Compare and Contrast Wireless Security Features and Capabilities of WPA Security (Including Open, WEP, WPA1/2)

An unsecured wireless network provides easy access for all users in range, including unauthorized, unwelcome, and possibly evil users. Wireless security features can help you keep the evil out of your network. Chapter 7 of *CCNA Discovery 1* and Chapter 8 of *CCNA Discovery 2* discuss methods available to better secure a WLAN.

CCNA Discovery 1, Chapter 7

7.3.1 and 7.3.2: Unauthorized users attempt to tap into a wireless LAN to obtain free Internet service and possibly steal data from the WLAN. Often an AP signal reaches outside a building or the desired range of the administrator. To avoid malicious war drivers or war walkers, an administrator should implement the following security features on a WLAN during initial setup:

- **SSID broadcast:** You can disable the SSID broadcast feature and require anyone connecting to the network to know the broadcast SSID. However, the SSID is transmitted in clear text, so it is not difficult to discover the SSID for a network.
- **Default settings:** You can change the default settings on your AP, including usernames, passwords, IP addresses, and the SSID to make it more difficult for an intruder to discover the unique settings.
- **MAC address filtering:** You can enable MAC address filtering and specify a list of MAC addresses for devices that are allowed to connect to the network. This requires the manual entry of each MAC address into the list. An intruder can sniff and clone an existing authorized MAC address.

7.3.3: In addition to the default settings and MAC filtering, you can implement authentication for the wireless LAN. Authentication requires the AP to verify a host before it connects to the network using criteria such as a username or password. Authentication occurs before MAC filtering. There are three types of wireless authentication:

- **Open authentication:** Typically used on a public network, open authentication allows all clients to connect to the WLAN. Open authentication is also used in configurations that require separate authentication for the Internet or additional network access as soon as the device has connected to the WLAN.
- **Preshared keys (PSK):** Both AP and client are configured with the same key. When the client requests a connection, the AP asks the client to use the client's key to encrypt a string of information. If the AP can then use its key to decrypt the information, the client is granted access. This is considered one-way authentication because the AP does not authenticate with the host. The user does not have to authenticate, only the host.

- **Extensible Authentication Protocol (EAP):** The EAP software installed on the client communicates with an authentication server such as a Remote Authentication Dial-In User Service (RADIUS). The RADIUS server maintains a database of users separate from the AP. When the user enters a login and password for the network, the AP forwards the login information to the RADIUS server to check its database for validity.

7.3.4: An unauthorized user who cannot authenticate to a network can still intercept wireless frames from a wireless network. You can encrypt all transmission on your network to make it more difficult for an unauthorized user to retrieve data from intercepted frames. Table 6-1 describes two methods of WLAN encryption that allow you to better protect your data.

Table 6-1 WLAN Encryption Protocols

Protocol	Key Length	Description
Wired Equivalent Privacy (WEP)	64 to 256 bits	All devices including the AP must have the same manually configured static key to understand transmissions on the WLAN. Some devices have a passphrase option to make the key easier to remember. Hacking software exists that can extract the static WEP key, so using WEP alone to secure a network is strongly discouraged today.
Wi-Fi Protected Access (WPA)	64 to 256 bits	WPA dynamically generates a different key with each client communication with the AP. The dynamic key makes WPA more difficult to crack than WEP.

7.3.5: In addition to authentication, MAC filtering, and transmission encryption, you can filter network traffic at the AP. The graphical user interface (GUI) in an AP typically allows you to filter network traffic by source and destination MAC address, source and destination port address, and source and destination IP address.

CCNA Discovery 2, Chapter 8

8.2.4: As a quick review with some additional information, remember the following key points about securing a wireless network:

- It is important to change the default settings, such as the SSID and the login, to unique settings for your WLAN.
- You can filter network access by MAC address, but users can clone an authorized MAC address to access the network.
- WEP provides encrypted transmission with a key up to 256 bits. However, WPA provides more secure encryption because it uses temporal key integrity protocol (TKIP) to generate new keys for clients and rotate key use at a configurable interval. WPA also does not require transmission of the key, because both client and AP have the key. WPA2 (802.11i) is an improved version of WPA that uses Advanced Encryption Standard (AES) technology.
- The 802.1x standard can also be implemented on an AP to provide additional security with EAP.

Identify Common Issues with Implementing Wireless Networks

Wireless networks can sometimes suffer from mysterious connectivity issues. The invisible interference and limitations you may encounter while implementing a wireless network are discussed in Chapters 7 and 9 of *CCNA Discovery 1*.

CCNA Discovery 1, Chapter 7

7.4.1–7.4.3: When planning a WLAN, consider the following factors:

- **Coverage areas:** 802.11b/g/n have a larger coverage area than 802.11a.
- **Existing implementations:** 802.11n generally is backward-compatible with 802.11a/b/g, but some access points (AP) do not support the 5-GHz frequency and are not backward-compatible with 802.11a. A preexisting 802.11a installation may require all new equipment to support the same standard if your new APs do not support the 5-GHz frequency.
- **Bandwidth requirements:** All users share bandwidth on a BSS. The number of simultaneous users and type of applications in use can dictate the need for higher-speed equipment.
- **Cost:** Consider the total cost of ownership (TCO), including the equipment, installation, and support.
- **Site survey:** It is important to measure signal strength and interference around the building to determine the most efficient place to install the APs on site.
- **Security:** As mentioned, it is important to plan how you will secure a network. This includes disabling the broadcast SSID, enabling MAC filtering and authentication, setting up WEP or WPA encryption, and filtering unwanted network traffic.
- **Backups:** APs typically have a menu option to back up a configuration to a place you specify on a PC or the network. This allows you to restore the configuration if you forget the password and have to press the reset button to restore your AP to factory defaults. I do this at home about once every four months.

CCNA Discovery 1, Chapter 9

9.3.4 and 9.3.5: Connectivity problems on a WLAN can occur because of authentication issues, interference, signal strength, standards mismatches, and bandwidth issues. Consider the following points when troubleshooting a WLAN:

- **Standards:** The client or AP may be using incompatible standards such as 802.11a on the 5-GHz frequency and 802.11b on the 2.4-GHz frequency.
- **Channels:** Overlapping channels for conversations between devices may be affecting connectivity.

- **Signal:** A lower-strength signal may cause a connection to periodically drop and/or become unreliable. In addition, outside sources such as wireless devices not associated with the WLAN may be interfering with the signal.
- **Bandwidth:** An increase in users or high bandwidth utilization may affect network performance. You can monitor traffic and identify users or applications that hog bandwidth and deal with them professionally, personally, and possibly technically.
- **Association:** Make sure that the case-sensitive SSID is correct on clients and the AP and that a client is not connecting to a different BSS.
- **Authentication:** Check that the same keys, encryption protocols, and proper usernames and passwords are in use on the network.

Summary

Security and a reliable connection are important features in any WLAN. Today you reviewed simple security steps such as SSID configuration and encryption. In addition, you reviewed possible issues that can arise during WLAN implementation, such as channel overlap and signal strength. Day 7 and today provide you with the basic knowledge you need to design, configure, secure, and troubleshoot a WLAN.

Your Notes