13.1.2 Wireless Facts

This lesson covers the following topics:

- Wireless overview
- Access points
- Wireless connection types
- Service Set Identifiers
- Wi-Fi authentication modes
- Wireless antenna types
- Wireless IEEE standards

Wireless Overview

In the earlier days of networking, most communication devices, such as laptops, servers, and routers, could be connected together using only wires. For example, most wired networks use Ethernet cables to transfer data between connected computers.

A wireless network (Wi-Fi) provides the same type of communication capabilities, but instead, uses radio waves to transmit data to and from the devices. This type of communication is often referred to as an unbounded data communication system since the data being transmitted is not bound by wires. While wired networks are faster, more reliable, and harder to hack into, wireless technology offers the convenience of mobility and, in many cases, is less expensive to implement.

Most work environments today use a combination of wired and wireless technology. For example, most office workers will be given a laptop that is capable of transmitting data using both wired and wireless technology. While working in the office, the worker's computer is typically connected to a wired Ethernet port that provides maximum bandwidth and throughput to all network resources. However, when the worker needs to go to another location, the computer is unplugged from the wired network and switches to a wireless network automatically. This allows the worker to continue to access corporate resources without a wired connection.

In a wired network, the unauthorized capture of data is generally limited only to those who have physical access to the wired network. With wireless technology, hackers have found it easier to target victims since the data flows freely through the air and often extends beyond the bounds of the building. As such, it’s critical that wireless communication is protected using technologies such as encryption, passwords, disabling broadcast of network names, physical protection, and so on.

Access Points

To properly protect a company’s valuable data, it’s important to understand the various methods and technologies used when implementing a wireless network. For example, to allow wireless and wired devices to communicate with each other, there must be some type of transition between the two technologies.

This type of transition is made possible using an access point. Access points can be implemented in a variety of ways, such as using a hardware-based access point or a software-based access point as follows:

Access Point Implementation Type	Description
Hardware-based	A hardware-based access point is a physical device that provides a bridge between a wireless client, such as a laptop, and the wired network.
Software-based (virtual Wi-Fi)	A software-based access point is a computer containing a wireless card configured, through software, to function as an access point and to provide a bridge between a wireless client and the wired network. This lets you avoid having to buy additional hardware for the purpose of an access point. Software-based access points can sometimes be configured to work as a wireless client as well.

Regardless of the type of access points used, it is important that each access point is strategically placed to provide an overlap with neighboring access points. This allows a user to easily move from one location to another without losing access to the network.

Wireless Connection Types

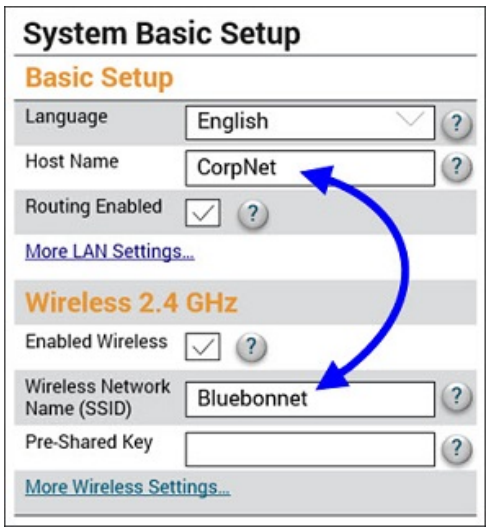
When working with wireless technology, consider the following wireless connection types:

Wireless Connection Type	Description
LAN-to-LAN wireless	The connection of two networks by means of a wireless connection. LAN-to-LAN connections can be less expensive in many circumstances and can provide a connection between sites that may be impossible or too expensive to connect otherwise.
Hotspots	Mobile hotspots let you connect an internet-capable device to the internet through a wireless, portable device, such as a phone or other physical device. Hotspots form an on-the-spot Wi-Fi network, allowing you to connect a number of computers or devices to the network for simple, fast internet access. Hotspots often use third, fourth, and fifth generation (3G, 4G, and 5G) technology to provide this type of connection. Although personal phones are often used as hotspots, many businesses, such as airports and coffee shops, provide hotspots for their customers.

Service Set Identifiers

To ensure that each wireless client is communicating with the desired network, access points are configured with a unique character ID known as a service set identifier (SSID). Each SSID can be a maximum of 32 characters. Once a connection to an access point has been established, each packet sent over a wireless network will include the SSID, ensuring that the data being sent over the air arrives at the correct location.

The name of an access point can be the same as the SSID; however, most wireless routers let you assign a unique SSID separate from the name that users or customers see when connecting the network. Although an SSID is necessary for a secure network, on its own, it doesn't do much to make a network more secure. For example, SSIDs are sent in a packet in plain text. A hacker can easily capture the packet using a sniffing tool, such as Wireshark and TCPDump. Some network administrators turn off SSID broadcasting in an attempt to hide a network, but many experts say that this can actually make a wireless LAN more vulnerable to attack.



Wi-Fi Authentication Modes

As part of the SSID configuration process, you will often need to configure the type of authentication that will be used.

Authentication Mode	Description
Open system authentication	Allows any device to connect to the wireless network. The major advantage of open mode is its simplicity. Any client can connect easily and without complex configuration. Open system authentication is often used at locations such as airports, coffee shops, and universities for guest access only.
Pre-shared encryption key	Uses a software key that is installed on each device that uses a wireless connection. The key is used to connect to the wireless network. Network access is only allowed if the client and the access point have the same key.

The basic steps used to connect to a wireless network using a pre-shared encryption key is as follows:

1. The client sends an authentication request to the access point.
2. The access point replies by sending a challenge text.
3. The client uses its pre-shared key to encrypt the challenge text and then sends it back to the access point.
4. The access point decrypts the text using its pre-shared encryption key, which should be the same as the client key.
5. If the decrypted challenge text matches the text that was sent, access is granted.

Wireless Antenna Types

A wireless antenna fulfills two key roles. First, it receives incoming radio signals from other devices. Second, it transmits outgoing radio signals to other devices. Some wireless antennas are mounted externally, such as on the top of a building or on the outside of an access point. Others are embedded within the device itself.

Selecting the right type of antenna has a critical impact on the function and security of your wireless network. Although there are many types of wireless antennas available. The following table describes three of the more commonly used antennas:

Antenna Type	Description
 Yagi	A special type of high-gain directional antenna. High-gain means that the antenna radiates a focused, narrow radio wave beam width. Directional antennas radiate their signals in one main direction and are often used to connect wireless networks between buildings.
	A high-gain antenna that uses a curved surface, known as a parabolic reflector, to direct the radio waves. When choosing a parabolic antenna, the larger the dish, in terms of wavelengths, the higher the gain. Parabolic antennas also provide high levels of directivity, meaning that they radiate their signal in a narrower beamwidth.

 Parabolic	
 Dipole	A straight electrical conductor measuring 1/2 wavelength from end to end and connected at the center to a radio-frequency feed line. Dipole antennas are typically the least expensive antennas.

Wireless IEEE Standards

As with other technologies, the Institute of Electrical and Electronic Engineers (IEEE) has created a set of standards that define communication for wireless LANs (wireless local area networks [WLANs]). End users or consumers of 802.11 normally refer to this standard as Wi-Fi.

Wi-Fi is transmitted at frequencies between 2.4 GHz or 80 GHz. This frequency is considerably higher than the frequencies used for cell phones, walkie-talkies, and televisions. The higher frequency allows the signal to carry more data.

Extensions of the 802.11 standard were given the same number with a letter suffix. The following table describes a few of the 802.11 specifications:

Wireless Standard	Transmission and Band	Description
802.11	Up to 2 Mbps transmission in the 2.4 GHz band	The original specification.
802.11b	Up to 11 Mbps transmission in the 2.4 GHz band	The slowest and least expensive standard. It uses complementary code keying (CCK) modulation to improve speeds.
802.11a	Up to 54 Mbps transmission in the 5 GHz band	Uses an Orthogonal Frequency Division Multiplexing (OFDM) communication system. OFDM is a more efficient coding technique that splits the radio signal into several sub-signals before it reaches a receiver. This greatly reduces interference.
802.11g	Up to 54 Mbps transmission in the 2.4 GHz band	This standard is faster than 802.11b and 802.11a because it uses the same OFDM coding as 802.11a.
802.11n	Up to 140 Mbps transmission in the 40 GHz band	This standard transmits up to four streams of data, each at a maximum of 150 Mbps. But most routers allow for only two or three streams. It is, perhaps, the most widely available of the standards, and is backward compatible with a, b, and g.
802.11ac	Up to 450 Mbps transmission in the 80 MHz band	This standard transmits up to eight streams of data, which can then be combined to make 160 MHz channels. 802.11ac is less prone to interference and far faster than its predecessors