

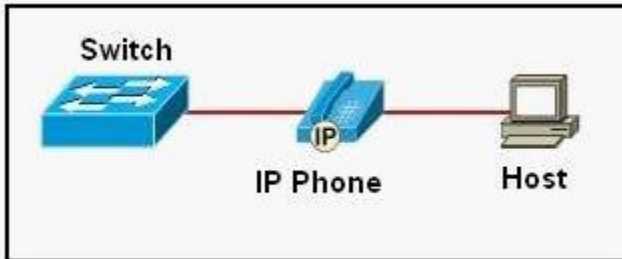


Exam : **642-812**

Title : Building Cisco Multilayer
Switched Networks

Version : Demo

1. Refer to the exhibit. What is the effect on the trust boundary of configuring the command `mls qos trust cos` on the switch port that is connected to the IP phone?



- A. Effectively the trust boundary has been moved to the IP phone.
- B. The host is now establishing the CoS value and has effectively become the trust boundary.
- C. The switch is rewriting packets it receives from the IP phone and determining the CoS value.
- D. The switch will no longer tag incoming voice packets and will trust the distribution layer switch to set the CoS.
- E. RTP will be used to negotiate a CoS value based upon bandwidth utilization on the link.

Answer: A

2. Refer to the exhibit. What is the effect when the switchport priority extend cos 3 command is configured on the switch port interface connected to the IP phone?



- A. Effectively, the trust boundary has been moved to the PC attached to the IP phone.
- B. The computer is now establishing the CoS value and has effectively become the trust boundary.
- C. The IP phone is enabled to override with a CoS value of 3 the existing CoS marking of the PC attached to the IP phone.
- D. The switch will no longer tag incoming voice packets and will extend the trust boundary to the distribution layer switch.
- E. RTP will be used to negotiate a CoS value based upon bandwidth utilization on the link.

Answer: C

3. Which three WLAN statements are true? (Choose three.)

- A. A lightweight AP receives control and configuration from a WLAN controller to which it is associated.
- B. A WLAN client that is operating in half-duplex mode will delay all clients in that WLAN.
- C. Ad hoc mode allows mobile clients to connect directly without an intermediate AP.
- D. Another term for infrastructure mode is independent service set (IBSS).
- E. The Aironet 1230 access point is an example of an access point that operates solely as a lightweight access point.
- F. WLANs are designed to share the medium and can easily handle an increased demand of channel contention.

Answer: ABC

4. Which statement is true about IP telephony calls?

- A. A Voice over IP (VoIP) packet consists of the voice payload, IP header, TCP header, RTP header, and Layer 2 link header.
- B. The voice carrier stream uses H.323 to set up, maintain, and tear down call endpoints.
- C. Call control signaling uses Real-Time Transport Protocol (RTP) packets that contain actual voice samples.
- D. The sum of bandwidth necessary for each major application, including voice, video, and data, should not exceed 75 percent of the total available bandwidth for each link.

Answer: D

5. Which three statements are true about the voice VLAN feature on a Catalyst 2950 switch? (Choose three.)

- A. The CoS value is trusted for 802.1p or 802.1q tagged traffic.
- B. The voice VLAN feature is disabled by default.
- C. The IP phone accepts the priority of all tagged and untagged traffic and sets the CoS value to 4.
- D. When the voice VLAN feature is enabled, all untagged traffic is sent according to the default CoS priority of the port.
- E. PortFast is automatically disabled when a voice VLAN is configured.
- F. The default CoS value for incoming traffic is set to 0.

Answer: BDF

6. In what three ways is QoS applied in the campus network? (Choose three.)

A. No traffic marking occurs at the core layer. Layer 2/3 QoS tags are trusted from distribution layer switches and used to prioritize and queue the traffic as it traverses the core.

B. IP precedence, DSCP, QoS group, IP address, and ingress interface are Layer 2 characteristics that are set by the access layer as it passes traffic to the distribution layer. The distribution layer, once it has made a switching decision to the core layer, strips these off.

C. MAC address, Multiprotocol Label Switching (MPLS), the ATM cell loss priority (CLP) bit, the Frame Relay discard eligible (DE) bit, and ingress interface are established by the voice submodule (distribution layer) as traffic passes to the core layer.

D. The distribution layer inspects a frame to see if it has exceeded a predefined rate of traffic within a certain time frame, which is typically a fixed number internal to the switch. If a frame is determined to be in excess of the predefined rate limit, the CoS value can be marked up in a way that results in the packet being dropped.

E. The access layer is the initial point at which traffic enters the network. Traffic is marked (or remarked) at Layers 2 and 3 by the access switch as it enters the network, or is "trusted" that it is entering the network with the appropriate tag.

F. Traffic inbound from the access layer to the distribution layer can be trusted or reset depending upon the ability of the access layer switches. Priority access into the core is provided based on Layer 3 QoS tags.

Answer: AEF

7. Which two Aironet enterprise solution statements are true? (Choose two.)

A. A Cisco Aironet AP handles the transmission of beacon frames and also handles responses to probe-request frames from clients.

B. A Cisco Aironet solution includes intelligent Cisco Aironet access points (APs) and Cisco Catalyst switches.

C. In the Cisco Aironet solution, each AP is locally configured by the use of either a web interface or the command line interface.

D. The Cisco Aironet AP handles real-time portions of the LWAPP protocol, and the WLAN controller handles those items which are not time sensitive.

E. Virtual MAC architecture allows the splitting of the 802.11 protocol between the Cisco Aironet AP and a LAN switch.

Answer: AD

8. Which statement about the Lightweight Access Point Protocol (LWAPP) is true?

A. LWAPP encrypts control traffic between the AP and the controller.

B. LWAPP encrypts user traffic with a x.509 certificate using AES-CCMP.

C. LWAPP encrypts both control traffic and user data.

D. When set to Layer 3, LWAPP uses a proprietary protocol to communicate with the Cisco Aironet APs.

Answer: A

9. Which issue or set of issues does the Lightweight Access Point Protocol (LWAPP) address?

A. reduction of processing in wireless controllers

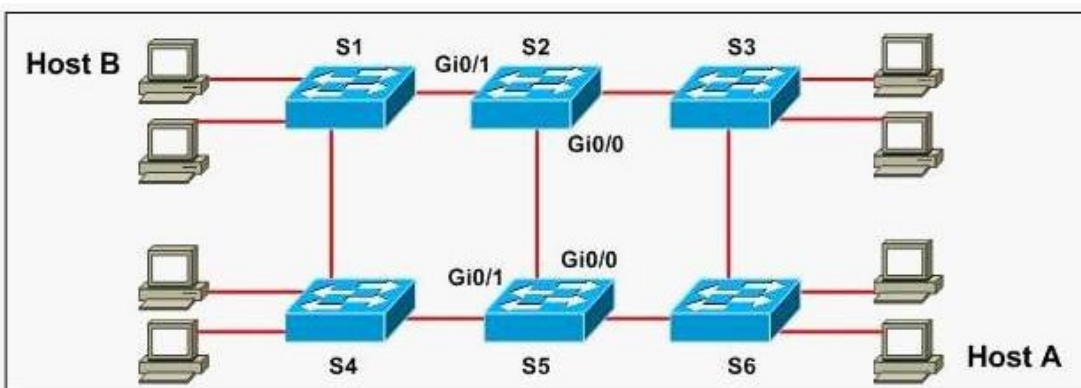
B. distributed approach to authentication, encryption, and policy enforcement

C. provides security by blocking communication between access points and wireless clients

D. access point discovery, information exchange, and configuration

Answer: D

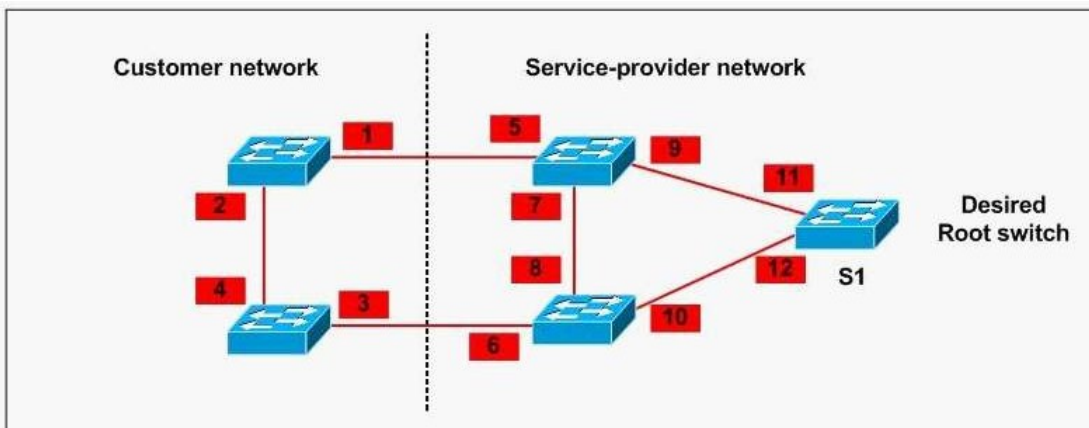
10. Refer to the exhibit. The command spanning-tree guard root is configured on interface Gi0/0 on both switch S2 and S5. The global configuration command spanning-tree uplinkfast has been configured on both switch S2 and S5. The link between switch S4 and S5 fails. Will Host A be able to reach Host B?



- A. Yes. Traffic can pass either from switch S6 to S3 to S2 to S1, or, from switch S6 to S5 to S2 to S1.
- B. No. Traffic will pass from switch S6 to S5 and dead-end at interface Gi 0/0.
- C. No. Traffic will loop back and forth between switch S5 and S2.
- D. Yes. Traffic will pass from switch S6 to S3 to S2 to S1.
- E. No. Traffic will either pass from switch S6 to S5 and dead-end, or traffic will pass from switch S6 to S3 to S2 and dead-end.

Answer: D

11. Refer to the exhibit. The service provider wants to ensure that switch S1 is the root switch for its own network. On which interfaces should root guard be configured to ensure that this happens?



- A. interfaces 1 and 2
- B. interfaces 1, 2, 3, and 4
- C. interfaces 1, 3, 5, and 6
- D. interfaces 5 and 6
- E. interfaces 5, 6, 7, and 8
- F. interfaces 11 and 12

Answer: D

12. Which two statements about the Cisco Aironet Desktop Utility (ADU) are true? (Choose two.)

- A. The Aironet Desktop Utility (ADU) can be used to establish the association between the client adapter and the access point, manage authentication to the wireless network, and enable data encryption.
- B. The Aironet Desktop Utility (ADU) and the Microsoft Wireless Configuration Manager can be used at

the same time to configure the wireless client adapter.

C. The Aironet Desktop Utility (ADU) can support only one wireless client adapter installed and used at a time.

D. The Aironet Desktop Utility (ADU) profile manager feature can create and manage only one profile for the wireless client adapter.

E. When the user selects a different profile in the Aironet Desktop Utility (ADU), the settings for the wireless client adapter are changed only after a reboot.

Answer: AC

13. Refer to the exhibit. A Cisco Aironet Wireless LAN Client Adapter has been installed and configured through the ADU on the PC. The Aironet System Tray Utility (ASTU) has been enabled during the installation and the icon appears in the system tray area in the lower right of the desktop. What is the significance of the icon?



A. It indicates that the radio of the client adapter is disabled.

B. It indicates that the client adapter is not associated to an access point or another client.

C. It indicates that the client adapter is associated to an access point or another client, but the user is not EAP authenticated.

D. It indicates that the client adapter is associated to an access point or another client, that the user is authenticated if the client adapter is configured for EAP authentication, and that the signal strength is excellent or good.

E. It indicates that the client adapter is associated to an access point or another client, that the user is authenticated if the client adapter is configured for EAP authentication, and that the signal strength is fair.

F. It indicates that the client adapter is associated to an access point or another client, that the user is authenticated if the client adapter is configured for EAP authentication, and that the signal strength is poor.

Answer: F

14. In each option, a Layer 2 security attack is specified. Which statement correctly matches the correct mitigation technique with the specified Layer 2 switch attack?

- A. Configure DHCP spoofing to mitigate ARP address spoofing attacks.
- B. Configure DHCP spoofing to mitigate DHCP spoofing attacks.
- C. Configure PVLANS to mitigate MAC address flooding attacks.
- D. Configure port security to mitigate MAC address flooding attacks.
- E. Enable root guard to mitigate ARP address spoofing attacks.
- F. Configure dynamic ARP inspection (DAI) to mitigate IP address spoofing on DHCP untrusted ports.

Answer: D

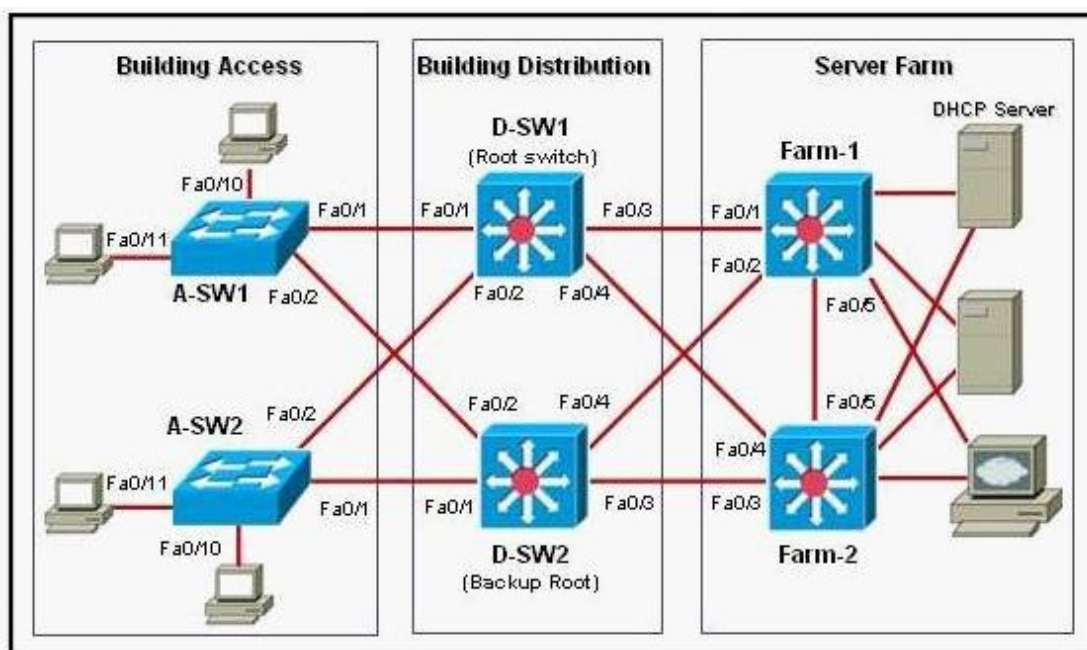
15. Which description correctly describes a MAC address flooding attack?

- A. The attacking device crafts ARP replies intended for valid hosts. The MAC address of the attacking device then becomes the destination address found in the Layer 2 frames sent by the valid network device.
- B. The attacking device crafts ARP replies intended for valid hosts. The MAC address of the attacking device then becomes the source address found in the Layer 2 frames sent by the valid network device.
- C. The attacking device spoofs a destination MAC address of a valid host currently in the CAM table. The switch then forwards frames destined for the valid host to the attacking device.
- D. The attacking device spoofs a source MAC address of a valid host currently in the CAM table. The switch then forwards frames destined for the valid host to the attacking device.
- E. Frames with unique, invalid destination MAC addresses flood the switch and exhaust CAM table space. The result is that new entries cannot be inserted because of the exhausted CAM table space, and traffic is subsequently flooded out all ports.
- F. Frames with unique, invalid source MAC addresses flood the switch and exhaust CAM table space. The result is that new entries cannot be inserted because of the exhausted CAM table space, and traffic is subsequently flooded out all ports.

Answer: F

16. Refer to the exhibit. An attacker is connected to interface Fa0/11 on switch A-SW2 and attempts to establish a DHCP server for a man-in-middle attack. Which recommendation, if followed, would mitigate

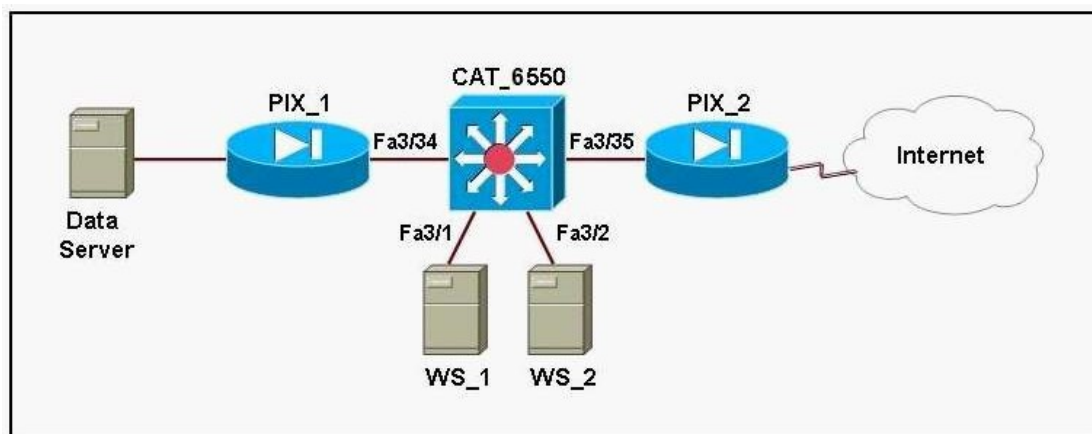
this type of attack?



- A. All switch ports in the Building Access block should be configured as DHCP trusted ports.
- B. All switch ports in the Building Access block should be configured as DHCP untrusted ports.
- C. All switch ports connecting to hosts in the Building Access block should be configured as DHCP trusted ports.
- D. All switch ports connecting to hosts in the Building Access block should be configured as DHCP untrusted ports.
- E. All switch ports in the Server Farm block should be configured as DHCP untrusted ports.
- F. All switch ports connecting to servers in the Server Farm block should be configured as DHCP untrusted ports.

Answer: D

17. Refer to the exhibit. The web servers WS_1 and WS_2 need to be accessed by external and internal users. For security reasons, the servers should not communicate with each other, although they are located on the same subnet. The servers do need, however, to communicate with a database server located in the inside network. What configuration will isolate the servers from each other?



- A. The switch ports 3/1 and 3/2 will be defined as secondary VLAN isolated ports. The ports connecting to the two firewalls will be defined as primary VLAN promiscuous ports.
- B. The switch ports 3/1 and 3/2 will be defined as secondary VLAN community ports. The ports connecting to the two firewalls will be defined as primary VLAN promiscuous ports.
- C. The switch ports 3/1 and 3/2 and the ports connecting to the two firewalls will be defined as primary VLAN promiscuous ports.
- D. The switch ports 3/1 and 3/2 and the ports connecting to the two firewalls will be defined as primary VLAN community ports.

Answer: A

18. What are three required steps to configure DHCP snooping on a switch? (Choose three.)

- A. Configure DHCP snooping globally.
- B. Configure DHCP snooping on an interface.
- C. Configure DHCP snooping on a VLAN or range of VLANs.
- D. Configure the switch as a DHCP server.
- E. Configure all interfaces as DHCP snooping trusted interfaces.
- F. Configure the switch to insert and remove DHCP relay information (option-82 field) in forwarded DHCP request messages.

Answer: ABC

19. A client is searching for an access point (AP). What is the correct process order that the client and access point go through to create a connection?

- A. probe request/response, authentication request/response, association request/response
- B. association request/response, authentication request/response, probe request/response
- C. probe request/response, association request/response, authentication request/response
- D. association request/response, probe request/response, authentication request/response

Answer: A

20. Which statement about the Lightweight Access Point Protocol (LWAPP) protocol is true?

- A. The processing of 802.11 data and management protocols and access point capabilities is distributed between a lightweight access point and a centralized WLAN controller.
- B. LWAPP aggregates radio management forward information and sends it to a wireless LAN solution engine.
- C. LWAPP authenticates all access points in the subnet and establishes a secure communication channel with each of them.
- D. LWAPP advertises its WDS capability and participates in electing the best WDS device for the wireless LAN.

Answer: A