# Practice Test 3

1. In which scenario would you most likely use the IEEE 802.1Q standard in a network setup?
   1. To optimize the routing information exchanged between routers using an advanced algorithm.
   2. To establish a secure VPN tunnel across an enterprise network.
   3. **To enable multiple VLANs to communicate over a single trunk connection. (X)**
   4. To manage and allocate IP addresses dynamically across multiple subnets in a network.

Correct answer: C

Explanation: IEEE 802.1Q is a networking standard that supports VLAN tagging, allowing multiple VLANs to share the same physical link by tagging Ethernet frames with a VLAN identifier. This enables network segmentation and better utilization of network resources over a trunk link.

1. Which security feature is primarily designed to protect the control plane of a network device?
   1. Intrusion Prevention System (IPS)
   2. **Control Plane Policing (CoPP)**
   3. Access Control List (ACL)
   4. Port Security

Correct answer: B

Control Plane Policing (CoPP) is a security feature designed to mitigate the effects of traffic destined to the control plane of network devices such as routers and switches. It allows admins to rate-limit and filter control plane traffic to protect the device from excessive CPU usage or potential DoS attacks.

1. In an enterprise network with multiple switches and VLANs, if a trunk link between two switches is configured with a native VLAN and the native VLAN is different on each switch, what will be the most likely outcome?
   1. **Frames belonging to the native VLAN from each switch will not be tagged, potentially causing VLAN hopping or traffic loss.**
   2. An error message will be logged, but the network traffic will continue to flow correctly.
   3. The trunk link will automatically negotiate the correct native VLAN using the DTP (Dynamic Trunking Protocol).
   4. STP (Spanning Tree Protocol) will block the trunk port to prevent the VLAN mismatch.

Correct answer: A

Explanation: When configuring trunk links between switches, the native VLAN must match on both ends to avoid issues like VLAN mismatch. If the native VLANs are different on each switch, frames from the native VLAN that are not tagged can be misdirected, causing potential traffic loss or creating opportunities for VLAN hopping attacks.

1. Which subnet mask would you use to configure a network with 1,022 usable IP addresses?
   1. 255.255.248.0
   2. **255.255.252.0**
   3. 255.255.240.0
   4. 255.255.254.0

Correct answer: B

Explanation: The subnet mask of 255.255.252.0 (/22) is the best fit for a network needing 1,022 usable IP addresses, as it provides just the right number of IPs without excessive surplus.

1. You need to configure a router to prioritize VoIP traffic over regular data traffic. Which of the following configurations is most appropriate to achieve this using QoS on a Cisco router?
   1. class-map match-any VOIP; match protocol RTP
   2. ip route 0.0.0.0 0.0.0.0 192.168.1.1
   3. access-list 101 permit ip any any
   4. **policy-map VOIP-PRIORITY; class VOIP; priority 1000**

Correct answer: D

Explanation: To prioritize VoIP traffic using Quality of Service (QoS) on a Cisco router, specific configurations involving class-maps and policy-maps are necessary. Class-maps allow you to define and match types of traffic, and policy-maps enable prioritization  in this case, setting higher priority to VoIP traffic.

1. Which of the following methods would reduce the broadcast domain size in a large Layer 2 switched network?
   1. Port Security
   2. Spanning Tree Protocol
   3. Subnetting
   4. **VLANs**

Correct answer: D

Explanation: the Correct answer is VLANs. VLANs allow network administrators to segment a Layer 2 network into multiple, smaller, and isolated broadcast domains. This is achieved by assigning different VLAN IDs to different groups of ports on a switch, effectively reducing the scope of broadcast traffic and improving overall network performance.

1. Which of the following options correctly describes the function of a router on a network?
   1. **Routers determine the best path to forward packets based on the destination IP address.**
   2. Routers segment a network into different collision domains.
   3. Routers operate at the Data Link layer and mainly handle MAC addresses.
   4. Routers convert IP addresses to MAC addresses using ARP.

Correct answer: A

Explanation: Routers are critical devices in networking that operate at the Network layer of the OSI model. They manage traffic between different networks by analyzing data packets and determining the optimal path based on destination IP addresses. This functionality is key to efficient and effective data transmission across large and small networks alike.

1. A network administrator needs to enhance the router security by implementing SSH (Secure Shell) for remote access. Which series of commands should be correctly used to achieve this while ensuring the highest security level?
   1. **router(config)# hostname R1 router(config)# ip domain-name example.com router(config)# crypto key generate rsa modulus 1024 router(config)# line vty 0 4 router(config-line)# transport input ssh router(config-line)# login local**
   2. router(config)# interface g0/0 router(config-if)# ip address 192.168.1.1 255.255.255.0 router(config-if)# no shutdown router(config)# ip domain-name example.com router(config)# line console 0 router(config-line)# transport input ssh router(config-line)# login local
   3. router(config)# hostname R1 router(config)# interface g0/0 router(config-if)# ip address 192.168.1.1 255.255.255.0 router(config-if)# exit router(config)# line vty 0 4 router(config-line)# login local
   4. router(config)# ip domain-name example.com router(config)# crypto key generate rsa modulus 2048 router(config)# username admin password Cisc0123 router(config)# line vty 0 4 router(config-line)# transport input telnet ssh router(config-line)# login local

Correct answer: A

Explanation: Option 1 provides the correct and secure method to enable SSH: setting the hostname, domain name, generating RSA keys, configuring VTY lines to accept only SSH connections, and requiring local login. This ensures encrypted communication and restricts access to authenticated users only.

1. In a network environment where both 802.1X and MAB (MAC Authentication Bypass) are implemented, how can a network administrator ensure that the devices that do not support 802.1X are still granted network access?
   1. By using port-based VLAN assignment to segregate devices and apply appropriate access policies
   2. By configuring a fallback mechanism to allow non-802.1X devices in periodically
   3. **By configuring the switch ports to use both 802.1X and MAB, with MAB acting as a fallback method**
   4. By disabling 802.1X on ports where non-802.1X devices are connected

Correct answer: C

Explanation: When both 802.1X and MAB are implemented, configuring the switch ports to use both protocols is the recommended approach. This allows MAB to act as a fallback authentication method for devices that do not support 802.1X, ensuring that these devices can still access the network without compromising security.

1. You have been asked to configure a new VLAN on a Cisco switch. What command would you use to assign an interface to VLAN 10 and set it to be an access port?
   1. switchport access vlan 10
   2. **switchport mode access and switchport access vlan 10**
   3. switchport mode trunk
   4. vlan database vlan 10

Correct answer: B

Explanation: To correctly assign an interface to a VLAN and set it to access mode, you must use the commands ‘switchport mode access‘ and ‘switchport access vlan 10‘. This sequence ensures that the interface is configured to carry traffic for a single VLAN and is assigned to the specified VLAN.