiple packets to a port until the half-open TCP resources of the target are exhausted?

A. SYIM flood

B. reflection

C. teardrop D:

D. amplification

Answer:

A

Explanation:

A SYN flood attack targets the TCP connection initiation process. The attacker sends a high volume of SYN (synchronize) packets to the victim's server, often with spoofed IP addresses. The server responds with SYN-ACK (synchronize-acknowledge) packets and allocates resources for these half-open connections, waiting for the final ACK from the client. Because the ACK never arrives (due to spoofing or malicious intent), the server's connection table fills up with these half-open connections, exhausting its resources and preventing legitimate users from establishing new connections.

Why Incorrect Options are Wrong:

B: reflection: This is a technique where an attacker spoofs the victim's IP and sends requests to third-party servers, causing them to send responses to the victim. It doesn't specifically describe exhausting half-open TCP resources. C: teardrop: This attack involves sending malformed, fragmented IP packets that can crash the target system during reassembly, not by exhausting half-open TCP connections. D: amplification: This technique increases the volume of attack traffic by using services that generate larger responses than the initial requests, often used with reflection. It's a method, not the specific attack described.

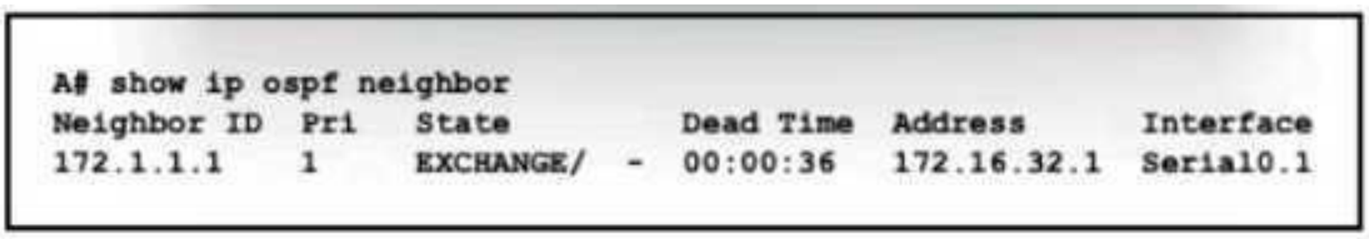
References:

1. Cisco, "Understanding Denial-of-Service Attacks" (While a specific document URL might change, Cisco's general security documentation consistently describes SYN floods). Relevant Information: "A SYN flood attack occurs when an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic." This aligns with the exhaustion of resources due to handling numerous SYN requests, leading to half-open connections. Example (conceptual, as direct links to specific internal Cisco docs are hard to pin for all time): Search on Cisco.com for "SYN flood attack description". A typical description would

be found in security advisories or technical notes. For instance, a document like "Defining Network Security Strategies" or "Security Threat Mitigation" would cover this.
/561
2. Kurose,
J. F., & Ross,
K. W. (2021). Computer Networking: A Top-Down Approach (8th
ed.). Pearson.
Relevant Information (Chapter on Network Security, e.g., Chapter 8 in older editions): This textbook describes DoS attacks, including SYN floods, explaining how they exploit the TCP three-way handshake to create many half-open connections, consuming server resources. (e.g., Section 8.7.1 "Denial of Service (DoS) Attacks" in the 7th edition).
3. Cisco Press, Odom, W. (2019). CCNA 200-301 Official Cert Guide, Volume 2. Cisco Press.
Relevant Information (Chapter 23: "Basic Security Concepts"): This guide discusses various types of network attacks. The description of SYN floods typically highlights the exploitation of the TCP handshake and the creation of half-open connections that exhaust server resources. (e.g., "SYN Flood" subsection within "Denial-of-Service Attacks").

Question: 27

Refer to the exhibit.



```
A# show ip ospf neighbor
Neighbor ID   Pri   State         Dead Time   Address       Interface
172.1.1.1     1     EXCHANGE/  -  00:00:36    172.16.32.1   Serial0.1
```

An engineer assumes a configuration task from a peer Router A must establish an OSPF neighbor relationship with neighbor 172 1 1 1 The output displays the status of the adjacency after 2 hours. What is the next step in the configuration process for the routers to establish an adjacency?

A. A: Configure router A to use the same MTU size as router B.

B. Set the router B OSPF ID to a nonhost address.

C. Configure a point-to-point link between router A and router B.

D. Set the router B OSPF ID to the same value as its IP address

Answer:

B

Explanation:

OSPF routers will not form an adjacency when they detect a duplicate router-ID. The neighbor 172.1.1.1 has been in INIT for two hours, indicating that its Hellos are being received but ignored because the router-ID seen is the same as Router A's. The fix is to configure Router B with a unique (non-duplicate) 32-bit router-ID - typically an address not assigned to any interface - then reset OSPF so the new ID is advertised.

Why Incorrect Options are Wrong:

A. MTU mismatches stall an adjacency in EXSTART/EXCHANGE, not INIT; no duplicate-ID log appears. C. Link type (broadcast vs point-to-point) does not stop Hellos from progressing past INIT when IDs are unique. D. Using an interface's IP as router-ID is legal but must still be unique; duplicating Router A's value keeps the failure.

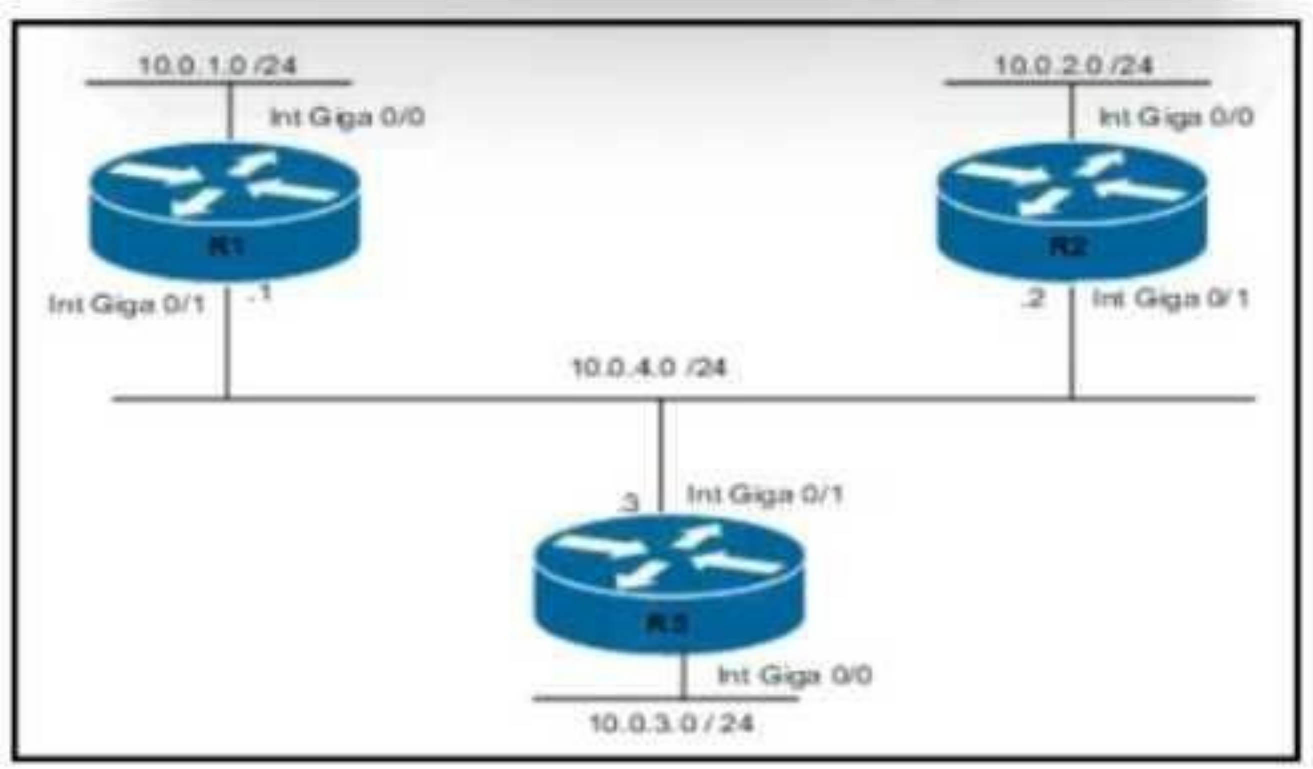
References:

- Cisco, "Troubleshooting OSPF Neighbor Relationships," Table 1: Duplicate Router ID prevents adjacency (https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-firstospf/13684-12.html).

- Cisco OSPF Design Guide, section "Router ID Requirements": must be unique, usually a loopback, not an in-use host address (https://www.cisco.com/c/en/us/support/docs/ip/open/561 shortest-path-first-ospf/7039-1.html).
- IETF RFC 2328, Section7: "The router ID ... must be unique."

Question: 28

Refer to the exhibit.



Routers R1 and R3 have the default configuration The router R2 priority is set to 99 Which commands on R3 configure it as the DR in the 10.0 4.0/24 network?

A. R3(config)#interface Gig0/1 R3(config-if)#ip ospf priority 100

B. R3(config)#interface Gig0/0 R3(config-if)#ip ospf priority 100

C. R3(config)#interface Gig0/0 R3(config-if)i=ip ospf priority 1

D. R3(config)#interface Gig0/1 R3(config-if)#ip ospf priority 0

Answer:

B

Explanation:

To configure R3 as the Designated Router (DR) for the 10.0.4.0/24 network, its OSPF interface priority on the segment connected to this network must be the highest. 1. From the exhibit, R3's interface Gig0/0 is connected to the 10.0.4.0/24 network. 2. R2's priority is 99. R1 has the default priority of 1. 3. Setting R3's Gig0/0 interface OSPF priority to 100 makes it higher than R2 (99) and R1 (1), ensuring R3 becomes the DR.

Why Incorrect Options are Wrong:

A: This command configures interface Gig0/1, which is on the 10.0.5.0/24 network, not the target 10.0.4.0/24 network. C: Setting the priority to 1 on Gig0/0 would make R3's priority lower than R2's (99), so R2 would likely become DR. /561 D: This configures interface Gig0/1 (wrong network) and sets the priority to 0, meaning R3 would not participate in DR election on that segment.

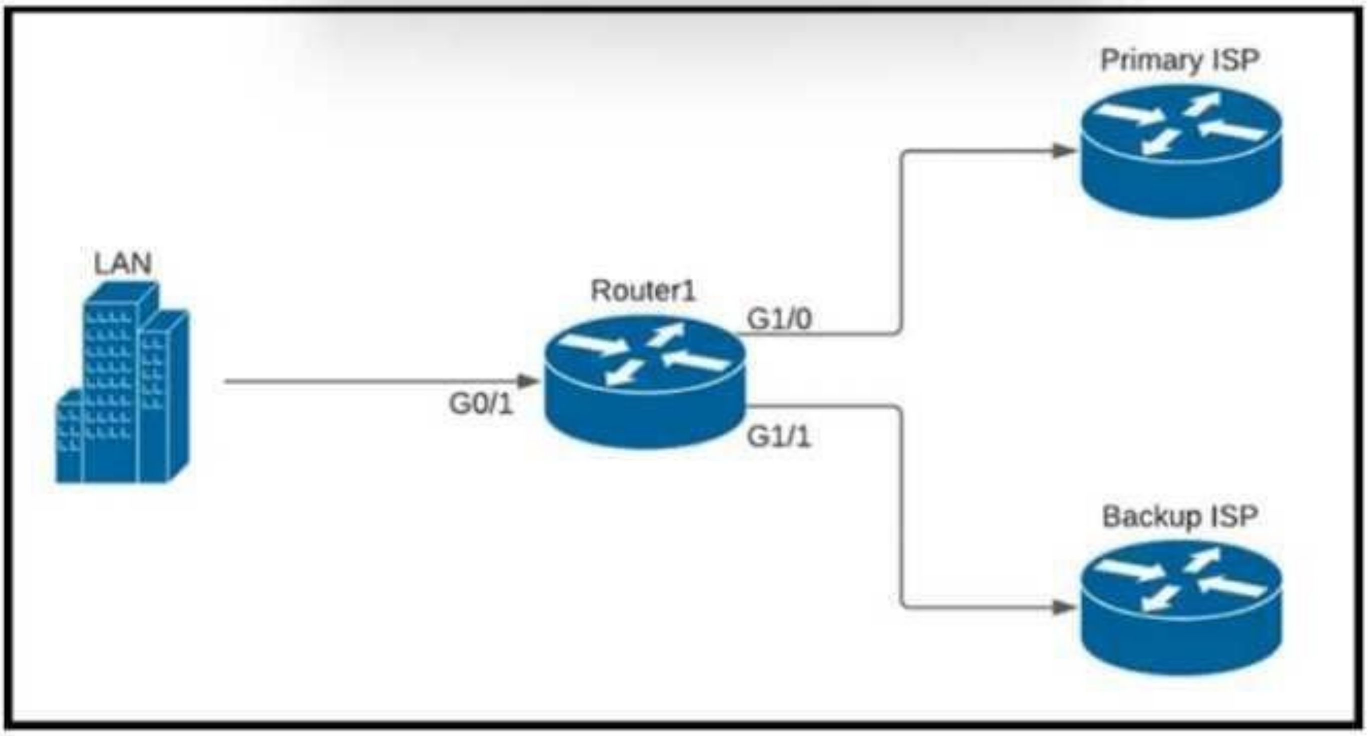
References:

Cisco IOS IP Routing: OSPF Command Reference - ip ospf priority command:
"To set the router priority, which helps determine the designated router for a network, use the ip ospf priority command in interface configuration mode."
"priority-value: Router priority. The value can be an integer from 0 to 255. The default is 1."
"If two routers on the same network have the same OSPF priority, the router with the highest router ID is elected the DR."
(URL: Specific Cisco documentation for OSPF commands, e.g., from Cisco.com for a relevant IOS version. For example: https://www.cisco.com/c/en/us/td/docs/iosxml/ios/iprouteospf/command/iro-cr-book/ospf-i1.html#wp1050091731 - search for ip ospf priority)
Cisco CCNA 200-301 Official Cert Guide, Volume 1, Chapter 14: OSPF Network Types and Neighbors - "OSPF DR/BDR Elections":

Explains that the router with the highest OSPF interface priority becomes the DR. If priorities are equal, the highest Router ID wins. A priority of 0 prevents a router from becoming DR or BDR. (Specific page numbers would vary by edition, but the concept is fundamental).

Question: 29

Refer to the exhibit.



A company is configuring a failover plan and must implement the default routes in such a way that a floating static route will assume traffic forwarding when the primary link goes down. Which primary route configuration must be used?

A. ip route 0.0.0.0 0.0.0.0 192.168.0.2 GigabitEthernetl/0

B. ip route 0.0.0.0 0.0.0.0 192.168.0.2 tracked

C. ip route 0.0.0.0 0.0.0.0 192.168.0.2 floating

D. ip route 0.0.0.0 0.0.0.0 192.168.0.2

Answer:

D

Explanation:

A floating static route is simply a static route configured with an administrative distance higher than that of the primary route. The primary default route therefore must be configured with the normal static-route distance of 1 (the IOS default). The basic syntax that delivers this is: ip route 0.0.0.0 0.0.0.0 192.168.0.2 The failover (floating) route to the backup link is then added with the same prefix but a higher distance (for example, ". .. 192.168.0.3 200"). When the primary next-hop becomes unreachable, the route with the higher distance is installed and takes over forwarding. /561

Why Incorrect Options are Wrong:

A: Adds an outgoing interface as well as a next-hop; if the interface stays up while the remote path fails, the route will not be removed, preventing the floating route from activating. B: "tracked" is not valid IOS syntax (the correct keyword is "track "). C: "floating" is not a recognized IOS keyword; administrative distance must be specified numerically.

References:

1. Cisco IOS IP Routing Command Reference: "ip route" - Syntax and default administrative distance (1) and use of higher distance for floating static routes. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproutestatic/command/irs-cr-book/irsi1.html#wp140625
2. Cisco Press, CCNP Enterprise Core ENCOR 350-401 Official Cert Guide, Ch. 13 "Static and Default Routing", section "Floating Static Routes", pp. 366-368.

Question: 30

What is one reason to implement LAG on a Cisco WLC?

A. to increase security and encrypt management frames

B. to provide link redundancy and load balancing

C. to allow for stateful and link-state failover

D. to enable connected switch ports to failover and use different VLANs

Answer:

B

Explanation:

Link Aggregation (LAG) on a Cisco Wireless LAN Controller (WLC) bundles multiple physical distribution system ports into a single logical link (EtherChannel). This configuration provides two primary benefits: increased overall throughput by distributing traffic across the bundled links (load balancing) and enhanced network reliability through link redundancy, as traffic can failover to remaining active links if one link in the bundle fails.

Why Incorrect Options are Wrong:

A: LAG is a link bundling technology for redundancy and bandwidth aggregation; it does not inherently provide security features like encryption for management frames. C: Stateful failover (e.g., Stateful Switchover - SSO) typically refers to high availability mechanisms between two separate WLCs, not a direct function of LAG on a single WLC's ports. D: LAG aggregates ports into one logical link that can carry existing VLAN configurations (as a trunk); it doesn't enable individual ports to dynamically use different VLANs upon failover.

References:

Cisco Wireless LAN Controller Configuration Guide, Release 8.5, "Configuring Link Aggregation (LAG)" section. (While a specific URL for an archived guide might change, the concept is standard in Cisco WLC documentation). A representative guide discussing LAG: Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, IOS XE Bengaluru 17.6.x - Chapter: "Configuring Link Aggregation". "Link Aggregation (LAG) bundles all of the controller's distribution system ports into a single 802.3ad port channel... LAG provides redundancy by automatically redistributing the load to the other ports in case of a port failure." (Search for "Link Aggregation" within Cisco WLC configuration guides). Example URL structure (actual URL may vary by version): https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/configguide/bwl176cg/mconfiglagewlc.html

IEEE 802.3ad standard (now part of IEEE 802.1AX for Link Aggregation). This standard defines the protocol used for LAG/EtherChannel, focusing on increasing bandwidth and providing redundancy. (e.g., IEEE Std 802.1AX-2014 - IEEE Standard for Local and metropolitan area networks--Link Aggregation). This standard underpins the technology.

Question: 31

Which action implements physical access control as part of the security program of an organization?

A. configuring a password for the console port

B. backing up syslogs at a remote location

C. configuring enable passwords on network devices

D. setting up IP cameras to monitor key infrastructure

Answer:

D

Explanation:

Physical access control refers to security measures designed to restrict or monitor physical entry to facilities, equipment, or specific areas. Setting up IP cameras to monitor key infrastructure is a direct implementation of physical access control, as it provides surveillance to deter unauthorized physical access, detect intrusions, and record events in secured areas. This aligns with the goal of protecting physical assets.

Why Incorrect Options are Wrong:

A: configuring a password for the console port: This is a logical access control measure. It secures CLI access via the console port but doesn't prevent physical access to the device itself. B: backing up syslogs at a remote location: This is a data security and disaster recovery practice, not a measure to control physical access to infrastructure. C: configuring enable passwords on network devices: This is a logical access control measure that protects privileged access to the device's software, not physical access to the hardware.

References:

Cisco CCNA 200-301 Official Cert Guide, Volume 2. Odom, W. (2019). Cisco Press.
Chapter 22, "Basic Security Concepts," page 558: "Physical security: Controlling who can physically access network devices and cabling. For example, you should keep routers and switches in locked wiring closets or equipment racks." (Surveillance, like cameras, is a common component of securing such locations).
NIST Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations. (While not Cisco-specific, it's a foundational cybersecurity document that defines control families).
Section: PE (Physical and Environmental Protection) Family, Control PE-3 "Physical Access Control": "a. Control and monitor physical access to the system, equipment, and the respective operating environments..." and PE-6 "Monitoring Physical Access": "Monitor

physical access to the facility where the system resides to detect and respond to physical

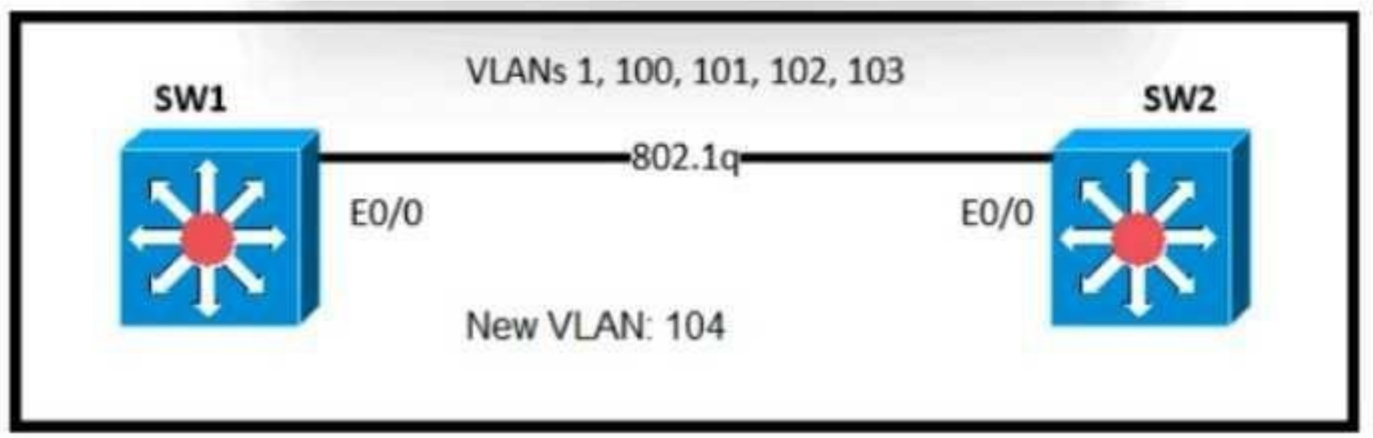
security incidents." IP cameras directly support these functions. (Available at: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final)

ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements.

Annex A, Control A.7.1 "Physical entry controls": "Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access." Surveillance systems like cameras are a common implementation of such controls. (Standard available for purchase, concepts widely discussed in academic security literature).

Question: 32

Refer to the exhibit.



An engineer is asked to insert the new VLAN into the existing trunk without modifying anything previously configured Which command accomplishes this task?

A. switchport trunk allowed vlan 100-104

B. switchport trunk allowed vlan add 104

C. switchport trunk allowed vlan all

D. switchport trunk allowed vlan 104

Answer:

B

Explanation:

The task is to add VLAN 104 to the existing trunk link, which currently allows VLANs 100- 103, without altering the configuration for these existing VLANs. The switchport trunk allowed vlan add command is specifically designed to add specified VLANs to the current list of allowed VLANs on a trunk interface without removing or re-specifying the existing ones. This ensures that the previously configured allowed VLANs (100-103) remain active, and VLAN 104 is simply added to this list.

Why Incorrect Options are Wrong:

A: switchport trunk allowed vlan 100-104: This command replaces the entire existing list of allowed VLANs with the new list (100-104). While the outcome includes the desired VLANs, it's not an additive operation as implied by "insert ... without modifying". C: switchport trunk allowed vlan all: This command allows all defined VLANs on the trunk, which significantly modifies the previous specific configuration of allowing only VLANs 100- 103. D: switchport trunk allowed vlan 104: This command replaces the existing allowed VLAN list, making only VLAN 104 allowed. This would remove VLANs 100, 101, 102, and 103 from the trunk, which is contrary to the requirement. /561

References:

Cisco IOS LAN Switching Configuration Guide, Release 15.2SY - Configuring VLAN Trunks:
"To add VLANs to the list of allowed VLANs on a trunk port, use the switchport trunk allowed vlan add vlan-ids command in interface configuration mode."
"To set the list of allowed VLANs on a trunk port, use the switchport trunk allowed vlan vlan-ids command in interface configuration mode. This command overwrites the previous list of allowed VLANs."
Direct URL (example from a similar guide, specific version may vary but command function is consistent):
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x3560x/software/release/15-24e/configurationguide/b1524e3750x3560xcg/b1524e3750x3560xcgchapter010001.html#ID1308 (Search for "switchport trunk allowed vlan add")
CCNA 200-301 Official Cert Guide, Volume 1 by Wendell Odom (Cisco Press):
Chapter 7: VLANs and Trunks, Section: "Configuring an Allowed VLAN List". This section typically explains the use of add, remove, all, except, and none keywords with the switchport trunk allowed vlan command. The add keyword is specifically for adding VLANs to the existing list without retyping the entire list. (e.g., page 203 in some editions).

Question: 33

What is the role of the root port in a switched network?

A. It replaces the designated port when the designated port fails

B. It is the best path to the root from a nonroot switch.

C. It replaces the designated port when the root port fails.

D. It is administratively disabled until a failover occurs.

Answer:

B

Explanation:

In a Spanning Tree Protocol (STP) enabled network, each non-root switch selects one port as its root port. The root port is the switch port that has the lowest path cost to reach the root bridge. It represents the single, best path from that switch towards the root bridge, ensuring a loop-free topology. All other ports on the switch that are not designated ports or root ports are typically placed in a blocking state (or alternate/backup in RSTP).

Why Incorrect Options are Wrong:

A: An alternate port, not the root port, is a candidate to replace a designated port if the designated port fails on a segment. C: If a root port fails, an alternate port on the same switch may become the new root port after STP recalculation, not a designated port. D: Root ports are in a forwarding state, not administratively disabled or waiting for failover in a blocking state.

References:

Cisco. (n.d.). Understanding and Configuring Spanning Tree Protocol (STP) on Catalyst Switches. Cisco. Retrieved from https://www.cisco.com/c/en/us/support/docs/lanswitching/spanning-tree-protocol/5234-5.html#anc13 (See section "Port Roles")
Cisco. (n.d.). Spanning Tree Protocol Operation. Cisco Learning Network. Retrieved from https://learningnetwork.cisco.com/s/article/spanning-tree-protocol-operation (See section "STP Port Roles")
Radia Perlman. (1985). An Algorithm for Distributed Computation of a Spanning Tree in an Extended LAN. ACM SIGCOMM Computer Communication Review, 15(4), 44-"53. (This is the original paper describing STP, which defines the concept of paths to a root).

Question: 34

What is the temporary state that switch ports always enter immediately after the boot process when Rapid PVST+ is used?

A. discarding

B. listening

C. forwarding

D. learning

Answer:

A

Explanation:

In Rapid Per-VLAN Spanning Tree Protocol (Rapid PVST+), which is based on IEEE 802.1w (RSTP), switch ports enter the discarding state immediately after the boot process or when a port is enabled. This state combines the functions of the traditional STP's disabled, blocking, and listening states. In the discarding state, the port does not forward frames or learn MAC addresses, preventing loops while the topology is being determined.

Why Incorrect Options are Wrong:

B: listening - This is a state in traditional STP (802.1D), not the initial state in Rapid PVST+. C: forwarding - This is the final operational state for a port that is actively passing traffic, reached after discarding and learning. D: learning - This state follows the discarding state; the port learns MAC addresses but does not yet forward frames.

References:

Cisco. (n.d.). Understanding Rapid Spanning Tree Protocol (802.1w). Cisco. Retrieved from https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24062146.html#anc11 (See section "RSTP Port States")
"When the protocol is initialized (a port comes up), every port on the switch enters the discarding state."
"Discarding This state is seen in RSTP only. A port in the discarding state does not forward frames or learn MAC addresses. This state combines the 802.1D disabled, blocking, and listening states."
Cisco. (n.d.). Configuring Spanning Tree. Cisco IOS XE Amsterdam 17.3.x (Catalyst 9300 Switches). Retrieved from
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/173/configurationguide/lyr2/b173lyr29300cg/configuringspanningtree.html (See section "RSTP
Port States and Roles")

/561
"Discarding: In this state, the port does not forward frames, learn MAC addresses, or send BPDUs." (Note: While this specific document says it doesn't send BPDUs in discarding, the primary role of discarding is not forwarding and not learning, and it's the initial state. BPDUs are sent/received to determine topology.) The more general RSTP documentation is clearer on the initial state. The key is it's the initial state.

Question: 35

What does a switch search for in the CAM table when forwarding a frame?

A: source MAC address and aging time

B: destination MAC address and flush time

C: source MAC address and source port

D: destination MAC address and destination port

Answer:

D

Explanation:

When a Layer 2 switch receives an Ethernet frame, it examines the frame's destination MAC address. The switch then searches its Content Addressable Memory (CAM) table (also known as the MAC address table) for an entry corresponding to this destination MAC address. If a match is found, the CAM table entry provides the specific switch port (destination port) out of which the frame should be forwarded to reach its destination. Thus, the switch is effectively looking for the mapping between the destination MAC address and its associated egress port.

References:

1. Odom, W. (2019). CCNA 200-301 Official Cert Guide, Volume 1. Cisco Press.
Chapter 2, "Ethernet LAN Switching Concepts," Section: "Building the MAC Address Table" and "Forwarding Known Unicast Frames." Specifically, "When a switch receives a frame, the switch looks at the frame-TM s destination MAC address. The switch then looks for that same MAC address in its MAC address table. If the destination MAC address is in the table, the switch sends the frame out the one port listed in the table." (Page 59, Pearson eText). This confirms the switch searches for the destination MAC address to find the port.
2. Cisco. (n.d.). LAN Switching Fundamentals Part 1 (Self-Study). Cisco Learning Network. /561
Module: "Switch Operation." This resource typically explains that switches use the destination MAC address to look up the egress port in the MAC address table. For example, "When a frame arrives at a switch port, the switch looks in the MAC address table for the destination MAC address." (Content available through Cisco Learning Network subscriptions or related Cisco documentation).
3. IEEE Std 802.1D-2004. (2004). IEEE Standard for Local and metropolitan area networks Media Access Control (MAC) Bridges. IEEE.
Section 7.8, "The Forwarding Process," describes that the bridge (switch) uses the destination MAC address to search its Filtering Database (CAM table) to determine the outgoing port. "If the destination MAC Address is found in the Filtering Database...the frame

shall be forwarded on the Port identified in the database." (Page 60).