5.10.5 Wireless Encryption Facts

Security for wireless networking can be implemented using the following methods:

Method	Description

Wired Equivalent Privacy	Wired Equivalent Privacy (WEP) is an optional component of the 802.11 specifications and was deployed in 1997. WEP was intended to provide wireless connections with the same security as wired connections. WEP was available in 64-bit and 128-bit implementations. WEP:
	▪ Uses Rivest Cipher 4 (RC4) with a 40-bit key and 24-bit initialization vector (IV) for encryption.
	▪ Uses CRC-32 for data integrity applied to the data only (not the header).
	▪ Requires that keys be manually configured on each device.
	▪ Uses a short initialization that allows hackers to easily crack the key.
	WEP uses the following authentication methods:
	▪ Open authentication, which requires that clients provide a MAC address in order to connect to the wireless network.
	  ▪ You can use open authentication to allow any wireless client to connect to the access point. Open authentication is typically used on public networks.
	  ▪ You can implement MAC address filtering to restrict access to the access point to only known or allowed MAC addresses. Because MAC addresses are easily spoofed, this provides little practical security.
	▪ Shared key authentication, which uses static pre-shared keys (PSKs) configured on the access point and the client.
	  ▪ With shared key authentication, all access points and all clients use the same authentication key.
	  ▪ A session is initiated with a four-way challenge–response handshake.
	  ▪ Disadvantages to the shared key method are:
	  ▪ The shared key is statically configured and must be changed manually.
	  ▪ Part of the WEP shared key is transmitted in cleartext with each network frame.
	  ▪ Shared key authentication is relatively insecure because the hashing methods used to protect the key can be easily broken.
	WEP is still better than nothing and may prevent the casual war driver from getting access to the network, but any hacker with the right tools can get in very quickly, making it an insecure method.

Wi-Fi Protected Access	Wi-Fi Protected Access (WPA) is the implementation name for wireless security based on initial 802.11i drafts and was deployed in 2003. It was intended as an intermediate measure to take the place of WEP while a fully secured system (802.11i) was prepared. WPA can use 802.1x authentication, which requires user names and passwords, certificates, or devices such as smart cards to authenticate wireless clients. Originally designed for Ethernet networks, the 802.1x standards have been adapted for use in wireless networks to provide secure authentication. WPA: ▪ Uses Temporal Key Integrity Protocol (TKIP) for encryption. ▪ Provides dynamic keys and dynamic key rotation. ▪ Can typically be implemented in WEP-only devices through a software/firmware update. ▪ Uses the Message Integrity Check (MIC) algorithm for data integrity applied to both the data and the header. ▪ Supports both pre-shared key (referred to as WPA-PSK or WPA Personal) and 802.1x (referred to as WPA Enterprise) authentication. ▪ Can be cracked if the passphrase is short enough using a brute force attack. A very long and complex passphrase is required to provide a degree of security with WPA.
Wi-Fi Protected Access 2	Wi-Fi Protected Access 2 (WPA2) adheres to the 802.11i specifications and was deployed in 2005. It is built upon the idea of Robust Secure Networks (RSN). Like WPA, it resolves the weaknesses inherent in WEP and is intended to replace both WEP and WPA. WPA2: ▪ Uses Cipher Block Chaining Message Authentication Code (CBC-MAC) for data integrity applied to both the data and the header. ▪ Uses Advanced Encryption Standard (AES) with either TKIP or Counter Mode with CBC-MAC Protocol (CCMP), also known as AES-CCMP. AES-CCMP is a strong encryption method and provides a high level of security. ▪ Supports dynamic key generation and rotation through CCMP. ▪ Supports both pre-shared key (referred to as WPA2-PSK or WPA2 Personal) and 802.1x (referred to as WPA2 Enterprise) authentication. WPA2 has the same advantages over WEP as WPA.

You can also enable IPsec on your wireless connections to provide data transmission encryption.