7.3.5 Access Point Configuration Facts

If the SOHO router includes a wireless access point, or if a standalone wireless access point is being used, use the following configuration steps to configure and secure the wireless network:

Action	Description
Change the Default SSID	Many manufacturers use a default SSID that contains identifying information (such as device manufacturer and model number), so it is important to change the device's SSID from the default. In addition to changing the default SSID, it is also possible to disable the SSID broadcast. This is known as *SSID suppression* or *cloaking*. With broadcasting disabled, the SSID needs to be manually entered into devices for them to connect to the network (the SSID will not show up in the list of available networks). Even with the broadcast disabled, it's relatively easy to identify the SSID of a network by using readily available applications. Because of this, SSID suppression should not be the only form of protection.
Configure the Wireless Protocol	If your access point supports multiple wireless protocols, select the protocols to support, such as 802.11n only or mixed mode (both 802.11n and 802.11g). Be aware that when using mixed mode, most access points will throttle all clients to the slowest connected protocol speeds (i.e. if a 802.11g client connects to the network, 802.11n clients will operate at 802.11g speeds).
Configure the Channel	The channel identifies the portion of the wireless frequency used by the access point and connected devices. ▪ You should use a channel that does not overlap or conflict with other access points in the area. A simple rule to minimize conflicts is to remember that the frequencies used by channels 2–5 compete with the frequencies used by channels 1 and 6, while the frequencies used by channels 7–10 compete with the frequencies used by channels 6 and 11. ▪ Many access points have an automatic channel feature that detects other access points and automatically selects the channel with the least amount of traffic.
Configure Encryption and Authentication	Add authentication to allow only authorized devices to connect. Use encryption to protect wireless communications from eavesdropping. ▪ Always use WPA2 when possible. If WPA2 isn't available, use WPA. ▪ Use pre-shared key (PSK) authentication with either AES (more secure) or TKIP (less secure) encryption for a SOHO network without a domain, ▪ Configure the shared secret (passphrase) value used with WPA2 or WPA. Each client needs to be configured with same secret value. Because WEP has several known security vulnerabilities and can be easily cracked, it should be used only as a last resort. When using WEP, *never* use shared key authentication; use only open authentication.
Enable MAC Address	By specifying which MAC addresses are allowed to connect to your network, you can prevent unauthorized devices from connecting to the access point. MAC address filtering

Filtering	can be implemented in one of two ways: - All MAC addresses are allowed to connect to the network, except for those specified in the deny list. - All MAC addresses are denied access, except for those specified in the allow list. MAC address filtering is considered a cumbersome and weak form of security. Permitted MAC addresses can be very easily captured and spoofed by even casual attackers.
Disable DHCP for Wireless Clients	Disabling DHCP on the wireless access points allows only users with a valid, static IP address in the range to connect. An attacker would have to be able to discover or detect the IP address range, subnet mask, and default gateway information to connect to the access point.
Determine Best Access Point Placement	The location of the access point can affect signal strength and network access. Keep in mind the following recommendations: - Place access points in central locations. Radio waves are broadcast in each direction, so the access point should be located in the middle of the area that needs network access. - Place access point to take advantage of the fact that devices often get better reception from access points that are above or below. - In general, place access points higher up to avoid interference problems caused by going through building foundations. - For security reasons, do not place access points near outside walls. The signal will extend outside beyond the walls. Placing the access point in the center of the building decreases the range of the signals available outside of the building. - Do not place the access point next to sources of interference, such as other wireless transmitting devices (cordless phones or microwaves) or other sources of interference (motors or generators).
Configure Wi-Fi Protected Setup (WPS)	The WPS security protocol makes it easier for WPS-enabled devices (e.g., a wireless printer) to connect to the wireless network. WPS can use several methods for connecting devices, including the PIN method and the push button method. The method used to connect devices must be supported by both the access point and the wireless device. Because of the inherent security vulnerabilities with WPS, it is best to disable this feature on the access point.