Wireless Architecture Facts

When you implement a radio frequency wireless network, you use radio waves rather than wires to connect your hosts. Radio waves are considered unbounded media because, unlike wires, they have nothing to encase them. The most commonly used frequency for wireless networking is the 2.4 GHz frequency.

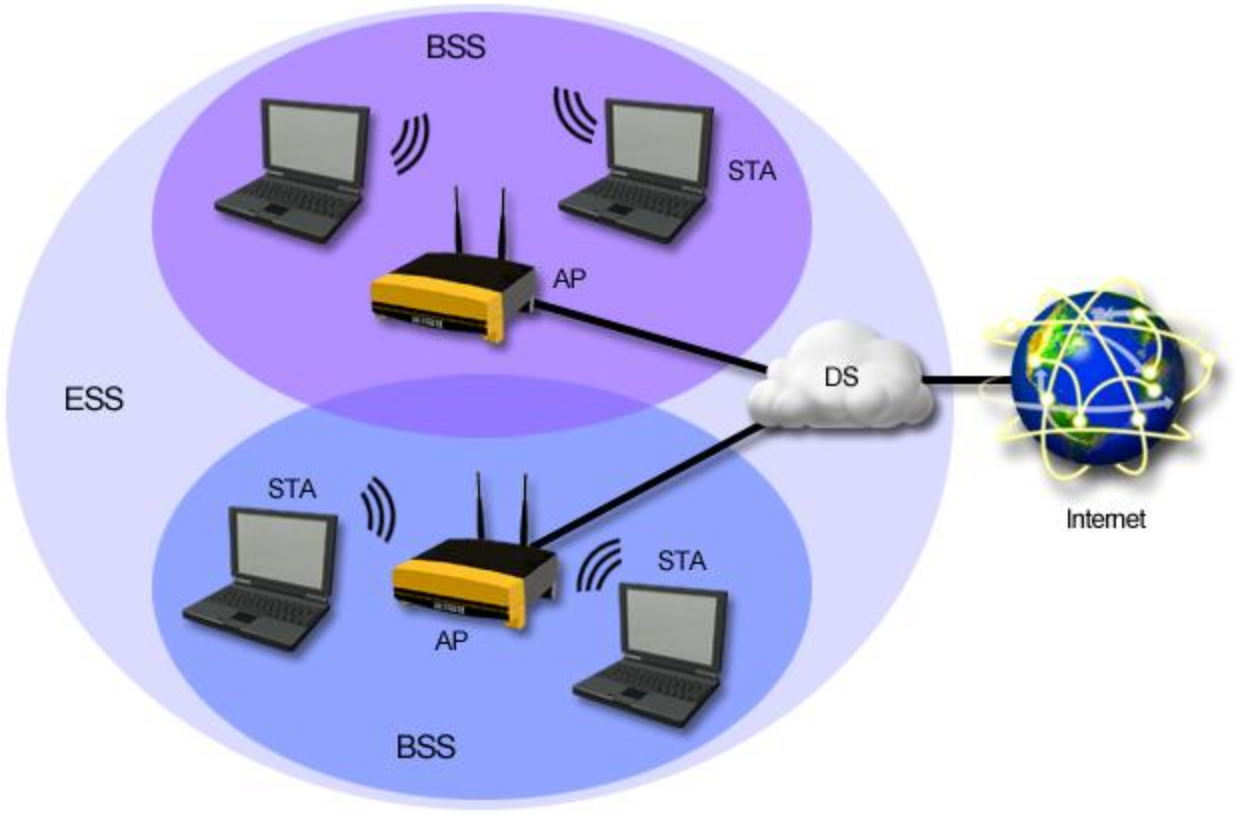
The following table describes details of a wireless networking architecture.

Characteristic	Description	
Signaling Method	Frequency Hopping Spread Spectrum (FHSS)	FHSS uses a narrow frequency band and 'hops' data signals in a predictable sequence from frequency to frequency over a wide band of frequencies. • Because FHSS shifts automatically between frequencies, it can avoid interference that may be on a single frequency. • Hopping between frequencies also increases transmission security by making eavesdropping and data capture more difficult.
	Direct-Sequence Spread Spectrum (DSSS)	The transmitter breaks data into pieces and sends the pieces across multiple frequencies in a defined range. DSSS is more susceptible to interference and less secure then FHSS.
Topology	Ad hoc	An *ad hoc* network works in peer-to-peer mode. The wireless NICs in each host communicate directly with one another. An ad hoc network: • Works in peer-to-peer mode without an access point (the wireless NICs in each host communicate directly with one another). • Uses a physical mesh topology with a logical bus topology. • Is cheap and easy to set up. • Cannot handle a large number of hosts. • Requires special modifications to reach wired networks. You will typically only use an ad hoc network to create a direct, temporary connection between two hosts.
	Infrastructure	An *infrastructure* wireless network employs an access point (AP) that functions like a hub on an Ethernet network. With an infrastructure network: • The network uses a physical star topology with a logical bus topology. • You can easily add hosts without increasing administrative efforts (scalable). • The access point can be easily connected to a wired network, allowing clients to access both wired and

		wireless hosts. • The placement and configuration of access points require planning to implement effectively. You should implement an infrastructure network for all but the smallest of wireless networks.
Media Access	Wireless networks use Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) to control media access and *avoid* (rather than detect) collisions. Collision avoidance uses the following process: 1. The sending device listens to make sure that no other device is transmitting. If another device is transmitting, the device waits a random period of time (called a *backoff* period) before attempting to send again. 2. If no other device is transmitting, the sending device broadcasts a Request-to-send (RTS) message to the receiver or access point. The RTS includes the source and destination, as well as information on the duration of the requested communication. 3. The receiving device responds with a Clear-to-send (CTS) packet. The CTS also includes the communication duration period. Other devices use the information in the RTS and CTS packets to delay attempting to send until the communication duration period (and subsequent acknowledgement) has passed. 4. The sending device transmits the data. The receiving device responds with an acknowledgement (ACK). If an acknowledgement is not received, the sending device assumes a collision and retransmits the affected packet. 5. After the time interval specified in the RTS and CTS has passed, other devices can start the process again to attempt to transmit. **Note:** Using RTS and CTS (steps 2 and 3 above) is optional and depends on the capabilities of the wireless devices. Without RTS/CTS, collisions are more likely to occur. Wireless communication operates in *half-duplex* (shared, two-way communication). Devices can both send and receive, but not at the same time. Devices must take turns using the transmission channel. Typically, once a party begins receiving a signal, it must wait for the transmitter to stop transmitting before replying.	
Devices	Devices on a wireless network include: • A wireless NIC for sending and receiving signals. • A wireless access point (AP) is the equivalent of an Ethernet hub. The wireless NICs connect to the AP, and the AP manages network communication. • A wireless bridge connects two wireless APs into a single network or connects your wireless AP to a wired network. Most APs today include bridging features. **Note:** Many wireless access points include ports (or hubs, switches, or routers) to connect the wireless network to the wired portion of the network.	

Wireless Infrastructure Facts

The following diagram shows a sample enterprise wireless network operating in infrastructure mode:



The various components of a wireless network are described in the following table.

Component	Description
Station (STA)	An STA is a wireless network card (NIC) in an end device such as a laptop or wireless PDA. STA often refers to the device itself, not just the network card.
Access Point (AP)	An *access point* (AP), sometimes called a *wireless access point*, is the device that coordinates all communications between wireless devices as well as the connection to the wired network. It acts as a hub on the wireless side and a bridge on the wired side. It also synchronizes the stations within a network to minimize collisions.
Basic Service Set (BSS)	A BSS, also called a *cell*, is the smallest unit of a wireless network. All devices in the BSS can communicate with each other. The devices in the BSS depend on the operating mode: • In an ad hoc implementation, each BSS contains two devices that communicate directly with each other. • In an infrastructure implementation, the BSS consists of one AP and all STAs associated with the AP. All devices within the BSS use the same radio frequency channel to communicate.
Independent Basic Service Set (IBSS)	An IBSS is a set of STAs configured in ad hoc mode.
Extended Service Set (ESS)	An ESS consists of multiple BSSs with a distribution system (DS). The graphic above is an example of an ESS. In an ESS, BSSs that have an overlapping transmission

	range use different frequencies.
Distribution System (DS)	The distribution system (DS) is the backbone or LAN that connects multiple APs (and BSSs) together. The DS allows wireless clients to communicate with the wired network and with wireless clients in other cells.

Wireless networks use the following for identification:

Identifier	Description
Service Set Identifier (SSID)	The Service Set Identifier (SSID), also called the network name, groups wireless devices together into the same logical network. • All devices on the same network (within the BSS and ESS) must have the same SSID. • The SSID is a 32-bit value that is inserted into each frame. The SSID is case-sensitive. • The SSID is sometimes called the ESS ID (Extended Service Set ID) or the BSS ID (Basic Service Set ID). In practice, each term means the same thing. **Note:** Using BSS ID to describe the SSID of a BSS is technically incorrect.
Basic Service Set Identifier (BSSID)	The BSSID is a 48-bit value that identifies an AP in an infrastructure network or a STA in an ad hoc network. The BSSID allows devices to find a specific AP within an ESS that has multiple access points, and is used by STAs to keep track of APs when roaming between BSSs. The BSSID is the MAC address of the access point and is set automatically. **Note:** Do not confuse the BSSID with the SSID. They are not the same thing.

Wireless Standards Facts

The original 802.11 specification operated in the 2.4 GHz range and provided up to 2 Mbps. Additional IEEE subcommittees have further refined wireless networking. Three of the most common standards as well as a new standard in draft stage are listed in the following table:

Specification	Standard			
	802.11a	**802.11b**	**802.11g**	**802.11n**
Frequency	5.75 GHz (U-NII)	2.4 GHz (ISM)	2.4 GHz (ISM)	2.4 GHz (ISM) or 5.75 GHz (U-NII)
Maximum speed	54 Mbps	11 Mbps	54 Mbps	600 Mbps
Maximum range	150 Ft.	300 Ft.	300 Ft.	1200 Ft.
Channels (non-overlapped)	23 (12)	11 (3)	11 (3)	2.4 GHz--23 (12 or 6) 5.75 GHz--11 (3 or 1)
Modulation technique	OFDM	DSSS, CCK, DQPSK, DBPSK	DSSS (and others) at lower data rates At higher data rates, OFDM, QPSK, BPSK	OFDM and others, depending on implementation
Backwards-compatibility	N/A	No	With 802.11b	With 802.11a/b/g, depending on implementation

802.11n uses the following technologies to improve the speed or the distance of wireless transmissions:

Technology	Details
Multiple Input Multiple Output (MIMO)	802.11n uses multiple send and receive radios (MIMO). The use of multiple antennas both at the transmitter and receiver improves the performance (stronger signal and increased speed) of radio communication systems. A system is described by the number of sending and receiving radios. The 802.11n specifications allow up to 4 sending and 4 receiving radios. The benefit of adding additional radios declines as the number increases. Going above 3x3 offers little practical return.
Channel bonding	*Channel bonding* combines two non-overlapping 20-MHz channels into a single 40-MHz channel, resulting in slightly more than double the bandwidth. • The 5.75 GHz range has a total of 23 channels, with 12 of those non-overlapping. This allows for a maximum of 6 non-overlapping bonded (combined) channels. • The 2.4 GHz range has a total of 11 channels, with 3 of those non-overlapping. This allows for a maximum of 1 non-overlapping channel. For this reason, channel bonding is typically not practical for the 2.4 GHz range.
Frame composition	802.11n changes the frame composition, resulting in increased efficiency of data transmissions (less overhead).

Be aware of the following regarding the wireless network implementation:

- The actual speed depends on several factors including distance, obstructions (such as walls), and interference.
- The actual maximum distance depends on several factors including obstructions, antenna strength, and interference. For example, for communications in a typical environment (with one or two walls), the actual distance would be roughly half of the maximums.
- The speed of data transmission decreases as the distance between the transmitter and receiver increases. In other words, in practice, you can get the maximum distance or the maximum speed, but not both.
- The ability of newer devices to communicate with older devices depends on the capabilities of the transmit radios in the access point. For example:
    - Some 802.11n devices can transmit at either 2.4 GHz or 5.75 GHz. This means that the radio is capable of transmitting at either frequency. However, a single radio cannot transmit at both frequencies at the same time.
    - Most 802.11g devices can transmit using DSSS, CCK, DQPSK, and DBPSK for backwards compatibility with 802.11b devices. However, the radio cannot transmit using both DSSS and OFDM at the same time.

  This means that when you connect a legacy device to the wireless network, all devices on the network operate at the legacy speed. For example, connecting an 802.11b device to an 802.11n or 802.11g access point slows down the network to 802.11b speeds.

- A *dual band* access point can use one radio to transmit at one frequency, and a different radio to transmit at a different frequency. For example, you can configure many 802.11n devices to use one radio to communicate at 5.75 GHz with 802.11a devices, and the remaining radios to use 2.4 GHz to communicate with 802.11n devices. Dual band 802.11a and 802.11g devices are also available.

- When you configure an access point, some configuration utilities use the term *mixed mode* to designate a network with both 802.11n and non-802.11n clients. In this configuration, one radio transmitter is used for legacy clients, and the remaining radio transmitters are used for 802.11n clients.
- Many 802.11n access points can support clients running other wireless standards (802.11a/b/g). When a mix of clients using different standards are connected, the access point must disable some 802.11n features to be compatible with non-802.11n devices, which decreases the effective speed.
- Some newer 802.11a or 802.11g devices provide up to 108 Mbps using 802.11n pre-draft technologies (MIMO and channel bonding).

Infrared and Bluetooth Facts

Infrared wireless networking employs light waves that are outside of the visible light spectrum. It uses light from three regions:

- The near IR band (the light wave closest to the color red)
- The intermediate (IM) IR band
- The far IR band

Infrared devices can operate in one of two modes:

Method	Description
Line of Sight (LoS)	• Devices must have a direct LoS (line-of-sight) connection. • The maximum distance between devices is 1 meter. • Because of the LoS connection requirement, communication signals are easily interrupted.
Diffuse Mode	• Diffuse mode (also called *scatter mode*) operates by broadcasting a large beam of light rather than a narrow beam. It does not require LOS connections. • Despite its advantages, diffuse mode still operates under range limitations. The IR access point and devices must be in the same room with each other. • Diffuse mode is also subject to signal disruptions (such as from obstructions).

You should know the following facts about wireless IR:

- IR data transfers occur at 4 Mbps.
- IR networks are very insecure because the signals are not encrypted, and they can be easily intercepted.
- A common use for IR in networking is in transferring data between a handheld or notebook computer and a desktop computer.

The Bluetooth standard was designed to allow people to connect in PAN (personal area network) configurations using cell phones, PDAs (personal digital assistants), printers, mice, keyboards and other Bluetooth equipped devices. Bluetooth is a proposed standard of the IEEE 802.15 committee.

Specification	Bluetooth

	(proposed 802.15)
Frequency	2.45 GHz
Speed	Bluetooth 1.0--Up to 1 Mbps (practical rates are about 720 Kbps) Bluetooth 2.0--Up to 3 Mbps (practical rates are about 2 Mbps)
Range	30 Ft.
Signal	FHSS

You should know the following facts about Bluetooth:

- A Bluetooth network uses a master/slave networking mode:
  - One master device controls up to seven slave devices.
  - A PAN can have up to 255 total slave devices.
- Bluetooth uses a 128-bit proprietary encryption mechanism to encrypt its signals.

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 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	With shared secret authentication, clients and access points 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. • With shared key authentication, all access points 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
Wired Equivalent Privacy (WEP)	WEP is an optional component of the 802.11 specifications and was deployed in 1997. WEP was designed to provide wireless connections with the same security as wired connections. WEP has the following weaknesses: • Static Pre-shared Keys (PSK) are configured on the access point and the client and cannot be dynamically changed or exchanged without administration. As a result, every host on large networks usually uses the same key. • Because it doesn't change, the key can be captured and easily broken. The key values are short, making it easy to predict. **Note**: When using WEP, use open authentication. Using shared key authentication with WEP uses the key that is used for encryption for authentication as well. This use exposes the key to additional attacks, making WEP more susceptible to being compromised.
Wi-Fi Protected Access (WPA)	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: • Uses TKIP for encryption. • Supports both Pre-shared Key (referred to as WPA-PSK or WPA Personal) and 802.1x (referred to as WPA Enterprise) authentication. • Can use dynamic keys or pre-shared keys. • Can typically be implemented in WEP-capable devices through a software/firmware update.
Wi-Fi Protected Access 2 (WPA2) or 802.11i	WPA2 is the implementation name for wireless security that 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 eventually replace both WEP and WPA. WPA2: • Uses Advanced Encryption Standard (AES) as the encryption method. It is similar to and more secure than TKIP, but requires special hardware for performing encryption. • Supports both Pre-shared Key (referred to as WPA2-PSK or WPA2 Personal) and 802.1x (referred to as WPA2 Enterprise) authentication. • Can use dynamic keys or pre-shared keys. **Note:** WPA2 has the same advantages over WEP as WPA. While more secure than WPA, its main disadvantage is that it requires new hardware for implementation.

Note: You can also enable IPSec on your wireless connections to provide encryption of data transmissions.

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

Method	Description
Change the administrator account name and password	The access point typically comes configured with a default username and password that is used to configure the access point settings. If possible, it is important to change the administrator account name and password from the defaults. This helps prevent outsiders from breaking into your system by guessing the default username and password.
Change SSID from defaults	Many manufacturers use a default SSID, so it is important to change your SSID from the defaults. You can also disable the SSID broadcast for further protection, this is known as *SSID suppression* or *cloaking*. **Note:** Even with SSID broadcast turned off, a determined hacker can still identify the SSID by analyzing wireless broadcasts.
Update the firmware	Update the firmware on the access point from the manufacturer's Web site frequently to prevent your system from being exposed to known bugs and security holes.
Enable the firewall on the access point	Most wireless access points 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 access points allows only users with a valid, static IP address in the range to connect.
Enable MAC address filtering	Every network board has a unique code assigned to it called a MAC address. By specifying which MAC addresses are allowed to connect to your network, you can prevent unauthorized MAC addresses from connecting to the access point. Configuring a MAC address filtering system is very time consuming and demands upkeep. **Note:** Attackers can still use tools to capture packets and then retrieve valid MAC addresses. An attacker could then spoof their wireless adapter's MAC address and circumvent the filter.

Wireless Configuration Tasks

To set up a wireless network, you need to configure the wireless access points and any wireless network cards. Most APs are configured to work right out of the box. However, you might need to perform some configuration to customize settings or enable security.

- Most APs have at least one wired port that you can use to connect to the AP and perform configuration tasks. Many come with a simple Web interface that you can use to perform initial configuration tasks.
- Depending on the operating system, wireless NICs might be configured automatically, or you might need to install special software (before or after) installing the hardware in the computer. Consult the NIC documentation to identify the necessary installation steps.

You might need to complete the following steps to configure wireless devices on your network.

Task	Description
Set the SSID	The SSID is also commonly referred to as the network name. • All devices on the same network must use the same SSID. • The SSID is case-sensitive. • To provide some level of security, consider using a cryptic name for the SSID. For example, using your name for your home network SSID makes it too easy to identify the network owner and could help hackers gain access.
Configure the region (AP only)	The region identifies the physical area where the AP will operate.
Configure the channel	Most wireless networks can transmit on one of multiple channels. When configuring the channel: • On the AP, accept the default channel or change it to one of your choice. Choose a channel that is not used by any other wireless transmitting devices (such as phones or other access points). • On the NIC, the channel is typically detected automatically and is configured to match the channel used by the AP. On some NICs you can also set the channel to a specific channel. When doing so, use the same channel on which the WAP transmits. Many access points can detect channels used in the area and automatically configure themselves with a channel that does not overlap with other channels used in the area.

Configure security	Many APs can be plugged in and start working immediately to enable a simple wireless LAN. However, this also means that the AP is not configured for security. At a minimum, you should enable some form of security or encryption on the AP and each wireless NIC. Following is a list of some common security features:
	
	• MAC access list. Some APs can restrict wireless access to specific MAC addresses. Only devices whose MAC addresses are identified will be allowed to access the WAP.
	• Disable SSID broadcast. By disabling the SSID broadcast, wireless devices must be statically configured with the SSID before they can connect because they will be unable to dynamically detect the SSID.
	• Configure the security protocol:
	  ○ For WEP, configure keys manually or use a passphrase to generate the keys (the passphrase *is* case-sensitive).
	  ○ For WPA or WPA2, configure the passphrase (the passphrase *is* case sensitive).
	
	Note: You cannot use both WEP and WPA at the same time.
	
	When configuring encryption, select the strongest method supported by all devices:
	
	• AES is used with WPA2. When using AES, all devices must be WPA2 capable.
	• TKIP is used with WPA. Most existing devices can use WPA. If not, check to see if a firmware update is available to add WPA capabilities to the device.

	• Use WEP only if no other encryption is supported. **Note:** Do not use WEP together with shared key authentication. • Public networks typically require no encryption.
Configure the beacon	A *beacon* is a frame that is sent out periodically by the access point. The beacon announces the access point and the characteristics of the network (such as the SSID, supported speeds, and the signaling method used). • When you turn off SSID broadcast, you prevent the access point from including the SSID in the beacon. • Wireless clients listen for beacons to identify access points in the area. • The beacon is sent at periodic intervals (typically 100 ms by default). • Sending the beacon uses some of the available bandwidth of the wireless network. You can reduce the traffic generated by the beacon by increasing the beacon interval. • Increasing the beacon interval can increase the time it takes wireless clients to locate the wireless network. To improve access times, decrease the beacon interval.

Wireless Network Considerations

Regardless of the type of wireless networking you are using, the actual transmission speed will likely be less than the rated speed. This is because various factors cause a degradation of the signal. If a single connection drops below 2 Mbps, the connection could be terminated. If you are having trouble establishing or keeping a wireless connection, consider the following factors.

Consideration	Description
Incorrect configuration	Probably the most common source of problems with wireless networking is incorrect configuration. Before considering other problems, verify that the correct SSID and WEP/WPA keys have been configured. Remember that WEP/WPA keys are not case-sensitive, but passphrases are case-sensitive. A similar form of an incorrect configuration is trying to access a wireless network that uses one standard (for example 802.11a) with a wireless card that only supports a different standard (802.11b or 802.11g).
Range and obstructions	Wireless standards have a limited range. Moving a notebook outside of the effective range will weaken the signal and likely cause intermittent reception while moving outside of the stated range can cause it to be completely dropped. In addition, many wireless devices have trouble transmitting through obstructions in the path. Infrared requires a line-of-sight path, while radio frequency wireless has trouble transmitting through certain materials such as concrete.
Channel interference	The 2.4 GHz frequency range is divided into 11 channels, with each channel having some overlap with the channels next to it. You might experience problems with your wireless network when other devices are trying to use the same or adjacent channels. Devices that use RF wireless include: • Cordless telephones that operate in the 2.4 GHz range. 900 MHz cordless phones do not cause interference.

	• Other access points in the area (for example, each of your neighbors might have a wireless network, with each configured to use a similar channel). To avoid interference, try changing the channel used on the access point. If the area has different wireless networks, configure each with a different channel with at least two channels separating the channels in use (for example you can use channels 1, 6, and 11).
Atmospheric and EMI conditions	Interference from atmospheric conditions such as weather or other sources of stray radio waves (electro-magnetic interference) can degrade the signal and cause service interruptions.
AP placement	The location of the AP can affect signal strength and network access. Keep in mind the following recommendations: • Place APs in central locations. Radio waves are broadcast in each direction, so the AP should be located in the middle of the area that needs network access. • Devices often get better reception from APs that are above or below. • In general, place APs higher up to avoid interference problems caused by going through building foundations. • For security reasons, do not place APs near outside walls. The signal will extend outside beyond the walls. Placing the AP in the center of the building decreases the range of the signals available outside of the building. • Overlapping wireless networks should use different channels to ensure that they do not conflict with each other.

Antennae orientation	For radio frequency wireless devices, the antenna orientation might have a small effect on signal strength. There are two types of antennas you should be aware of:
	
	• Directional antenna:
	  ○ Creates a narrow, focused signal in a particular direction.
	  ○ Focused signal provides greater signal strength increasing the transmission distance.
	  ○ Provides a stronger point-to-point connection, better equipping them to handle obstacles.
	• Omni-directional antenna:
	  ○ Disperses the RF wave in an equal 360-degree pattern.
	  ○ Used to provide access to many clients in a radius.
	
	For other devices such as infrared or satellite, the orientation of the receiving device is critical. For these types of devices, make sure the receivers have a line-of-sight path to communicate.