CCNA 2 v7 Modules 10 – 13: L2 Security and WLANs Exam Answers

itexamanswers.net/ccna-2-v7-modules-10-13-l2-security-and-wlans-exam-answers.html

December 21, 2019

How to find: Press **"Ctrl + F"** in the browser and fill in whatever wording is in the question to find that question/answer. If the question is not here, find it in **Questions Bank**.

NOTE: If you have the new question on this test, please comment Question and Multiple-Choice list in form below this article. We will update answers for you in the shortest time. Thank you! We truly value your contribution to the website.

Modules 10 – 13: L2 Security and WLANs Exam Answers

Switching, Routing, and Wireless Essentials (Version 7.00) – L2 Security and WLANs Exam

1. Which Layer 2 attack will result in legitimate users not getting valid IP addresses?

- ARP spoofing
- **DHCP starvation**
- IP address spoofing
- MAC address flooding

Explanation: The DHCP starvation attack causes the exhaustion of the IP address pool of a DHCP server before legitimate users can obtain valid IP addresses.

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

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

Explanation: A MAC address (CAM) table overflow attack, buffer overflow, and MAC address spoofing can all be mitigated by configuring port security. A network administrator would typically not want to disable STP because it prevents Layer 2 loops. DTP is disabled to

prevent VLAN hopping. Placing unused ports in an unused VLAN prevents unauthorized wired connectivity.

3. Which three Cisco products focus on endpoint security solutions? (Choose three.)

- IPS Sensor Appliance
- **Web Security Appliance**
- **Email Security Appliance**
- SSL/IPsec VPN Appliance
- Adaptive Security Appliance
- **NAC Appliance**

Explanation: The primary components of endpoint security solutions are Cisco Email and Web Security appliances, and Cisco NAC appliance. ASA, SSL/IPsec VPN, and IPS sensor appliances all provide security solutions that focus on the enterprise network, not on endpoint devices.

4. True or False?
In the 802.1X standard, the client attempting to access the network is referred to as the supplicant.

- **true**
- false

5. Which authentication method stores usernames and passwords in the router and is ideal for small networks?

- server-based AAA over TACACS+
- local AAA over RADIUS
- server-based AAA
- local AAA over TACACS+
- **local AAA**
- server-based AAA over RADIUS

Explanation: In a small network with a few network devices, AAA authentication can be implemented with the local database and with usernames and passwords stored on the network devices. Authentication using the TACACS+ or RADIUS protocol will require dedicated ACS servers although this authentication solution scales well in a large network.

6. What represents a best practice concerning discovery protocols such as CDP and LLDP on network devices?

- Enable CDP on edge devices, and enable LLDP on interior devices.
- Use the open standard LLDP rather than CDP.

- Use the default router settings for CDP and LLDP.
- **Disable both protocols on all interfaces where they are not required.**

Explanation: Both discovery protocols can provide hackers with sensitive network information. They should not be enabled on edge devices, and should be disabled globally or on a per-interface basis if not required. CDP is enabled by default.

7. Which protocol should be used to mitigate the vulnerability of using Telnet to remotely manage network devices?

- SNMP
- TFTP
- **SSH**
- SCP

Explanation: Telnet uses plain text to communicate in a network. The username and password can be captured if the data transmission is intercepted. SSH encrypts data communications between two network devices. TFTP and SCP are used for file transfer over the network. SNMP is used in network management solutions.

8. Which statement describes the behavior of a switch when the MAC address table is full?

- It treats frames as unknown unicast and floods all incoming frames to all ports on the switch.
- It treats frames as unknown unicast and floods all incoming frames to all ports across multiple switches.
- **It treats frames as unknown unicast and floods all incoming frames to all ports within the local VLAN.**
- It treats frames as unknown unicast and floods all incoming frames to all ports within the collision domain.

Explanation: When the MAC address table is full, the switch treats the frame as an unknown unicast and begins to flood all incoming traffic to all ports only within the local VLAN.

9. What device is considered a supplicant during the 802.1X authentication process?

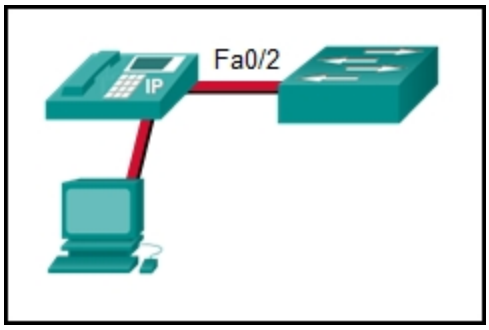
- the router that is serving as the default gateway
- the authentication server that is performing client authentication
- **the client that is requesting authentication**
- the switch that is controlling network access

Explanation: The devices involved in the 802.1X authentication process are as follows:

- The supplicant, which is the client that is requesting network access
- The authenticator, which is the switch that the client is connecting to and that is actually controlling physical network access
- The authentication server, which performs the actual authentication

10. Refer to the exhibit. Port Fa0/2 has already been configured appropriately. The IP phone and PC work properly. Which switch configuration would be most appropriate for port Fa0/2 if the network administrator has the following goals?

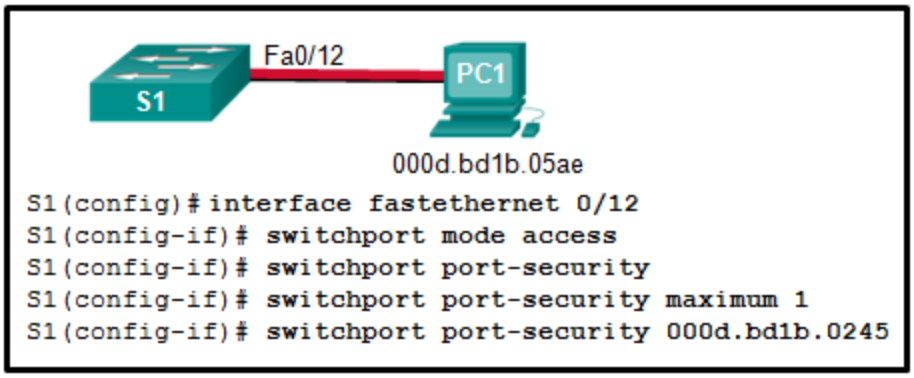
No one is allowed to disconnect the IP phone or the PC and connect some other wired device.
If a different device is connected, port Fa0/2 is shut down.
The switch should automatically detect the MAC address of the IP phone and the PC and add those addresses to the running configuration.



- SWA(config-if)# switchport port-security
  SWA(config-if)# switchport port-security mac-address sticky
- SWA(config-if)# switchport port-security
  SWA(config-if)# switchport port-security maximum 2
  SWA(config-if)# switchport port-security mac-address sticky
  SWA(config-if)# switchport port-security violation restrict
- SWA(config-if)# switchport port-security mac-address sticky
  SWA(config-if)# switchport port-security maximum 2
- **SWA(config-if)# switchport port-security**
  SWA(config-if)# switchport port-security maximum 2
  SWA(config-if)# switchport port-security mac-address sticky

Explanation: The default mode for a port security violation is to shut down the port so the **switchport port-security violation** command is not necessary. The **switchport port-security** command must be entered with no additional options to enable port security for the port. Then, additional port security options can be added.

11. Refer to the exhibit. Port security has been configured on the Fa 0/12 interface of switch S1. What action will occur when PC1 is attached to switch S1 with the applied configuration?



- Frames from PC1 will be forwarded since the switchport port-security violation command is missing.
- Frames from PC1 will be forwarded to its destination, and a log entry will be created.
- Frames from PC1 will be forwarded to its destination, but a log entry will not be created.
- **Frames from PC1 will cause the interface to shut down immediately, and a log entry will be made.**
- Frames from PC1 will be dropped, and there will be no log of the violation.
- Frames from PC1 will be dropped, and a log message will be created.

Explanation: Manual configuration of the single allowed MAC address has been entered for port fa0/12. PC1 has a different MAC address and when attached will cause the port to shut down (the default action), a log message to be automatically created, and the violation counter to increment. The default action of shutdown is recommended because the restrict option might fail if an attack is underway.

12. Which type of VLAN-hopping attack may be prevented by designating an unused VLAN as the native VLAN?

- DHCP spoofing
- DHCP starvation
- **VLAN double-tagging**
- DTP spoofing

Explanation: Spoofing DTP messages forces a switch into trunking mode as part of a VLAN-hopping attack, but VLAN double tagging works even if trunk ports are disabled. Changing the native VLAN from the default to an unused VLAN reduces the possibility of this type of attack. DHCP spoofing and DHCP starvation exploit vulnerabilities in the DHCP message exchange.

13. A network administrator is configuring DAI on a switch with the command ip arp inspection validate src-mac. What is the purpose of this configuration command?

- It checks the source MAC address in the Ethernet header against the user-configured ARP ACLs.
- It checks the source MAC address in the Ethernet header against the MAC address table.
- **It checks the source MAC address in the Ethernet header against the sender MAC address in the ARP body.**
- It checks the source MAC address in the Ethernet header against the target MAC address in the ARP body.

Explanation: DAI can be configured to check for both destination or source MAC and IP addresses:

- **Destination MAC** – Checks the destination MAC address in the Ethernet header against the target MAC address in the ARP body.
- **Source MAC** – Checks the source MAC address in the Ethernet header against the sender MAC address in the ARP body.
- **IP address** – Checks the ARP body for invalid and unexpected IP addresses including addresses 0.0.0.0, 255.255.255.255, and all IP multicast addresses.

14. Which two commands can be used to enable BPDU guard on a switch? (Choose two.)

- S1(config)# spanning-tree bpduguard default
- S1(config-if)# spanning-tree portfast bpduguard
- **S1(config)# spanning-tree portfast bpduguard default**
- S1(config-if)# enable spanning-tree bpduguard
- **S1(config-if)# spanning-tree bpduguard enable**

Explanation: BPDU guard can be enabled on all PortFast-enabled ports by using the **spanning-tree portfast bpduguard default** global configuration command. Alternatively, BPDU guard can be enabled on a PortFast-enabled port through the use of the **spanning-tree bpduguard enable** interface configuration command.

15. As part of the new security policy, all switches on the network are configured to automatically learn MAC addresses for each port. All running configurations are saved at the start and close of every business day. A severe thunderstorm causes an extended power outage several hours after the close of business. When the switches are brought back online, the dynamically learned MAC addresses are retained. Which port security configuration enabled this?

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

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

16. Which type of management frame may regularly be broadcast by an AP?

- authentication
- probe request
- probe response
- **beacon**

Explanation: Beacons are the only management frame that may regularly be broadcast by an AP. Probing, authentication, and association frames are used only during the association (or reassociation) process.

17. What are the two methods that are used by a wireless NIC to discover an AP? (Choose two.)

- delivering a broadcast frame
- **receiving a broadcast beacon frame**
- initiating a three-way handshake
- sending an ARP request
- **transmitting a probe request**

Explanation: Two methods can be used by a wireless device to discover and register with an access point: passive mode and active mode. In passive mode, the AP sends a broadcast beacon frame that contains the SSID and other wireless settings. In active mode, the wireless device must be manually configured for the SSID, and then the device broadcasts a probe request.

18. A technician is configuring the channel on a wireless router to either 1, 6, or 11. What is the purpose of adjusting the channel?

- to enable different 802.11 standards
- **to avoid interference from nearby wireless devices**
- to disable broadcasting of the SSID
- to provide stronger security modes

Explanation: Channels 1, 6, and 11 are selected because they are 5 channels apart. thus minimizing the interference with adjacent channels. A channel frequency can interfere with channels on either side of the main frequency. All wireless devices need to be used on nonadjacent channels.

19. While attending a conference, participants are using laptops for network connectivity. When a guest speaker attempts to connect to the network, the laptop fails to display any available wireless networks. The access point must be operating in which mode?

- mixed
- passive
- **active**
- open

Explanation: Active is a mode used to configure an access point so that clients must know the SSID to connect to the access point. APs and wireless routers can operate in a mixed mode meaning that that multiple wireless standards are supported. Open is an authentication mode for an access point that has no impact on the listing of available wireless networks for a client. When an access point is configured in passive mode, the SSID is broadcast so that the name of wireless network will appear in the listing of available networks for clients.

20. A network administrator is required to upgrade wireless access to end users in a building. To provide data rates up to 1.3 Gb/s and still be backward compatible with older devices, which wireless standard should be implemented?

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

Explanation: 802.11ac provides data rates up to 1.3 Gb/s and is still backward compatible with 802.11a/b/g/n devices. 802.11g and 802.11n are older standards that cannot reach speeds over 1Gb/s. 802.11ad is a newer standard that can offer theoretical speeds of up to 7 Gb/s.

21. A technician is about to install and configure a wireless network at a small branch office. What is the first security measure the technician should apply immediately upon powering up the wireless router?

- Enable MAC address filtering on the wireless router.
- Configure encryption on the wireless router and the connected wireless devices.
- **Change the default user-name and password of the wireless router.**
- Disable the wireless network SSID broadcast.

Explanation: The first action a technician should do to secure a new wireless network is to change the default user-name and password of the wireless router. The next action would usually be to configure encryption. Then once the initial group of wireless hosts have connected to the network, MAC address filtering would be enabled and SSID broadcast disabled. This will prevent new unauthorized hosts from finding and connecting to the wireless network.

22. On a Cisco 3504 WLC dashboard, which option provides access to the full menu of features?

- Access Points
- Network Summary
- **Advanced**
- Rogues

Explanation: The Cisco 3504 WLC dashboard displays when a user logs into the WLC. It provides some basic settings and menus that users can quickly access to implement a variety of common configurations. By clicking the **Advanced** button, the user will access the advanced **Summary** page and access all the features of the WLC.

23. Which step is required before creating a new WLAN on a Cisco 3500 series WLC?

- Create a new SSID.
- Build or have an SNMP server available.
- Build or have a RADIUS server available.
- **Create a new VLAN interface.**

Explanation: Each new WLAN configured on a Cisco 3500 series WLC needs its own VLAN interface. Thus it is required that a new VLAN interface to be created first before a new WLAN can be created.

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

- Requiring the users to switch to the 5 GHz band for streaming media is inconvenient and will result in fewer users accessing these services.
- **The 5 GHz band has more channels and is less crowded than the 2.4 GHz band, which makes it more suited to streaming multimedia.**

- The 5 GHz band has a greater range and is therefore likely to be interference-free.
- The only users that can switch to the 5 GHz band will be those with the latest wireless NICs, which will reduce usage.

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

25. A network administrator is configuring a RADIUS server connection on a Cisco 3500 series WLC. The configuration requires a shared secret password. What is the purpose for the shared secret password?

- It is used by the RADIUS server to authenticate WLAN users.
- It is used to authenticate and encrypt user data on the WLAN.
- **It is used to encrypt the messages between the WLC and the RADIUS server.**
- It allows users to authenticate and access the WLAN.

Explanation: The RADIUS protocol uses security features to protect communications between the RADIUS server and clients. A shared secret is the password used between the WLC and the RADIUS server. It is not for end users.

26. Which three parameters would need to be changed if best practices are being implemented for a home wireless AP? (Choose three.)

- wireless client operating system password
- antenna frequency
- **wireless network password**
- wireless beacon time
- **AP password**
- **SSID**

Explanation: As soon as an AP is taken out of a box, the default device password, SSID, and security parameters (wireless network password) should be set. The frequency of a wireless antenna can be adjusted, but doing so is not required. The beacon time is not normally configured. The wireless client operating system password is not affected by the configuration of a home wireless network.

27. Which access control component, implementation, or protocol is based upon usernames and passwords?

- 802.1X
- accounting
- **authentication**
- authorization

28. Which type of wireless network is based on the 802.11 standard and a 2.4-GHz or 5-GHz radio frequency?

- wireless metropolitan-area network
- wireless wide-area network
- **wireless local-area network**
- wireless personal-area network

29. Which two Cisco solutions help prevent DHCP starvation attacks? (Choose two.)

- **DHCP Snooping**
- IP Source Guard
- Dynamic ARP Inspection
- **Port Security**
- Web Security Appliance

Explanation: Cisco provides solutions to help mitigate Layer 2 attacks including these:

- **IP Source Guard (IPSG)** – prevents MAC and IP address spoofing attacks
- **Dynamic ARP Inspection (DAI)** – prevents ARP spoofing and ARP poisoning attacks
- **DHCP Snooping** – prevents DHCP starvation and SHCP spoofing attacks
- **Port Security** – prevents many types of attacks including MAC table overflow attacks and DHCP starvation attacks

Web Security Appliance (WSA) is a mitigation technology for web-based threats.

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

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

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

31. Refer to the exhibit. What can be determined about port security from the information that is shown?

```
ATC_S2# show port-security interface fastethernet 0/3
Port Security               : Enabled
Port Status                 : Secure-up
Violation Mode              : Shutdown
Aging Time                  : 0 mins
Aging Type                  : Absolute
SecureStatic Address Aging  : Disabled
Maximum MAC Addresses       : 2
Total MAC Addresses         : 1
Configured MAC Addresses    : 0
Sticky MAC Addresses        : 1
Last Source Address:Vlan    : 00D0.D3B6.C26B:10
Security Violation Count    : 0
```

- The port has the maximum number of MAC addresses that is supported by a Layer 2 switch port which is configured for port security.
- The port has been shut down.
- **The port violation mode is the default for any port that has port security enabled.**
- The port has two attached devices.

Explanation: The *Port Security* line simply shows a state of *Enabled* if the **switchport port-security** command (with no options) has been entered for a particular switch port. If a port security violation had occurred, a different error message appears such as *Secure-shutdown*. The maximum number of MAC addresses supported is 50. The *Maximum MAC Addresses* line is used to show how many MAC addresses can be learned (2 in this case). The *Sticky MAC Addresses* line shows that only one device has been attached and learned automatically by the switch. This configuration could be used when a port is shared by two cubicle-sharing personnel who bring in separate laptops.

32. A network administrator of a college is configuring the WLAN user authentication process. Wireless users are required to enter username and password credentials that will be verified by a server. Which server would provide such service?

- AAA
- NAT
- **RADIUS**
- SNMP

Explanation: Remote Authentication Dial-In User Service (RADIUS) is a protocol and server software that provides user-based authentication for an organization. When a WLAN is configured to use a RADIUS server, users will enter username and password credentials

that are verified by the RADIUS server before allowing to the WLAN.

33. A technician is troubleshooting a slow WLAN that consists of 802.11b and 802.11g devices . A new 802.11n/ac dual-band router has been deployed on the network to replace the old 802.11g router. What can the technician do to address the slow wireless speed?

- **Split the wireless traffic between the 802.11n 2.4 GHz band and the 5 GHz band.**
- Update the firmware on the new router.
- Configure devices to use a different channel.
- Change the SSID.

Explanation: Splitting the wireless traffic between the 802.11n 2.4 GHz band and the 5 GHz band will allow for the 802.11n to use the two bands as two separate wireless networks to help manage the traffic, thus improving wireless performance.

34. The company handbook states that employees cannot have microwave ovens in their offices. Instead, all employees must use the microwave ovens located in the employee cafeteria. What wireless security risk is the company trying to avoid?

- improperly configured devices
- rogue access points
- **accidental interference**
- interception of data

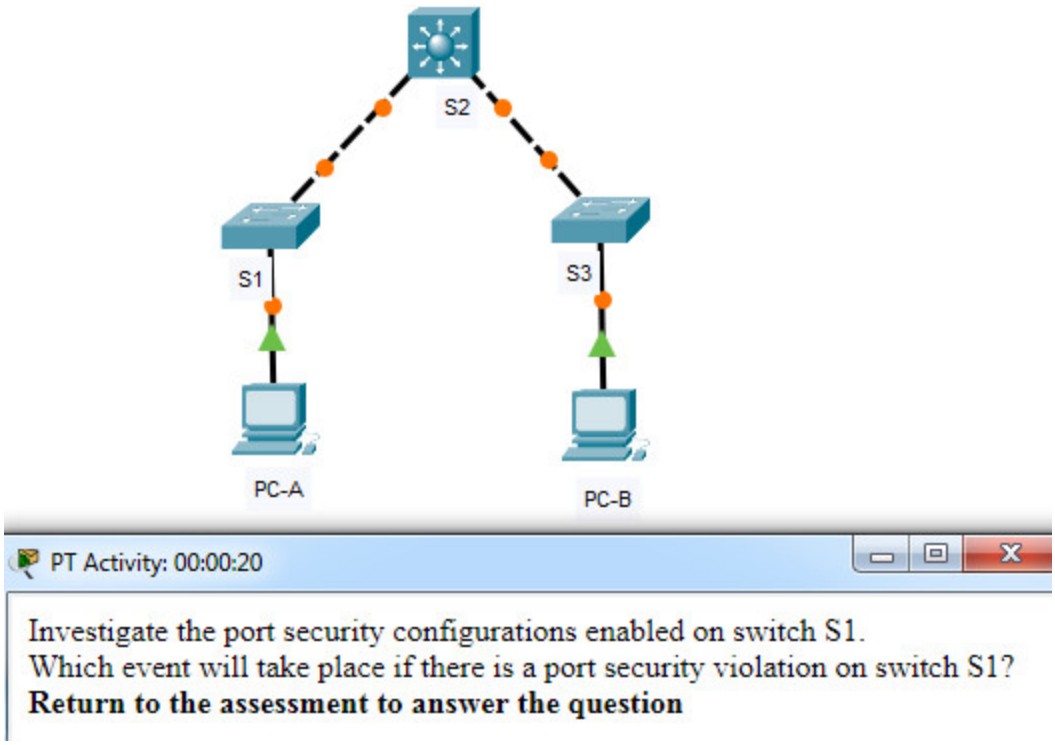
Explanation: Denial of service attacks can be the result of improperly configured devices which can disable the WLAN. Accidental interference from devices such as microwave ovens and cordless phones can impact both the security and performance of a WLAN. Man-in-the-middle attacks can allow an attacker to intercept data. Rogue access points can allow unauthorized users to access the wireless network.

35. What is the function provided by CAPWAP protocol in a corporate wireless network?

- CAPWAP creates a tunnel on Transmission Control Protocol (TCP) ports in order to allow a WLC to configure an autonomous access point.
- **CAPWAP provides the encapsulation and forwarding of wireless user traffic between an access point and a wireless LAN controller.**
- CAPWAP provides connectivity between an access point using IPv6 addressing and a wireless client using IPv4 addressing.
- CAPWAP provides the encryption of wireless user traffic between an access point and a wireless client.

Explanation: CAPWAP is an IEEE standard protocol that enables a WLC to manage multiple APs and WLANs. CAPWAP is also responsible for the encapsulation and forwarding of WLAN client traffic between an AP and a WLC.

36. Open the PT Activity. Perform the tasks in the activity instructions and then answer the question.



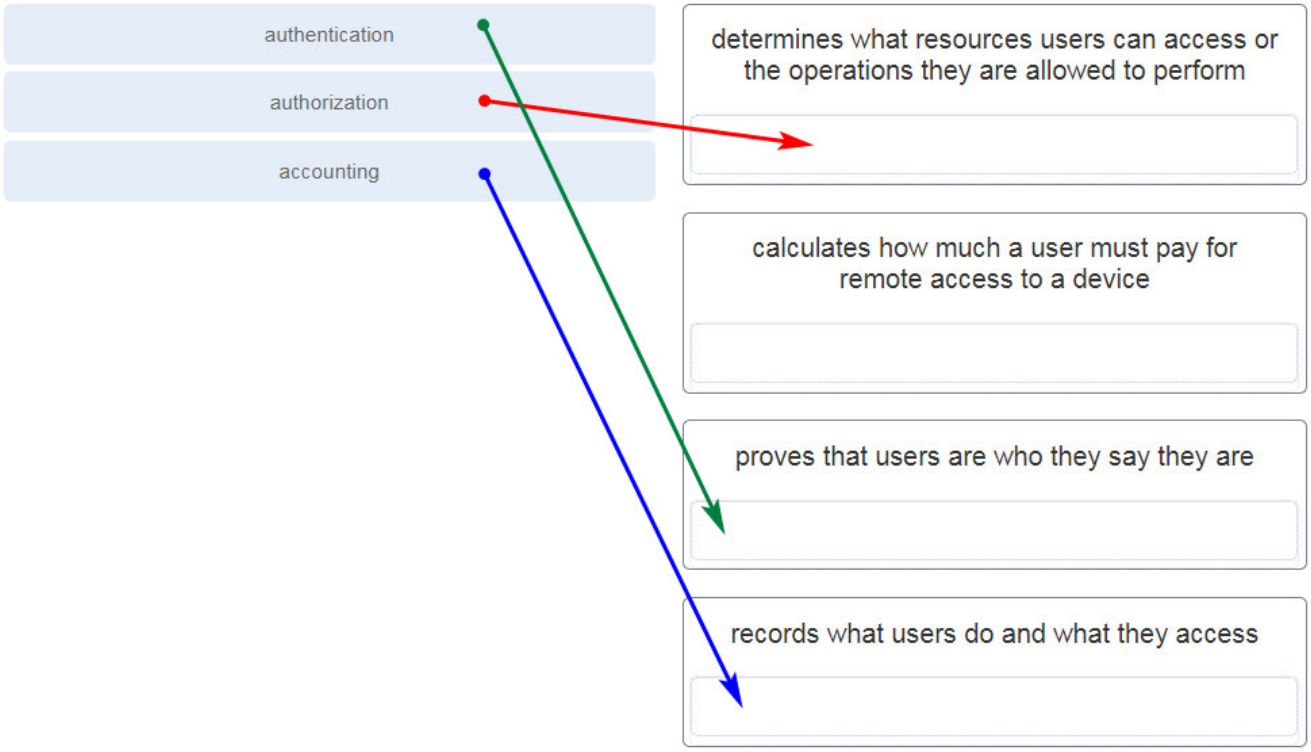
Modules 10 – 13: L2 Security and WLANs Exam Answers

Which event will take place if there is a port security violation on switch S1 interface Fa0/1?

- A syslog message is logged.
- The interface will go into error-disabled state.
- **Packets with unknown source addresses will be dropped.**
- A notification is sent.

Explanation: The violation mode can be viewed by issuing the **show port-security interface** <*int*>command. Interface FastEthernet 0/1 is configured with the violation mode of protect. If there is a violation, interface FastEthernet 0/1 will drop packets with unknown MAC addresses.

37. Match each functional component of AAA with its description. (Not all options are used.)



38. What are two protocols that are used by AAA to authenticate users against a central database of usernames and password? (Choose two.)

- SSH
- HTTPS
- **TACACS+**
- **RADIUS**
- CHAP
- NTP

Explanation: By using TACACS+ or RADIUS, AAA can authenticate users from a database of usernames and passwords stored centrally on a server such as a Cisco ACS server.

39. What is the result of a DHCP starvation attack?

- The attacker provides incorrect DNS and default gateway information to clients.
- The IP addresses assigned to legitimate clients are hijacked.
- Clients receive IP address assignments from a rogue DHCP server.
- **Legitimate clients are unable to lease IP addresses.**

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

40. Which feature or configuration on a switch makes it vulnerable to VLAN double-tagging attacks?

- the limited size of content-addressable memory space
- the automatic trunking port feature enabled for all ports by default
- **the native VLAN of the trunking port being the same as a user VLAN**
- mixed duplex mode enabled for all ports by default

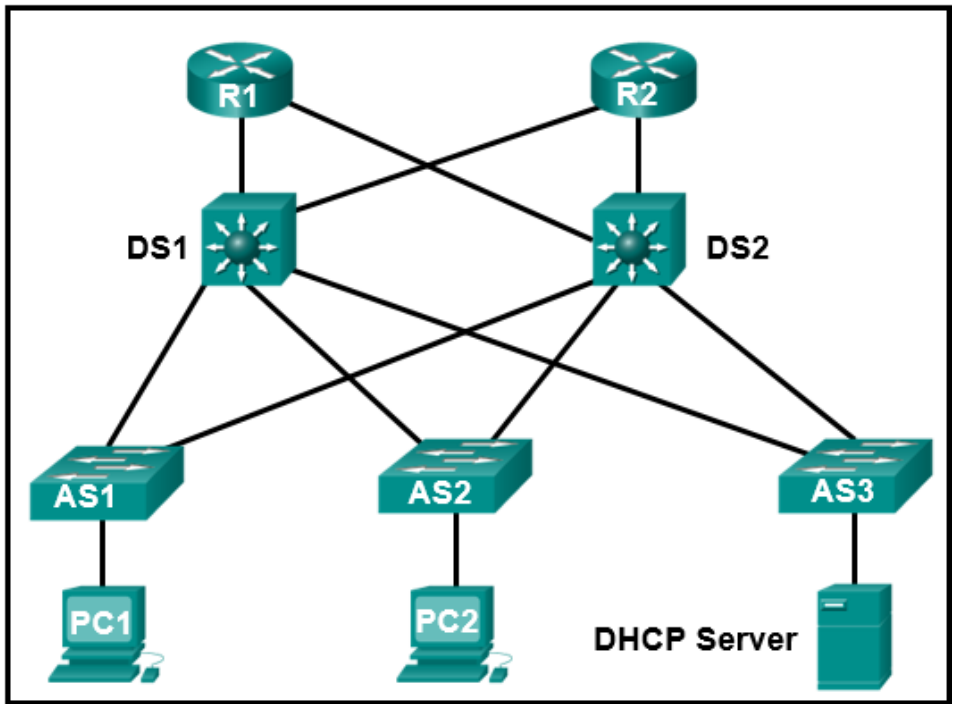
Explanation: A double-tagging (or double-encapsulated) VLAN hopping attack takes advantage of the way that hardware on most switches operates. Most switches perform only one level of 802.1Q de-encapsulation, which allows an attacker to embed a hidden 802.1Q tag inside the frame. This tag allows the frame to be forwarded to a VLAN that the original 802.1Q tag did not specify. An important characteristic of the double-encapsulated VLAN hopping attack is that it works even if trunk ports are disabled, because a host typically sends a frame on a segment that is not a trunk link. This type of attack is unidirectional and works only when the attacker is connected to a port residing in the same VLAN as the native VLAN of the trunk port.

41. Which component of AAA allows an administrator to track individuals who access network resources and any changes that are made to those resources?

- authentication
- **accounting**
- accessibility
- authorization

Explanation: One of the components in AAA is accounting. After a user is authenticated through AAA, AAA servers keep a detailed log of exactly what actions the authenticated user takes on the device.

42. Refer to the exhibit. PC1 and PC2 should be able to obtain IP address assignments from the DHCP server. How many ports among switches should be assigned as trusted ports as part of the DHCP snooping configuration?



- 1
- 3
- 5
- 7

Explanation: The DHCP snooping configuration includes building the DHCP Snooping Binding Database and assigning necessary trusted ports on switches. A trusted port points to the legitimate DHCP servers. In this network design, because the DHCP server is attached to AS3, seven switch ports should be assigned as trusted ports, one on AS3 toward the DHCP server, one on DS1 toward AS3, one on DS2 toward AS3, and two connections on both AS1 and AS2 (toward DS1 and DS2), for a total of seven.

43. An IT security specialist enables port security on a switch port of a Cisco switch. What is the default violation mode in use until the switch port is configured to use a different violation mode?

- **shutdown**
- disabled
- restrict
- protect

Explanation: If no violation mode is specified when port security is enabled on a switch port, then the security violation mode defaults to shutdown.

44. A laptop cannot connect to a wireless access point. Which two troubleshooting steps should be taken first? (Choose two.)

- Ensure that the correct network media is selected.
- Ensure that the laptop antenna is attached.
- **Ensure that the wireless NIC is enabled.**
- **Ensure that the wireless SSID is chosen.**
- Ensure that the NIC is configured for the proper frequency.

Explanation: A wireless laptop normally does not have an antenna attached unless a repair has recently been implemented. If the wireless NIC is enabled, the correct media, radio, will be used. When the NIC detects an access point, the correct frequency is automatically used.

45. What is an advantage of SSID cloaking?

- **Clients will have to manually identify the SSID to connect to the network.**
- It is the best way to secure a wireless network.
- SSIDs are very difficult to discover because APs do not broadcast them.
- It provides free Internet access in public locations where knowing the SSID is of no concern.

Explanation: SSID cloaking is a weak security feature that is performed by APs and some wireless routers by allowing the SSID beacon frame to be disabled. Although clients have to manually identify the SSID to be connected to the network, the SSID can be easily discovered. The best way to secure a wireless network is to use authentication and encryption systems. SSID cloaking does not provide free Internet access in public locations, but an open system authentication could be used in that situation.

46. What is a wireless security mode that requires a RADIUS server to authenticate wireless users?

- personal
- shared key
- **enterprise**
- WEP

Explanation: WPA and WPA2 come in two types: personal and enterprise. Personal is used in home and small office networks. Shared key allows three different authentication techniques: (1) WEP, (2) WPA, and (3) 802.11i/WPA2. WEP is an encryption method.

47. A company has recently implemented an 802.11n wireless network. Some users are complaining that the wireless network is too slow. Which solution is the best method to enhance the performance of the wireless network?

- Disable DHCP on the access point and assign static addresses to the wireless clients.
- Upgrade the firmware on the wireless access point.
- **Split the traffic between the 2.4 GHz and 5 GHz frequency bands.**

- Replace the wireless NICs on the computers that are experiencing slow connections.

Explanation: Because some users are complaining about the network being too slow, the correct option would be to split the traffic so that there are two networks using different frequencies at the same time. Replacing the wireless NICs will not necessarily correct the network being slow and it could be expensive for the company. DHCP versus static addressing should have no impact of the network being slow and it would be a huge task to have all users assigned static addressing for their wireless connection. Upgrading the firmware on the wireless access point is always a good idea. However, if some of the users are experiencing a slow network connection, it is likely that this would not substantially improve network performance.

48. Which protocol can be used to monitor the network?

- DHCP
- **SNMP**
- RADIUS
- AAA

Explanation: Simple Network Management Protocol (SNMP) is used to monitor the network.

49. A network administrator deploys a wireless router in a small law firm. Employee laptops join the WLAN and receive IP addresses in the 10.0.10.0/24 network. Which service is used on the wireless router to allow the employee laptops to access the internet?

- DHCP
- RADIUS
- DNS
- **NAT**

Explanation: Any address with the 10 in the first octet is a private IPv4 address and cannot be routed on the internet. The wireless router will use a service called Network Address Translation (NAT) to convert private IPv4 addresses to internet-routable IPv4 addresses for wireless devices to gain access to the internet.

50. Which service can be used on a wireless router to prioritize network traffic among different types of applications so that voice and video data are prioritized over email and web data?

- **QoS**
- DNS
- DHCP

- NAT

Explanation: Many wireless routers have an option for configuring quality of service (QoS). By configuring QoS, certain time-sensitive traffic types, such as voice and video, are prioritized over traffic that is not as time-sensitive, such as email and web browsing.

51. Which access control component, implementation, or protocol is based on device roles of supplicant, authenticator, and authentication server?

- accounting
- authentication
- authorization
- **802.1X**

52. Which type of wireless network is suitable for national and global communications?

- wireless metropolitan-area network
- wireless local-area network
- wireless personal-area network
- **wireless wide-area network**

53. Which feature on a switch makes it vulnerable to VLAN hopping attacks?

- the mixed duplex mode enabled for all ports by default
- the limited size of content-addressable memory space
- mixed port bandwidth support enabled for all ports by default
- **the automatic trunking port feature enabled for all ports by default**

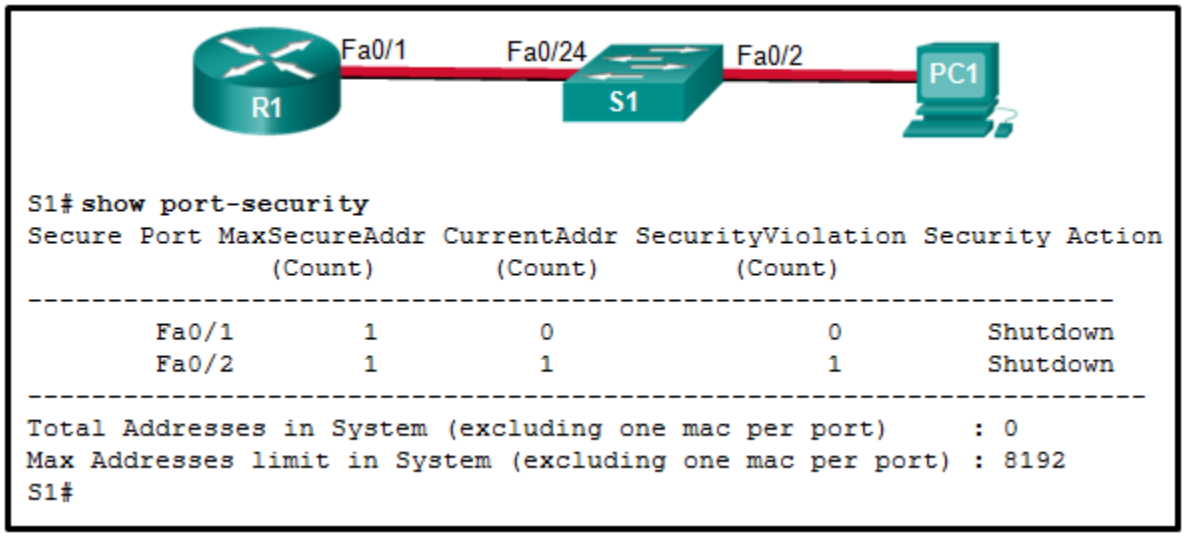
Explanation: A VLAN hopping attack enables traffic from one VLAN to be seen by another VLAN without routing. In a basic VLAN hopping attack, the attacker takes advantage of the automatic trunking port feature enabled by default on most switch ports.

54. Which component of AAA is used to determine which resources a user can access and which operations the user is allowed to perform?

- accounting
- authentication
- auditing
- **authorization**

Explanation: One of the components in AAA is authorization. After a user is authenticated through AAA, authorization services determine which resources the user can access and which operations the user is allowed to perform.

55. Refer to the exhibit. The Fa0/2 interface on switch S1 has been configured with the switchport port-security mac-address 0023.189d.6456 command and a workstation has been connected. What could be the reason that the Fa0/2 interface is shutdown?



CCNA 2 v7 Modules 10 – 13: L2 Security and WLANs Exam Answers 55

- The Fa0/24 interface of S1 is configured with the same MAC address as the Fa0/2 interface.
- The connection between S1 and PC1 is via a crossover cable.
- S1 has been configured with a `switchport port-security aging` command.
- **The MAC address of PC1 that connects to the Fa0/2 interface is not the configured MAC address.**

Explanation: The security violation counter for Fa0/2 has been incremented (evidenced by the 1 in the SecurityViolation column). The most secure addresses allowed on port Fa0/2 is 1 and that address was manually entered. Therefore, PC1 must have a different MAC address than the one configured for port Fa0/2. Connections between end devices and the switch, as well as connections between a router and a switch, are made with a straight-through cable.

56. A network administrator enters the following commands on the switch SW1.

```
SW1(config)# interface range fa0/5 - 10
SW1(config-if)# ip dhcp snooping limit rate 6
```

What is the effect after these commands are entered?

- If any of the FastEthernet ports 5 through 10 receive more than 6 DHCP messages per second, the port will be shut down.
- FastEthernet ports 5 through 10 can receive up to 6 DHCP messages per second of any type.

- If any of the FastEthernet ports 5 through 10 receive more than 6 DHCP messages per second, the port will continue to operate and an error message will be sent to the network administrator.
- **FastEthernet ports 5 through 10 can receive up to 6 DHCP discovery messages per second.**

Explanation: When DHCP snooping is being configured, the number of DHCP discovery messages that untrusted ports can receive per second should be rate-limited by using the ip dhcp snooping limit rate interface configuration command. When a port receives more messages than the rate allows, the extra messages will be dropped.

57. A network administrator is configuring port security on a Cisco switch. The company security policy specifies that when a violation occurs, packets with unknown source addresses should be dropped and no notification should be sent. Which violation mode should be configured on the interfaces?

- off
- restrict
- **protect**
- shutdown

Explain: On a Cisco switch, an interface can be configured for one of three violation modes, specifying the action to be taken if a violation occurs:Protect – Packets with unknown source addresses are dropped until a sufficient number of secure MAC addresses are removed, or the number of maximum allowable addresses is increased. There is no notification that a security violation has occurred.
Restrict – Packets with unknown source addresses are dropped until a sufficient number of secure MAC addresses are removed, or the number of maximum allowable addresses is increased. In this mode, there is a notification that a security violation has occurred.
Shutdown – The interface immediately becomes error-disabled and the port LED is turned off.

58. A network administrator is working to improve WLAN performance on a dual-band wireless router. What is a simple way to achieve a split-the-traffic result?

- Add a Wi-Fi range extender to the WLAN and set the AP and the range extender to serve different bands.
- Check and keep the firmware of the wireless router updated.
- **Make sure that different SSIDs are used for the 2.4 GHz and 5 GHz bands.**
- Require all wireless devices to use the 802.11n standard.

Explanation: By default, dual-band routers and APs use the same network name on both the 2.4 GHz band and the 5 GHz band. The simplest way to segment traffic is to rename one of the wireless networks.

59. Which access control component, implementation, or protocol controls what users can do on the network?

- accounting
- 802.1X
- **authorization**
- authentication

60. Which type of wireless network is suitable for providing wireless access to a city or district?

- wireless wide-area network
- wireless personal-area network
- wireless local-area network
- **wireless metropolitan-area network**

61. On a Cisco 3504 WLC Summary page (Advanced > Summary), which tab allows a network administrator to access and configure a WLAN for a specific security option such as WPA2?

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

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

62. What type of wireless antenna is best suited for providing coverage in large open spaces, such as hallways or large conference rooms?

- Yagi
- **omnidirectional**
- dish
- directional

Explanation: Omnidirectional antennas send the radio signals in a 360 degree pattern around the antenna. This provides coverage to devices situated anywhere around the access point. Dishes, directional, and Yagi antennas focus the radio signals in a single direction, making them less suitable for covering large, open areas.

64. What security benefit is gained from enabling BPDU guard on PortFast enabled interfaces?

- preventing buffer overflow attacks
- **preventing rogue switches from being added to the network**
- protecting against Layer 2 loops
- enforcing the placement of root bridges

Explanation: BPDU guard immediately error-disables a port that receives a BPDU. This prevents rogue switches from being added to the network. BPDU guard should only be applied to all end-user ports.

65. Which access control component, implementation, or protocol logs EXEC and configuration commands configured by a user?

- authentication
- authorization
- 802.1X
- **accounting**

66. Which type of wireless network uses transmitters to provide coverage over an extensive geographic area?

- wireless metropolitan-area network
- wireless local-area network
- wireless personal-area network
- **wireless wide-area network**

67. Which access control component, implementation, or protocol controls who is permitted to access a network?

- authorization
- 802.1X
- accounting
- **authentication**

68. What two IEEE 802.11 wireless standards operate only in the 5 GHz range? (Choose two.)

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

Explanation: The 802.11a and 802.11ac standards operate only in the 5 GHZ range. The 802.11b and 802.11g standards operate only in the 2.4 GHz range. The 802.11n standard operates in both the 2.4 and 5 GHz ranges. The 802.11ad standard operates in the 2.4, 5, and 60 GHz ranges.

69. Which type of wireless network uses low powered transmitters for a short-range network, usually 20 to 30 ft. (6 to 9 meters)?

- wireless metropolitan-area network
- **wireless personal-area network**
- wireless local-area network
- wireless wide-area network

71. Which wireless network topology would be used by network engineers to provide a wireless network for an entire college building?

- ad hoc
- hotspot
- **infrastructure**
- mixed mode

72. Which type of wireless network uses transmitters to provide wireless service over a large urban region?

- wireless wide-area network
- wireless personal-area network
- **wireless metropolitan-area network**
- wireless local-area network.

73. Which type of wireless network is suitable for use in a home or office?

- wireless wide-area network
- wireless personal-area network
- **wireless local-area network**
- wireless metropolitan-area network

74. Which access control component, implementation, or protocol indicates success or failure of a client-requested service with a PASS or FAIL message?

- accounting
- authentication
- 802.1X
- **authorization**

75. Which type of wireless network often makes use of devices mounted on buildings?

- wireless local-area network
- **wireless metropolitan-area network**
- wireless personal-area network
- wireless wide-area network

76. A network administrator is configuring DAI on a switch with the command ip arp inspection validate src-mac . What is the purpose of this configuration command?

- It checks the source MAC address in the Ethernet header against the user-configured ARP ACLs.
- It checks the source MAC address in the Ethernet header against the MAC address table.
- **It checks the source MAC address in the Ethernet header against the sender MAC address in the ARP body.**
- It checks the source MAC address in the Ethernet header against the target MAC address in the ARP body.

Explanation: DAI can be configured to check for both destination or source MAC and IP addresses:
Destination MAC – Checks the destination MAC address in the Ethernet header against the target MAC address in the ARP body.
Source MAC – Checks the source MAC address in the Ethernet header against the sender MAC address in the ARP body.
IP address – Checks the ARP body for invalid and unexpected IP addresses including addresses 0.0.0.0, 255.255.255.255, and all IP multicast addresses.

77. Which access control component, implementation, or protocol collects and reports usage data?

- **accounting**
- authentication
- authorization
- 802.1X

78. Which type of wireless network uses transmitters to cover a medium-sized network, usually up to 300 feet (91.4 meters)?

Wireless LANs (WLAN)

79. Which access control component, implementation, or protocol audits what users actions are performed on the network?

- **Accounting**
- Authorization
- Authentication
- 802.1X

Explanation:
The final plank in the AAA framework is accounting, which measures the resources a user consumes during access. This can include the amount of system time or the amount of data a user has sent and/or received during a session. Accounting is carried out by logging of session statistics and usage information and is used for authorization control, billing, trend analysis, resource utilization, and capacity planning activities.

80. Which type of wireless network commonly uses Bluetooth or ZigBee devices?

- wireless wide-area network
- **wireless personal-area network**
- wireless local-area network
- wireless metropolitan-area network

81. Which access control component, implementation, or protocol is implemented either locally or as a server-based solution?

- authorization
- 802.1X
- accounting
- **authentication**

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

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

83. Which access control component, implementation, or protocol restricts LAN access through publicly accessible switch ports?

- **802.1X**
- authorization
- accounting
- authentication