10.6.2 Wireless Security Facts

Authentication to wireless networks is implemented using the following methods:

Method	Description
Open	Open authentication 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 AP. Open authentication is typically used on public networks. ▪ You can implement MAC address filtering to restrict access to the AP to only known (or allowed) MAC addresses. Because MAC addresses are easily spoofed, this provides little practical security.
Shared Key	With shared key authentication, clients and APs are configured with a shared key (called a secret or a passphrase). Only devices with the correct shared key can connect to the wireless network. ▪ All APs and all clients use the same authentication key. ▪ Use shared key authentication on small, private networks. ▪ Shared key authentication is relatively insecure, as hashing methods used to protect the key can be easily broken.
802.1x	802.1x authentication uses usernames 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. 802.1x authentication requires the following components: ▪ A RADIUS server to centralize user account and authentication information. A centralized database for user authentication is required to allow wireless clients to roam between cells but authenticate using the same account information. ▪ A PKI for issuing certificates. At a minimum, the RADIUS server must have a server certificate. To support mutual authentication, each client must also have a certificate. Use 802.1x authentication on large, private networks. Users authenticate with unique usernames and passwords.

Security for wireless networking is provided from the following standards:

Method	Description
Wi-Fi Protected Access (WPA)	WPA is the implementation name for wireless security based on initial 802.11i drafts that was deployed in 2003. It was intended to be an intermediate measure to take the place of WEP while a fully secured system (802.11i) was prepared. WPA: ▪ Uses Temporal Key Integrity Protocol (TKIP) for encryption. ▪ Supports both pre-shared key (WPA-PSK or WPA Personal) and 802.1x (WPA Enterprise) authentication. ▪ Can use dynamic keys or pre-shared keys. ▪ Can typically be implemented in WEP-capable devices through a software/firmware update. WPA keys can also be predicted by reconstructing the Message Integrity Check (MIC) of an intercepted packet, sending the packet to an AP, and observing whether the packet is accepted by the AP.
Wi-Fi Protected Access 2 (WPA2) or 802.11i	WPA2 is the implementation name for wireless security that adheres to the 802.11i specifications. It was deployed in 2005. It is built upon the idea of Robust Secure Networks (RSN). Like WPA, it resolves the weaknesses inherent in WEP; it is intended to eventually replace both WEP and WPA. WPA2: ▪ Uses Advanced Encryption Standard (AES) as the encryption method. It is similar to (yet more secure than) TKIP but requires special hardware for performing encryption. ▪ Uses Counter Mode with CBC-MAC Protocol (CCMP), also known as AES-CCMP. ▪ Supports both pre-shared key (WPA2-PSK or WPA2 Personal) and 802.1x (WPA2 Enterprise) authentication. ▪ Can use dynamic keys or pre-shared keys. WPA2 has the same advantages over WEP as WPA. While WPA2 is more secure than WPA, its main disadvantage is that it requires new hardware for implementation.

When transmitting data on a wireless network, it's important to know if the channel you are using is encrypted. Information sent on unencrypted channels, where no security is being used, can be easily intercepted and viewed. If needed, IPsec can be used to provide security when sending information on an unencrypted channel.

In addition to using the security measures outlined above, you can provide a level of security using the following practices. These methods by themselves do not provide much security, but they do keep curious people from trying to access the wireless network.

Method	Description
Change the Default Name and Password	APs typically come configured with a default username and password that is used to configure AP settings. It's important to change the administrator account name and password from the defaults. This prevents outsiders from breaking into your system by guessing the default username and password.
Change Default SSID and Broadcast	Many manufacturers use a default SSID, so it's important to change your SSID from the default. You can also disable the SSID broadcast for further protection; this is known as SSID suppression, or cloaking. Even if the SSID broadcast is turned off, a determined hacker can still identify the SSID by analyzing wireless broadcasts.
Enable MAC Address Filtering	Every network board has a unique MAC address. By specifying which MAC addresses are allowed to connect to your network, you can prevent unauthorized MAC addresses from connecting to the AP. Configuring a MAC address filtering system is very time consuming and demands upkeep. Attackers can still use tools to capture packets and retrieve valid MAC addresses. An attacker could spoof their wireless adapter's MAC address and circumvent the filter.
Update the Firmware	Update the firmware on the AP from the manufacturer's website frequently to prevent your system from being exposed to known bugs and security vulnerabilities. While it's extremely important to keep your devices up to date, it's just as important to properly test new updates before pushing them out to the entire network. Proper testing will save you the headache of troubleshooting new bugs or problems on the live network that the update may have introduced.
Enable the Firewall on the AP	Most wireless APs come with a built-in firewall that connects the wireless network to a wired network.
Disable DHCP	DHCP servers dynamically assign IP addresses, gateway addresses, subnet masks, and DNS addresses whenever a computer on the wireless network starts up. Disabling DHCP on the wireless APs allows only users with a valid, static IP address in the range to connect.
Geofencing	Geofencing requires users to be in a physical location by using virtual boundaries, or fences, can add another layer of security to your network.