Chapter 21: Quiz – Troubleshooting Wireless Connectivity (Answers) CCNPv8 ENCOR

itexamanswers.net/chapter-21-quiz-troubleshooting-wireless-connectivity-answers-ccnpv8-encor.html

January 11, 2021

13. A wireless LAN is being deployed inside the new one room office that is occupied by the park ranger. The office is located at the highest part of the national park. After network testing is complete, the technicians report that the wireless LAN signal is occasionally affected by some type of interference. What are two possible causes of the signal distortion? (Choose two.)

- **the microwave oven**
- the large number of trees that surround the office
- **the cellular phones that are used by the employees**
- the elevated location where the wireless LAN was installed
- the number of wireless devices that are used in the wireless LAN

Explanation: Wireless LAN connectivity is not affected by trees or the elevation of the equipment. Because this is a one room office in an isolated area, there will not be a large number of wireless devices or source of interference operating in the immediate vicinity, apart from a cellular phone or a microwave oven.

14. Which protocol could be used by a company to monitor devices such as a wireless LAN controller (WLC)?

- NTP
- PAT
- **SNMP**
- SSH

Explanation: The Simple Network Management Protocol (SNMP) is an application layer protocol used to monitor and manage the network. Network devices must be configured with a community name and IP address of the SNMP server.

15. HealthOne, Inc. provides wireless connectivity in its clinic facilities for staff access to internal network resources. The wireless security policy specifies that the staff must perform user-based authentication with a special back-end authentication server before they are allowed to access the WLAN. Which technology should be chosen in the WLAN implementation to meet this requirement?

- **EAP**

- PSK
- WEP
- WPA

Explanation: Extensible Authentication Protocol (EAP) is an authentication framework that supports multiple authentication mechanisms without having to pre-negotiate a particular one. EAP authentication is initiated by the server (authenticator), whereas many other authentication protocols are initiated by the client (peer).

16. A threat actor uses network scanning tools and penetration tools to discover the IP address and manufacturer of a home wireless router. The threat actor then uses internet searches to discover the default administrative access details. Successful remote access of the home router allows the threat actor to use it as a vector to attack other devices. Which element of smart home security is affected by this attack?

- WPA2
- firmware
- encryption
- **authentication**

Explanation: In general, the security requirements for a Smart Home should include these:

- **WPA2** – The wireless network should use the latest Wi-Fi security which is currently WPA2.
- **Encryption** – It protects the confidentiality and integrity of information transmitted over a network.
- **Authentication** – Strong authentication protects the device from unauthorized use or reconfiguration and prevents disclosure or modification of the data stored on the device.
- **Firmware** – The IoT device manufacturers should update the firmware for any newly discovered vulnerabilities. The home IoT device users should enable the checking of updates automatically.

17. Which device provides wireless connectivity to users as its primary function?

- switch
- router
- **access point**
- modem

Explanation: A switch connects multiple devices to a network. A router will forward traffic between networks. A wireless router will connect multiple wireless devices to a network. An access point will provides wireless connectivity to multiple devices and has fewer features

than a wireless router. A modem will connect a home or small office to the Internet.

18. What is a DHCP scope as it relates to a WLAN configured on the WLC controller?

- a corporate plan for allocation of IP addresses for wireless clients
- **a pool of IP addresses for WLAN clients**
- security rules associated with DHCP for WLANs
- the distance allotted for wireless clients that can receive IP addressing information

Explanation: When configuring a WLC controller as a DHCP server, use the DHCP Scope menu option to configure IP address-related settings such as the range of IP addresses to assign to WLAN devices, a DNS server address, and lease time.

19. Included in a Bill of Materials (BOM) for a SOHO wired implementation is a Cisco 2811 router, Catalyst 2560 switch, four PCs, three laptops, and a networked printer. Wireless LAN capability will be implemented on this network. Which two equipment types must be added to the BOM to implement this request? (Choose two.)

- DNS server
- LAN switch
- **wireless NICs**
- DHCP server
- **wireless access points**

Explanation: In order to connect to a 802.11 WLAN network, a client must first authenticate and then associate with the AP. Because association only occurs on wireless infrastructure networks, wireless NICs and at least one AP (access point) would be required by the clients.

20. Which WLC tab would a network administrator typically use to see a summary view of the most heavily used WLANs including the number of clients using a particular WLAN?

- Commands
- Controller
- **Monitor**
- WLANs

Explanation: Use the **Monitor** tab and then the **Summary** option to see information about the WLC, including the IP address and system uptime as well as information associated with the top WLANs configured and active within the organization.

21. A network administrator is configuring the SNMP function on a Cisco 3500 series WLC. The task is to add an SNMP trap server to which this WLC will forward SNMP log messages. Which tab should the administrator use to add the SNMP trap server information?

- MONITOR
- COMMANDS
- CONTROLLER
- **MANAGEMENT**

Explanation: On the Cisco 3500 series WLC, click the **MANAGEMENT** tab. SNMP is listed at the top of the menu on the left. Click **SNMP** to expand the sub-menus, and then click **Trap Receivers**. Click **New...** to configure a new SNMP trap receiver.

22. After the administrator manually configures the correct SSID on a new laptop, the computer is still unable to connect to the wireless LAN. Which additional action should the administrator take to resolve this problem?

- Modify the group account of the user to include all file permissions.
- Reboot the wireless access point.
- Rename the laptop and reset the user password on the network.
- **Verify that the MAC address for the laptop is in the MAC address filter table.**

Explanation: MAC address filtering sets up authorized MAC addresses, preventing unauthorized devices from accessing the WLAN. When adding a new device to a WLAN with a MAC filter, the MAC address of the new device must be added to the filter list before it will be able to join the network.

23. Which feature or function does an AP provide in a wireless LAN?

- An AP is easier to configure and to set up than Wi-Fi range extenders.
- Each AP advertises one or more SSIDs and a user can choose to connect to the closest SSID.
- **A wireless device has to be associated to an AP in order to have access to network resources.**
- A wireless client can connect to more than one AP at a time.

Explanation: Although range extenders are easy to set up and configure, the best solution would be to install another wireless access point to provide dedicated wireless access to the user devices. Wireless clients use their wireless NIC to discover nearby APs advertising their SSID. Clients then attempt to associate and authenticate with an AP. After being authenticated, wireless users have access to network resources.

24. Which statement describes an autonomous access point?

- It is used for networks that require a large number of access points.
- **It is a standalone access point.**
- It is server-dependent.
- It is managed by a WLAN controller.

Explanation: An autonomous access point is used in environments that require a small number of access points. As network demands increase, more access points can be added to the environment with each access point acting independently of another. An autonomous access point can be configured using either a GUI or CLI.