Installing WLAN Networks

by Sophia

WHAT'S COVERED

In this lesson, you will learn about what is involved with wireless network installation.

Specifically, this lesson will cover the following:

1. WLAN Installation

Let's say you just bought a wireless access point (AP) for your laptop to use to connect to the internet. What's next? That all depends on the type of installation you want to create with your new hardware.

KEY CONCEPT

It is important you understand where to place the AP. For example, you don't want to place the AP on or near a metal filing cabinet, a thick wall, or other obstructions. Once you decide on the AP's placement, you can configure your wireless network.

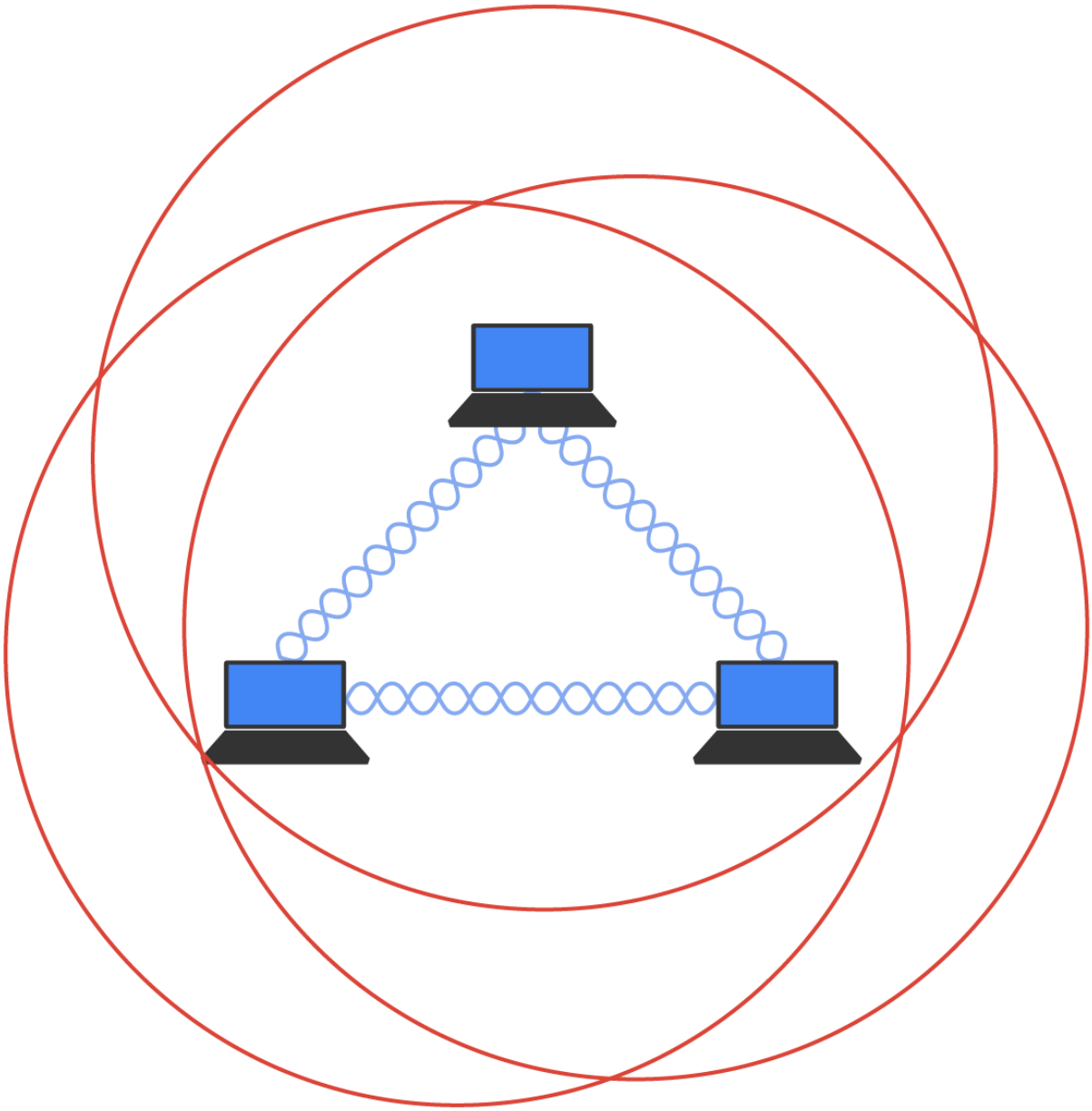
There are two main installation types: ad hoc and infrastructure mode. Each 802.11 wireless network device can be installed in one of these two modes, which are also referred to as **service sets**.

1a. Ad Hoc Mode: Independent Basic Service Set

This is a simple method to install wireless 802.11 devices. In this mode, the wireless NICs can communicate directly without the need for an AP.

EXAMPLE Two laptops have wireless NICs installed. If both cards are set up to operate in ad hoc mode, they can connect and transfer files as long as the other network settings, like protocols, are set up to enable this as well. We'll also call this an **independent basic service set (IBSS)**, which is created as soon as two wireless devices communicate.

The diagram below shows an example of an **ad hoc wireless network**. Note the absence of an AP.



An ad hoc network would not scale well and really is not recommended because of collision and organization issues. With the low costs of APs, this type of network is just not needed today.

TERM TO KNOW

Independent Basic Service Set (IBSS)

A service set with no access point where wireless devices connect directly to each other.

Ad Hoc Wireless Network

A device-to-device network independent of a built network structure that uses routers or access points.

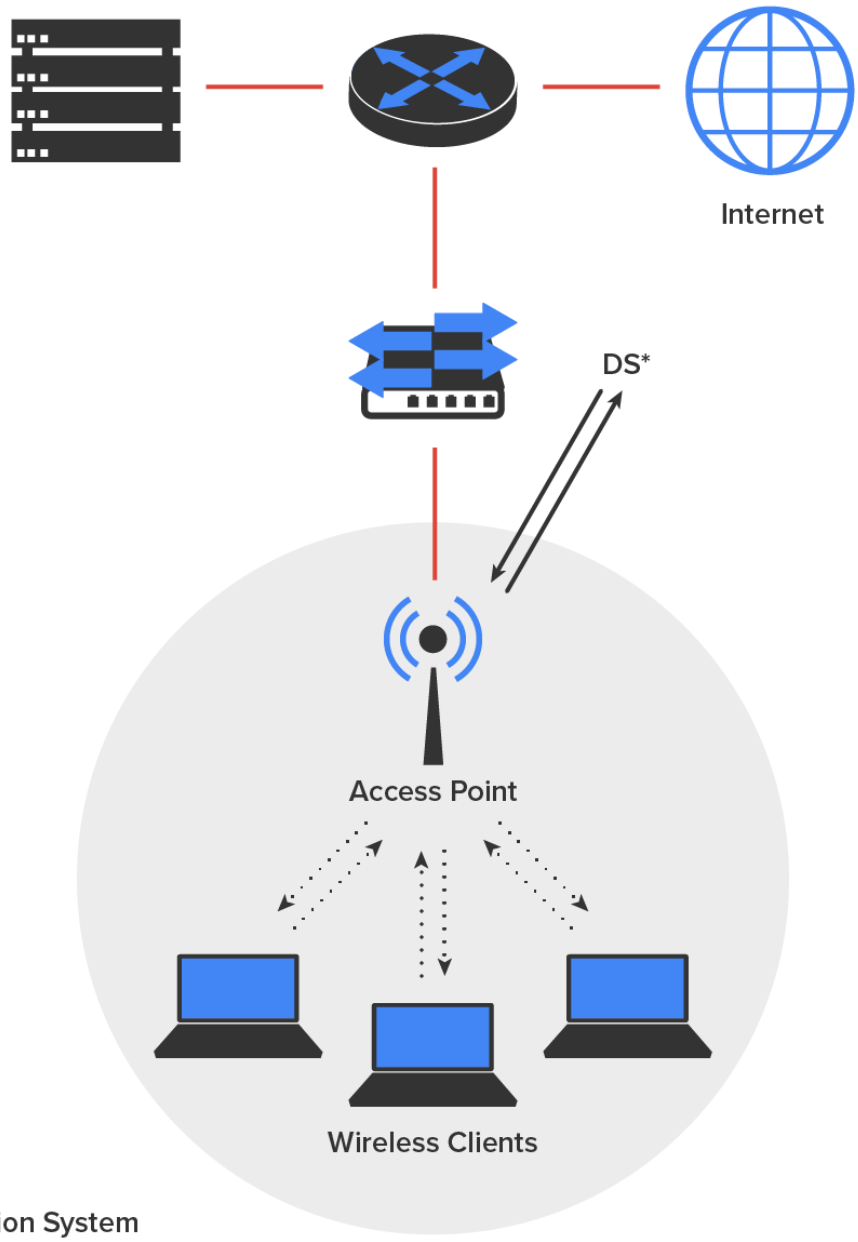
1b. Infrastructure Mode

The most common use of wireless networking equipment is to give us the wireless equivalent of a wired network. To do this, all 802.11 wireless equipment has the ability to operate in what's known as infrastructure mode, also referred to as a **basic service set (BSS)**, which is provided by an AP.

KEY CONCEPT

In **infrastructure mode**, NICs communicate only with an AP instead of directly with each other, as they do when they're in ad hoc mode. All communication between hosts, plus communication with any wired portion of the network, must go through the AP. A really important fact to remember is that in this mode, wireless clients actually appear to the rest of the network as though they were standard, wired hosts.

The figure below shows a typical infrastructure mode wireless network. Pay special attention to the AP and the fact that it's also connected to the wired network. This connection from the AP to the wired network is called the **distribution system (DS)** and is referred to as wireless bridging.



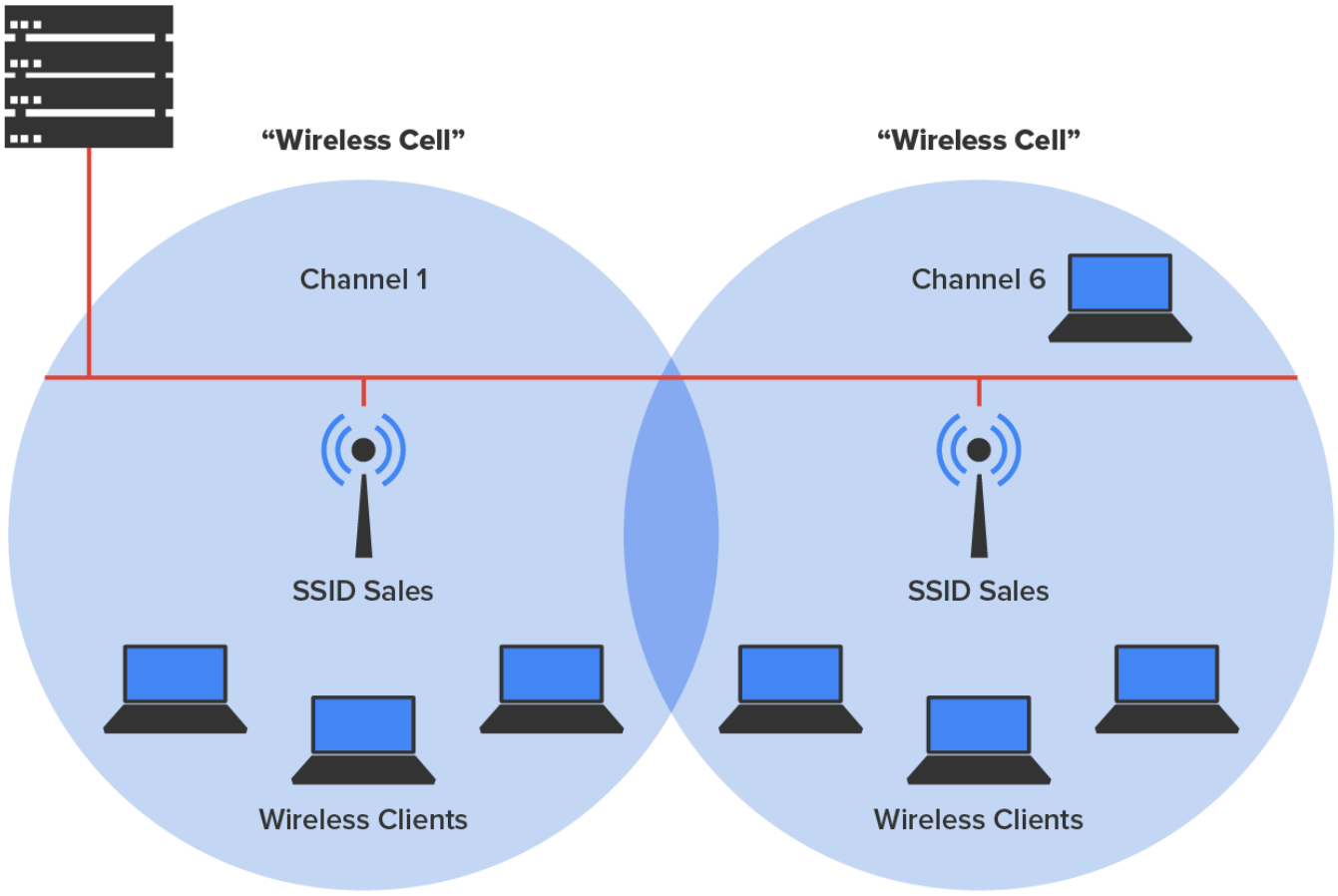
*DS = Distribution System

When you configure a client to operate in wireless infrastructure mode, you need to understand SSID and security.

KEY CONCEPT

The service set identifier (SSID) refers to the unique 32-character identifier that represents a particular wireless network and defines the basic service set. Oh, and by the way, a lot of people use the terms SSID and BSS interchangeably, so don't let that confuse you! All devices involved in a particular wireless network must be configured with the same SSID.

If you set all your APs to the same SSID, mobile wireless clients can roam around freely within the same network. Doing this creates an **extended service set (ESS)** and provides more coverage than a single AP. The diagram below shows two APs configured with the same SSID in an office, thereby creating the ESS network.



For users to be able to roam throughout the wireless network—from AP to AP without losing their connection to the network—all AP signal areas must overlap by 10% of their signal or more.

HINT

To make this happen, be sure the channels on each AP are set differently. And remember, in an 802.11b/g network, there are only three nonoverlapping channels (1, 6, 11), so careful design is important.

TERMS TO KNOW

Basic Service Set (BSS)

A subgroup, within a service set, of devices that share physical-layer medium access.

Infrastructure Mode

A mode in which NICs communicate only with an access point.

Distribution System (DS)

The connection from a wireless network to a wired network.

Extended Service Set (ESS)

A wireless network created by multiple access points that appears to users as a single, seamless network, such as a network covering an area that is too large for reliable coverage by a single access

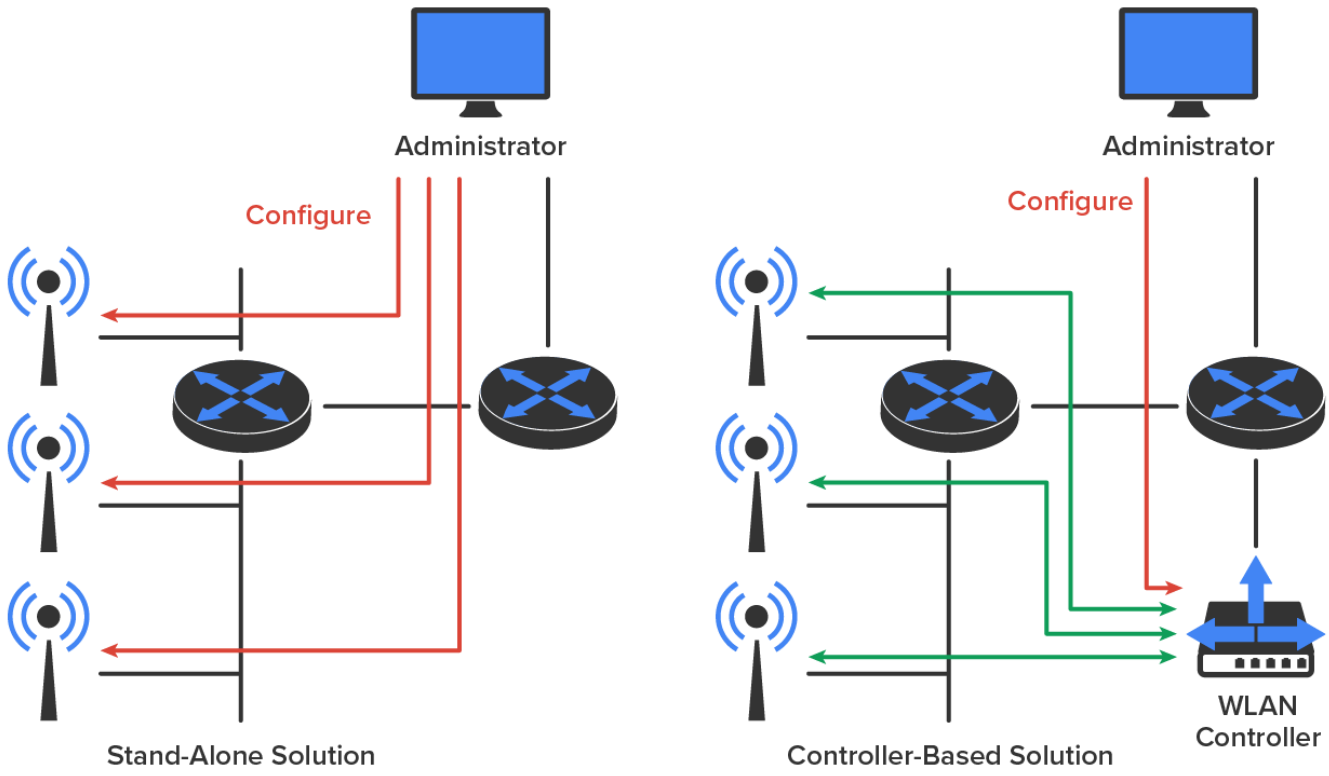
point.

1c. Wireless Controllers

Every wireless enterprise manufacturer has a **wireless controller** to manage the APs in the network.

The diagram below illustrates the difference between stand-alone APs and the controller solution. In a stand-alone solution, all the APs have a full operating system loaded and running, and each must be managed separately.

In a controller-based system, the APs are what we refer to as lightweight, meaning they do not have a full operating system running on them. The controller and AP split duties, which is a solution known as split MAC. APs running with a controller are referred to as lightweight, but you'll also come across the term "thin" AP, whereas you'll come across the term "thick" in reference to APs that run a full OS.



In the diagram above, you can also see that the administrator doesn't manage each AP independently when using the WLAN controller solution. Instead, the administrator configures the controller, which in turn pushes out the configuration needed for each AP. Controllers allow us to design and implement larger enterprise wireless networks efficiently.

KEY CONCEPT

Wireless controllers and APs typically use an open protocol called **Control and Provisioning of Wireless Access Points (CAPWAP)** to communicate with each other. CAPWAP is the standard that most controller manufacturers use today.

TERMS TO KNOW

Wireless Controller

A device that manages multiple wireless network access points as a group.

Control and Provisioning of Wireless Access Points (CAPWAP)

A networking protocol that enables a central wireless controller to manage a set of wireless access points.

1d. Mobile Hotspots

Let us say you're in a location that does not have an AP installed, or they want to charge you for access, and you want to connect your laptop, tablet, or even play a game. What can you do?

You have a couple of options, but they all include the cellular network as an infrastructure. The illustration below shows a mobile hotspot device that connects your laptop, tablet, media devices, or even a gaming device to the internet at decent speeds. Pretty much all cellular vendors sell a version of these hotspots now.

However, if you do not want to carry yet another device around with you and you just want to use your smartphone instead, the illustration below shows how an iPhone can be used as an AP.

2. Signal Degradation

When installing a wireless network, it is important to consider **signal degradation**. Because the 802.11 wireless protocols use radio frequencies, the signal strength varies according to many factors. The weaker the signal, the less reliable the network connection, and so the less usable it will be as well.

There are several key factors that affect signal strength:

- The farther away from the WAP you get, the weaker the signal you get. Most APs have a range of fewer than 100 m. You can extend this range to some degree using amplifiers or repeaters or even by using different antennas.
- The more walls and other office barriers a wireless signal has to pass through, the more attenuated (reduced) the signal becomes. Also, the thicker the wall, the more it interrupts the signal. So, in an indoor office area with lots of walls, the range of your wireless network could be as low as 25 ft! You really have to be careful where you place your APs!

- The various wireless 802.11 protocols have different maximum ranges. The maximum effective range varies quite a bit depending on the 802.11 protocol used. For example, if you have a client running the 802.11ax protocol but it connects to an AP running only the 802.11n protocol, you'll get a throughput of only 600 Mbps to the client.
- The final factor that affects wireless performance is outside interference. Because 802.11 wireless protocols operate in the 900 MHz, 2.4 GHz, and 5 GHz ranges, interference can come from many sources. These include wireless devices like Bluetooth, cordless telephones, cell phones, microwave ovens, other wireless LANs, and any other device that transmits a radio frequency (RF) near the frequency bands that 802.11 protocols use.

TERM TO KNOW

Signal Degradation

A reduction in the quality of an analog or digital signal.

3. Other Wireless Network Infrastructure Implementations

We've discussed the wireless LANs (WLANs) created by installing APs, but there are other technologies like personal area networks (PANs) that create wireless infrastructures too. By far, the best-known technology is the ever-popular Bluetooth,

KEY CONCEPT

Bluetooth operates in the 2.4 GHz range, so while it can cause some interference with 802.11b/g, it's really low power. Plus, the electronics in our WLANs are much better today than they were in the past, so it really isn't much of an issue anymore, and so at last, modern wireless communication works nicely for us today, enabling the mobility that users find so convenient.

To delve a little deeper into wireless technologies, the idea of PANs is to allow personal items such as keyboards, mice, and phones to communicate to our PC/laptop/display/TV wirelessly instead of having to use any wires at all over short distances of up to 10 m (about 30 ft). Bluetooth really has helped us out tremendously in our offices and especially in our cars!

There are two other network infrastructure implementations in the PAN area: infrared and near-field communication.

Infrared (IR) can be used to communicate short range with our devices, like Bluetooth-enabled ones, but it isn't really as popular as Bluetooth in terms of being used within network infrastructures. Unlike Wi-Fi and Bluetooth, infrared wireless signals cannot penetrate walls and only work line-of-sight. Lastly, the rates are super slow, and most transfers only operate from 115 Kbps up to 4 Mbps. These could include older models of remote controls.

Near-field communication (NFC) can be used for wireless communication between devices like smartphones and/or tablets, but you need to be very near the device transmitting the RF to pick up the signal. A solid

example would be when you touch a credit card to a merchant terminal that has an NFC card reader.

HINT

For NFC to work, the actual antenna must be smaller than the wavelength on both the transmitter and receiver. For instance, if you look at a 2.4 GHz or 5 GHz antenna, they are the exact length of one wavelength for that specific frequency. With NFC, the antenna is about one-quarter the size of the wavelength, which means that the antenna can create either an electric field or a magnetic field, but not an electromagnetic field.

TERMS TO KNOW

Bluetooth
A technical specification for wireless personal area networks.

Infrared (IR)
The electromagnetic radiation of a wavelength longer than visible light, but shorter than microwave radiation, having a wavelength between 700 nm and 1 mm.

Near-Field Communication (NFC)
Communication over very short distances, such as by contact or near contact of electronic devices.

SUMMARY

In this lesson, you learned about the types of **wireless network installation**, including **ad hoc mode**, **infrastructure mode**, **wireless controllers**, and **mobile hotspots**. We also considered some causes of **signal degradation** and its impact on performance. We introduced **other wireless network infrastructure implementations**, including Bluetooth, infrared, and near-field communications.

Source: This content and supplemental material has been adapted from CompTIA Network+ Study Guide: Exam N10-007, 4th Edition. Source **Lammle: CompTIA Network+ Study Guide: Exam N10-007, 4th Edition - Instructor Companion Site (wiley.com)**

TERMS TO KNOW

Ad Hoc Wireless Network
A device-to-device network independent of a built network structure that uses routers or access points.

Basic Service Set (BSS)
A subgroup, within a service set, of devices that share physical-layer medium access.

Bluetooth
A technical specification for wireless personal area networks.

Control and Provisioning of Wireless Access Points (CAPWAP)

A networking protocol that enables a central wireless controller to manage a set of wireless access points.

Distribution System (DS)

The connection from a wireless network to a wired network.

Extended Service Set (ESS)

A wireless network created by multiple access points that appears to users as a single, seamless network, such as a network covering an area that is too large for reliable coverage by a single access point.

Independent Basic Service Set (IBSS)

A service set with no access point where wireless devices connect directly to each other.

Infrared (IR)

The electromagnetic radiation of a wavelength longer than visible light, but shorter than microwave radiation, having a wavelength between 700 nm and 1 mm.

Infrastructure Mode

A mode in which NICs communicate only with an access point.

Near-Field Communication (NFC)

Communication over very short distances, such as by contact or near contact of electronic devices.

Service Set

A group of wireless network devices that share a service set identifier (SSID).

Signal Degradation

A reduction in the quality of an analog or digital signal.

Wireless Controller

A device that manages multiple wireless network access points as a group.