7.1 802.11 Wireless

As you study this section, answer the following questions:

- What type of device is required to create an infrastructure wireless network configuration?
- What is the purpose of an SSID?
- Which wireless standards are typically backwards compatible with 802.11g?
- Two access points are part of the same wireless network. Should they use the same channel, or a different channel? Why?
- How does MIMO differ from channel bonding?
- What happens to the speed of a wireless connection as you move away from the access point?
- Which authentication and security method should be used on a wireless network?
- Why should default security settings be changed when dealing with wireless networking?

In this section, you will learn to:

- Connect to a wireless network
- Create a home wireless network
- Secure home wireless network
- Configure a wireless profile

Key terms for this section include the following:

Term	Definition
Ad hoc	A temporary peer-to-peer mode network.
Infrastructure wireless network	An infrastructure wireless network employs an access point that functions like a hub on an Ethernet network.
Service set identifier (SSID)	The network name.
Multiple-input multiple-output (MIMO)	An enhancement that allows multiple antennas to use the same radio frequency.
Channel bonding	Combining channels into one to increase bandwidth.
Multi-user multiple-input multiple-output (MU-MIMO)	An enhancement to MIMO that allows a set of devices with individual antennas, rather than just one device with an antenna, to communicate with each other.
Dual-band access point	A network device that connects Wi-Fi devices to form a Wi-Fi network.
Open authentication	A token-based authentication standard that requires a MAC address to use.
Shared key authentication	A wireless network access protocol that uses WEP.
802.1x authentication	An authentication standard that uses username/passwords, certificates, or devices such as smart cards to authenticate clients.

Wired Equivalent Privacy (WEP)	An optional component of the 802.11 specifications.
Wi-Fi Protected Access (WPA)	A wireless security based on 802.11i specifications.
Wi-Fi Protected Access II (WPA2)	A wireless security that adheres to 802.11i specifications.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut PC Pro	1.5 Configure networking devices 1.5.1 Install and configure a wired and wireless network adapters and cables 1.5.2 Install and configure internet connection devices

CompTIA 220-1001	1.2 Given a scenario, install components within the display of a laptop
	▪ Types
	  ▪ WiFi antenna connector/placement
	2.3 Given a scenario, install and configure a basic wired/wireless SOHO network.
	▪ Wireless settings
	  ▪ Encryption
	2.4 Compare and contrast wireless networking protocols.
	▪ 802.11a
	▪ 802.11b
	▪ 802.11g
	▪ 802.11n
	▪ 802.11ac
	▪ Frequencies
	  ▪ 2.4Ghz
	  ▪ 5Ghz
	2.5 Summarize the properties and purposes of services provided by networked hosts.
	▪ Server roles
	  ▪ Authentication server
	3.9 Given a scenario, install and configure common devices.
	▪ Laptop/common mobile devices

	▪ Wireless settings

CompTIA 220-1002	1.8 Given a scenario, configure Microsoft Windows networking on a client/desktop
	▪ Establish networking connections
	  ▪ Wireless
	
	2.2 Explain logical security concepts.
	▪ Certificates
	
	2.3 Compare and contrast wireless security protocols and authentication methods.
	▪ Protocols and encryption
	  ▪ WEP
	  ▪ WPA
	  ▪ WPA2
	  ▪ TKIP
	  ▪ AES
	▪ Authentication
	  ▪ RADIUS
	  ▪ TACACS