Site Survey and Installation Configurations

by Sophia

WHAT'S COVERED

In this lesson, you will learn about how to conduct a pre-installation site survey.

Specifically, this lesson will cover the following:

1. Site Survey
   - 1a. Information Gathering
   - 1b. Providing Capacity
   - 1c. Multiple Floors
   - 1d. Site Survey Tools
2. Installing and Configuring WLAN Hardware
   - 2a. NIC Configuration
   - 2b. AP Configuration
   - 2c. Wireless Security Basics

1. Site Survey

Site surveys are absolutely imperative to designing a premium-quality, or even just a reasonably viable, enterprise wireless network. You should carry out a predeployment survey and a postdeployment survey, but keep in mind that your predeployment survey is not actually your first step to begin this key process.

Because it is vital to know how to formulate and implement a solid site survey, we are going to walk through executing the three major steps to doing that effectively. And just to be really thorough, we are also going to cover some issues commonly encountered as we progress through these steps.

TERM TO KNOW

Site Surveys

The process of planning and designing a wireless network.

1a. Information Gathering

☆ BIG IDEA

This is the first step. During this stage, you must determine three key factors:

- The scope of the network, including all applications that will be used, the data types that will be present, and how sensitive these data types are to delay
- The areas that must be covered and the expected capacity at each location
- The types of wireless devices that will need to be supported, such as laptops, iPads/iPhones, IP phones, and barcode readers

During this phase, a key goal is to create a coverage model that maps to all areas that need coverage, along with those that do not, and have the client sign off in agreement with this document before doing anything else.

KEY CONCEPT

In the predeployment survey phase, we use live APs to verify the optimal distances between their prospective locations. We base this placement on the expected speed at the edge of the cell, the anticipated number of devices, and other information gathered. Usually, after we get one AP positioned, we will place the next one based on the distance from the first, with special consideration given to any sources of interference we have found.

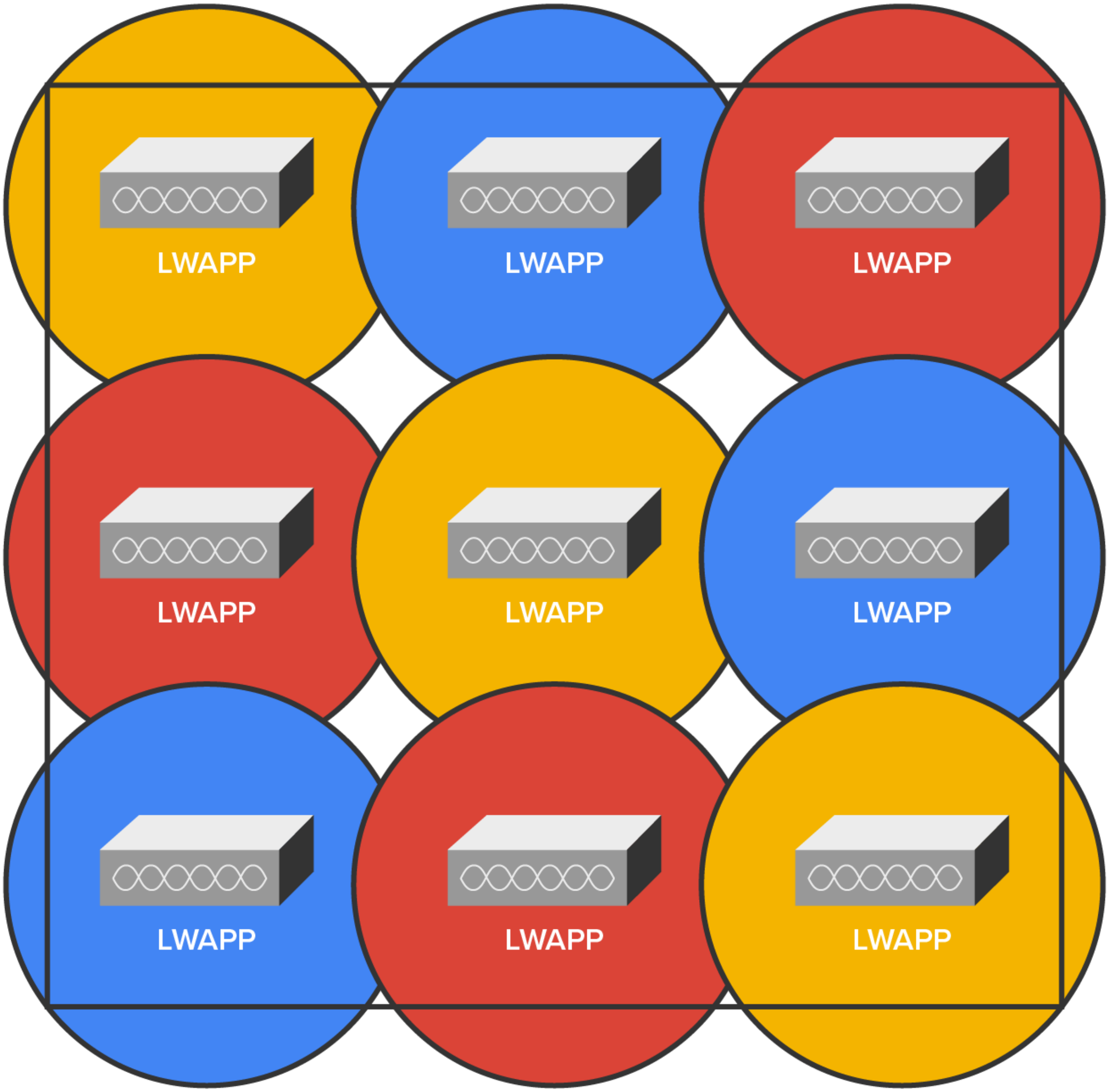
HINT

We utilize the postdeployment survey phase to confirm and verify that the original design and placements are functioning well and are free of problems when all stations are using the network. This rarely happens, so at this point, it is likely that changes will need to be made in order to optimize the performance of a WLAN operating under full capacity.

1b. Providing Capacity

It can be challenging to provide enough capacity in areas where many wireless stations will be competing for airwaves. Remember that stations share access to the RF environment with all other stations in the BSS, as well as with the AP, so really, the only way to increase capacity is by increasing the number of APs in an area requiring serious density.

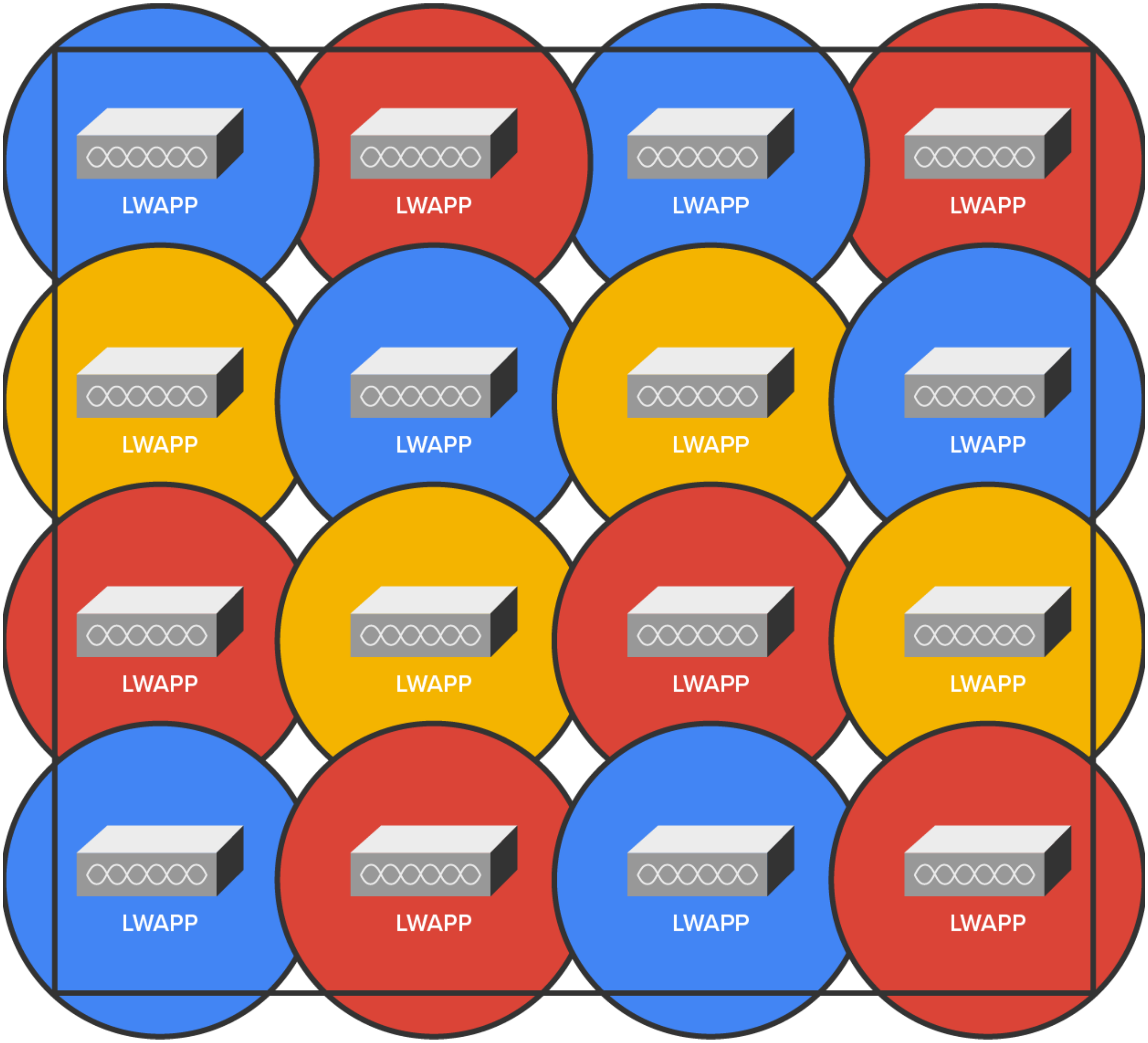
➦ EXAMPLE This can get complicated but, basically, it comes down to placing APs on nonoverlapping channels while still sharing the same SSID. The image below demonstrates this:



In the diagram above of a Lightweight Access Point Protocol (LWAPP), the nine APs have been configured in the same area using the three nonoverlapping channels in the 2.4 GHz frequency (1, 6, and 11). Each shade represents a different channel. Even though the APs on the same channel have been positioned far enough away from one another so that they don't overlap much and/or cause interference, surprisingly, it is actually better if there is some overlap. But bear in mind that the channels should be used in a way such that no APs on the same channel overlap in a detrimental way.

Another thing to note that is not ideal about this arrangement is that all the APs would have to run at full power. This is generally not a good way to design a WLAN because it does not provide much fault tolerance.

There are two problems with this design: lack of overlap and lack of fault tolerance. To address both issues, you need more APs, which would get you more channels and provide better throughput, as shown below.



HINT

A key benefit to this design is that it would also gain the critical ability to run the APs at less than full power. This allows the controller to strategically boost the power of specific APs in the event of an AP outage in a given area.

When you know exactly the type of applications and activity a WLAN will need to support, you can then determine the data rate that must be attained in a particular area. Since **received signal strength indicator (RSSI)**, **signal-to-noise ratio (SNR)**, and data rate are correlated, the required data rate will tell you what the required RSSI or SNR should be, as seen at the AP from the stations. Keep in mind that stations located at the edge of the cell will automatically drop the data rate and that the data rate will increase as a station moves toward the AP.

TERMS TO KNOW

Received Signal Strength Indicator (RSSI)

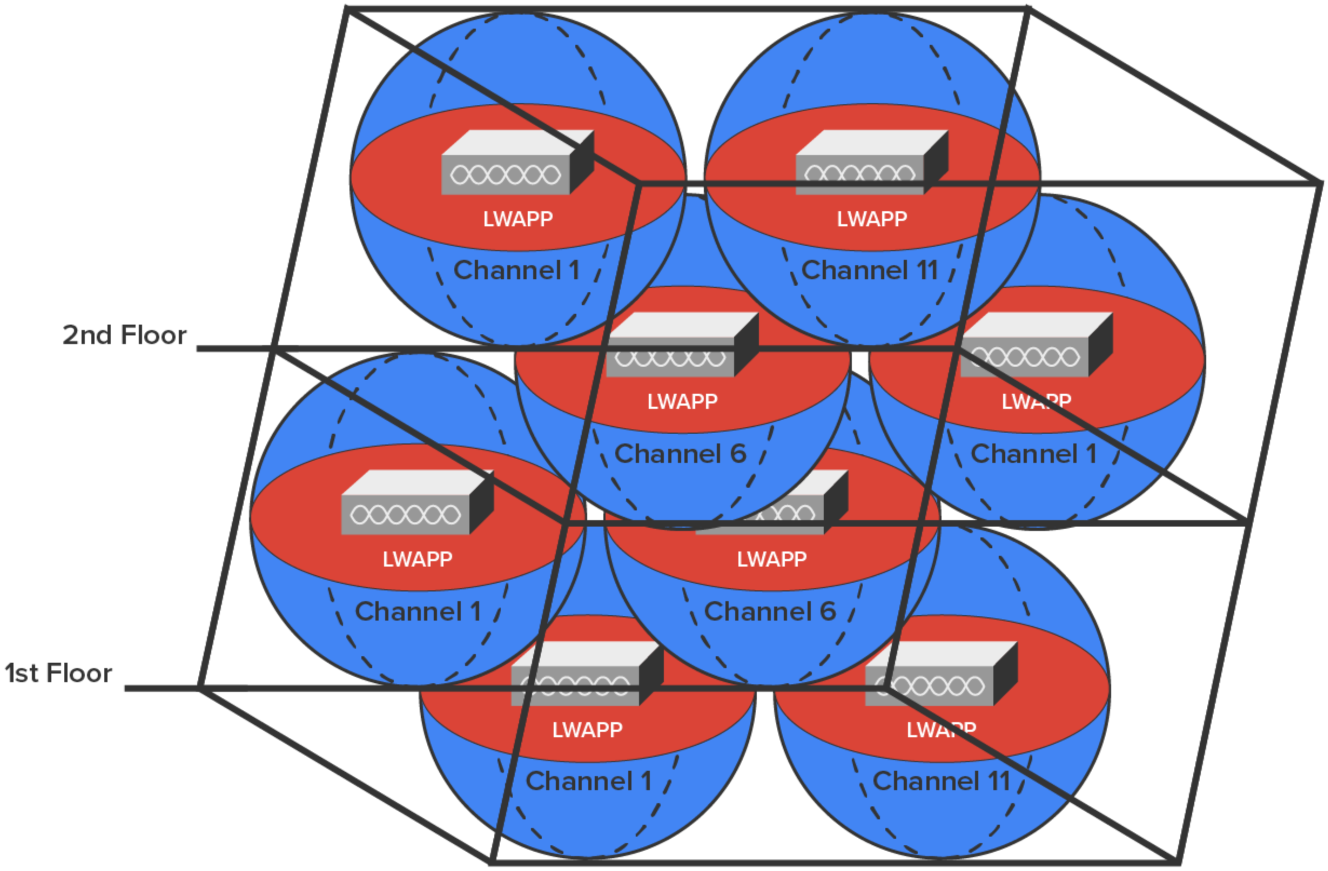
A measure of the energy observed by an antenna when receiving a signal.

Signal-to-Noise Ratio (SNR)

A ratio comparing signal power to noise power.

1c. Multiple Floors

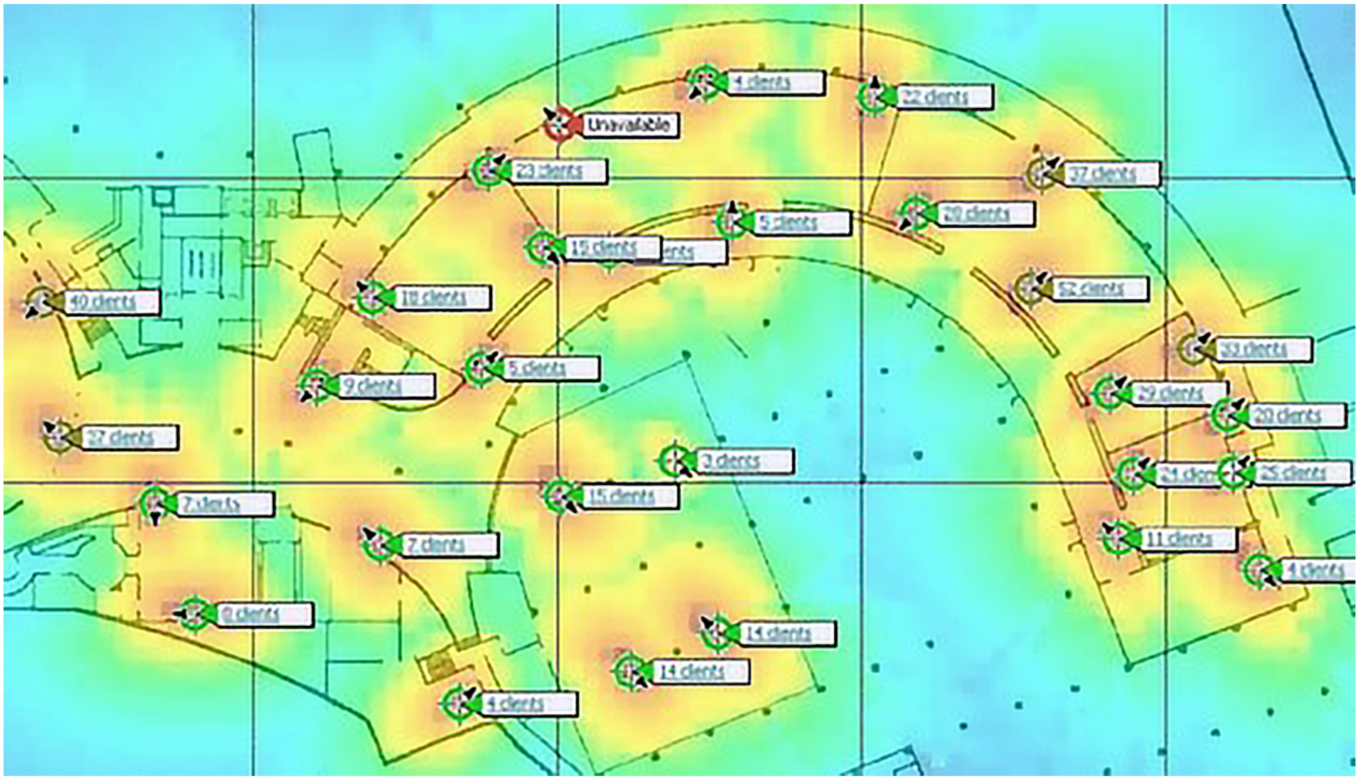
Another special challenge is found in a multistory building where WLANs are located on all floors. In these conditions, you have to think about channel usage in a three-dimensional way, and you may need to coordinate with the other administrators of different WLANs to make this work well. Facing this scenario, your channel spacing should be deployed as shown below.



1d. Site Survey Tools

As we touched upon at the beginning of our site survey section, there are some highly specialized site survey tools that can help you achieve your goals. The AirMagnet Survey and Ekahau Site Survey tools make it possible to do a client walk-through with the unit running, and you can click each location on the map.

These tools will gather RSSI and SNR from each AP in the range, and at the end of your tour, global heat map coverage will be magically displayed, as shown below.



2. Installing and Configuring WLAN Hardware

It is fairly simple to install 802.11 equipment. There are only two main types of components in 802.11 networks: APs and NICs. Wireless NIC installation is just like installing any other network card; however, at present, most (if not all) laptops have wireless cards preinstalled. And just as with connecting an Ethernet card to a LAN switch, you need the wireless network card to connect to an AP.

The AP installation can be fairly simple as well. Take it out of the box, connect the antenna(s) if necessary, connect the power, and then place the AP where it can reach the highest number of clients. This last part is probably the trickiest, but it really just involves a little common sense and maybe a bit of trial and error.

KEY CONCEPT

Knowing that walls obstruct the signal means that putting the AP out in the open typically works better. An AP should be placed away from sources of RF interference, so putting it next to the microwave or a phone system is probably a really bad idea too. Just experiment and move your AP around to find the spot that gives you the best signal strength for all the clients that need to use it.

Configuring an AP and a NIC to work together is not as tricky as it sounds. Most wireless equipment is designed to work almost without configuration, so by default, you can pretty much turn things on and start working. The only things you need to configure are customization settings (name, network address, and so on) and security settings, and even though these are not required, it is typically best practice to configure them.

2a. NIC Configuration

Modern Microsoft Windows computers include software to automatically configure a wireless connection, and they do so automatically when you install a wireless NIC, assuming that somehow you have a Windows machine without a wireless NIC installed on the motherboard. And if you have one without a NIC installed, your Windows machine is really old!

2b. AP Configuration

Once you have successfully configured your workstation(s), it is time to move on and configure the AP. There are literally hundreds of different APs out there, and of course, each uses a different method to configure its internal software. The good news is that, for the most part, they all follow the same general patterns.

Out of the box, the AP should come configured with an IP address that's usually something similar to 192.168.1.1. But check the documentation that comes with the AP to be sure. You can just take the AP out of its box, plug it into a power outlet, and connect it to your network, but in order to manage the AP, you've got to configure its IP address scheme to match your network addressing scheme.

KEY CONCEPT

A workstation PC should receive a DHCP address from the AP when you connect, but if you do not get one, start by configuring a workstation on the wired network with an IP address (192.168.1.2 or similar) and subnet mask on the same subnet as the AP's. You should then be able to connect to the AP to begin the configuration process. Usually, you do this via a web browser or with a manufacturer-supplied configuration program. If the workstation that you are trying to connect wirelessly also has an Ethernet port, you can temporarily connect it to the AP via cable. Most APs have at least one jack.

Once you have successfully connected to the AP, you then get to configure its parameters.

KEY CONCEPT

The minimum parameters common to APs that you should configure for your AP to work properly are outlined below. Remember, typically, an AP works right out of the box, but it is unsecure too!

- SSID: User-friendly name for your AP
- AP IP Addresses: For configuring and managing your AP
- Operating Mode: Select between access point or bridging
- Password: To secure your AP
- Wireless Channel: 802.11 wireless networks can operate on different channels to avoid interference.

HINT

Most wireless APs are set to work on a particular channel from the factory and you can change it if other networks in the area are using that channel, but be aware that no particular channel is any more secure than another. Wireless stations do not use channel numbers as the criteria when seeking a connection. They only pay attention to SSIDs!

2c. Wireless Security Basics

Although it is not a requirement, it is best practice to enable security right from the start as soon as you turn on the AP. Commercial APs typically come configured as an open network so that it is easy to log in, whereas enterprise APs come unconfigured and do not work until they are configured.

Wired Equivalent Privacy (WEP) and **Wi-Fi Protected Access (WPA)** allow data to be encrypted before they are sent over the wireless connection, and all configuring entails is to enable this and pick a key to be used for the connections. Simple, easy-to-configure security is certainly worth your time! WPA3, which is the third version of the protocol, is much more secure than WEP, WPA, and WPA2. You'll learn more about wireless security in a future tutorial.

First, you will enter one or more human-readable passphrases called **shared keys**, which are secret passwords that will never be sent over the wire. After entering each one, you will generally click a button to initiate a one-way hash to produce a WEP key of a size related to the number of bits of WEP encryption you want.

HINT

Entering the same passphrase on a wireless client causes the hash (not the passphrase) to be sent from the wireless client to the AP during a connection attempt.

Most configuration utilities enable you to create multiple keys in case you want to grant someone temporary access to the network but still want to keep the primary passphrase a secret. You can just delete the key you enabled to permit temporary access after you don't need it anymore without affecting access by any primary LAN participants.

TERMS TO KNOW

Wired Equivalent Privacy (WEP)

A legacy security algorithm for 802.11 wireless networks.

Wi-Fi Protected Access (WPA)

A wireless encryption standard.

Shared Key

Algorithm for cryptography that use the same cryptographic key for both the encryption of plaintext and the decryption of ciphertext.

SUMMARY

In this lesson, you learned about doing WLAN **site surveys**, including **information gathering**, predeployment surveying, and postdeployment surveying to **provide appropriate capacity** and performance. We discussed how to survey a **multiple-floor** environment and some specific **site survey tools**. We also learned ideas about **installing and configuring WLAN hardware**, including **NIC** and **AP** configuration settings, and explored some **wireless security basics**.

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

Received Signal Strength Indicator (RSSI)

A measure of the energy observed by an antenna when receiving a signal.

Shared Key

Algorithm for cryptography that use the same cryptographic key for both the encryption of plaintext and the decryption of ciphertext.

Signal-to-Noise Ratio (SNR)

A ratio comparing signal power to noise power.

Site Surveys

The process of planning and designing a wireless network.

Wi-Fi Protected Access (WPA)

A wireless encryption standard.

Wired Equivalent Privacy (WEP)

A legacy security algorithm for 802.11 wireless networks.