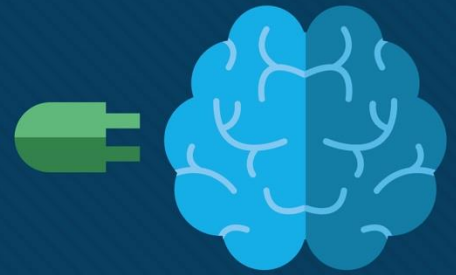

Chapter 19: Understanding Wireless Roam and Location Services

Instructor Materials

CCNP Enterprise: Core Networking

Chapter 19 Content

This chapter covers the following content:

- **Roaming Overview -** This section discusses client mobility from the AP and controller perspectives.
- **Roaming Between Centralized Controllers -** This section explains the mechanisms that allow wireless devices to roam from one AP/controller pair onto another.
- **Locating Devices in a Wireless Network -** This section explains how the components of a wireless network can be used to compute the physical location of wireless devices.

Roaming Overview

- To understand how wireless roaming works, start with simple scenarios such as roaming between access points when no controller is present and when only one controller is present.

Before Roaming Between Autonomous APs

A wireless client must associate and authenticate with an AP before it can use the AP's BSS to access the network. A client can also move from one BSS to another by roaming between APs. The client actively scans channels and sends probe requests to discover candidate APs, and then the client selects one and tries to reassociate with it.

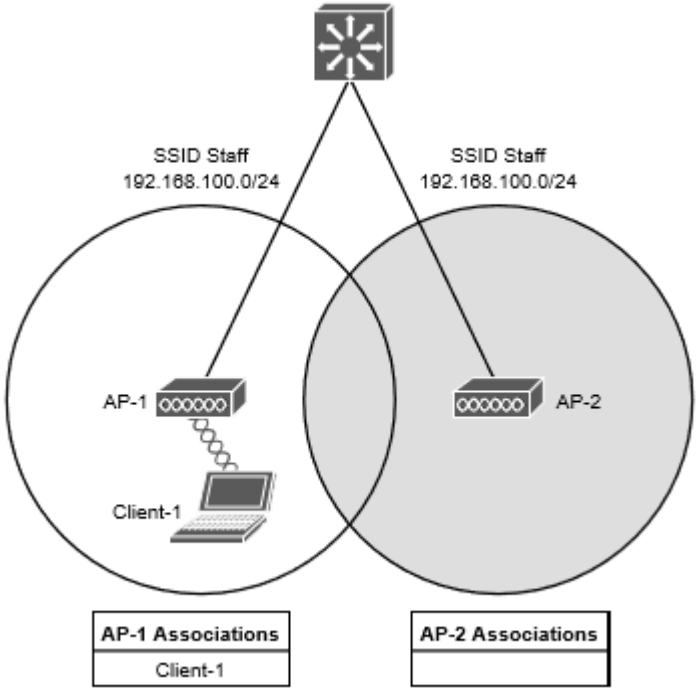

Figure 19-1 *Before Roaming Between Autonomous APs*

After Roaming Between Autonomous APs

The client begins to move into AP 2's cell. Somewhere near the cell boundary, the client decides that the signal from AP 1 has degraded and it should look elsewhere for a stronger signal. The client decides to roam and reassociate with AP 2.

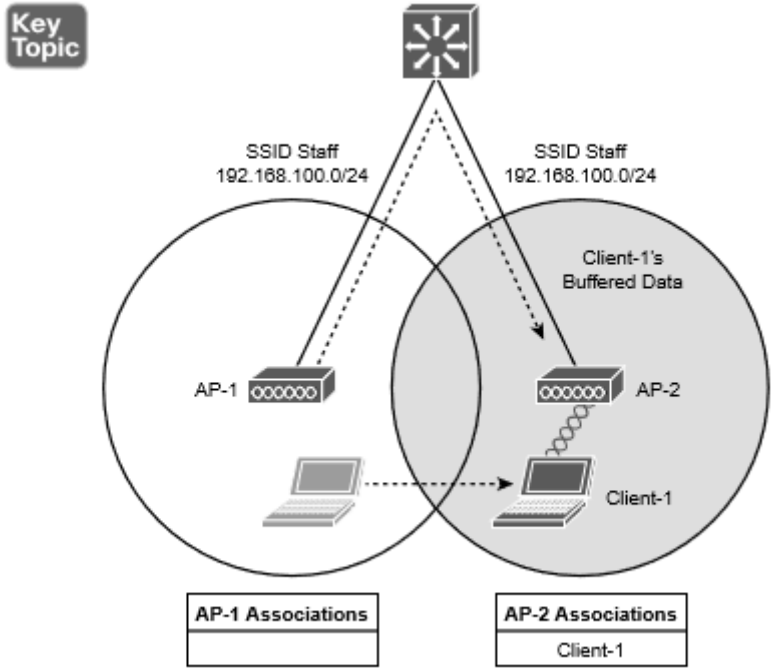

Figure 19-2 *After Roaming Between Autonomous APs*

Successive Roams of a Mobile Client

When a wireless client begins to move, it might move along an arbitrary path. Each time the client decides that the signal from one AP has degraded enough, it attempts to roam to a new, better signal belonging to a different AP and cell. The exact location of each roam depends on the client's roaming algorithm. To illustrate typical roaming activity, each roam in Figure 19-3 is marked with a dark ring.

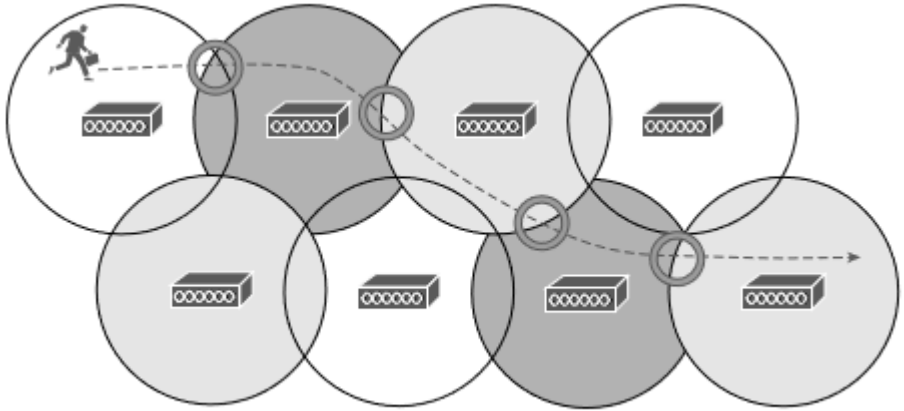

Figure 19-3 *Successive Roams of a Mobile Client*

Intracontroller Roaming

Key Topic

In a Cisco wireless network, lightweight APs are bound to a wireless LAN controller through CAPWAP tunnels. The controller handles the roaming process, rather than the APs, because of the split-MAC architecture.

If both APs involved in a client roam are bound to the same controller, the controller has to update its client association table so that it knows which CAPWAP tunnel to use to reach the client.

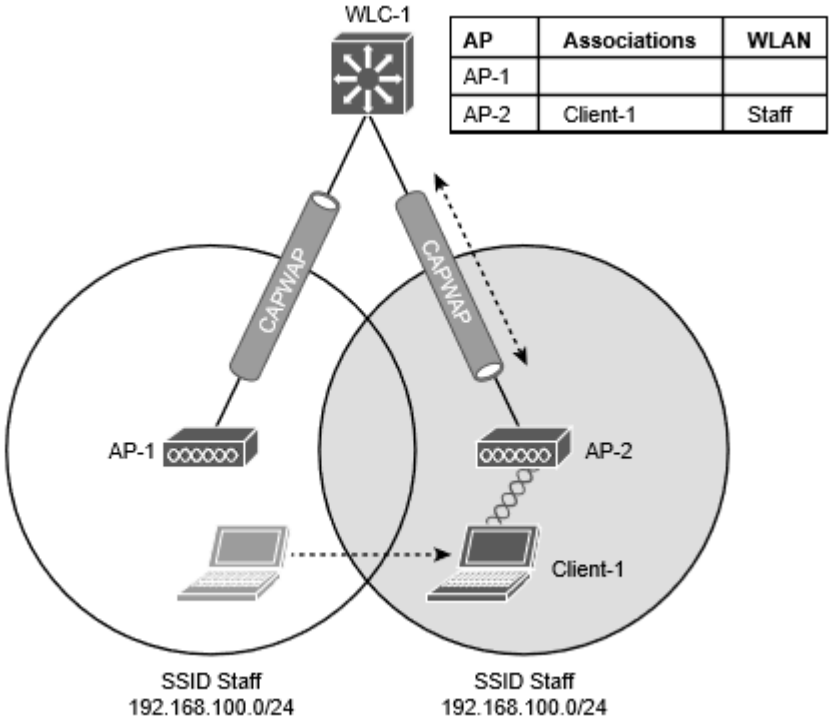

Figure 19-5 *Cisco Wireless Network After an Intracontroller Roam*

Intracontroller Roaming (Cont.)

Efficient roaming is especially important when time-critical applications are being used over the wireless network.

When a roam occurs, there could be a brief time when the client is not fully associated with either AP. So long as that time is held to a minimum, the end user probably will not even notice that the roam occurred.

Along with the client reassociation, a couple other processes can occur:

- **DHCP -** The client may be programmed to renew the DHCP lease on its IP address or to request a new address.
- **Client authentication -** The controller might be configured to use an 802.1x method to authenticate each client on a WLAN.

Cryptographic Key Exchange Techniques

The client authentication process presents a challenge because the dialog between a controller and a RADIUS server, in addition to the cryptographic keys that need to be generated and exchanged, can take a considerable time to accomplish.

Cisco controllers offer three techniques to help streamline this process:

- **Cisco Centralized Key Management (CCKM) -** One controller maintains a database of clients and keys on behalf of its APs and provides them to other controllers and their APs as needed during client roams. CCKM requires Cisco Compatible Extensions (CCX) support from clients.
- **Key caching -** Each client maintains a list of keys used with prior AP associations and presents them as it roams. The destination AP must be present in this list, which is limited to eight AP/key entries.
- **802.11r -** This 802.11 amendment addresses fast roaming or fast BSS transition; a client can cache a portion of the authentication server's key and present that to future APs as it roams. The client can also maintain its QoS parameters as it roams.

Roaming Between Centralized Controllers

- When two or more controllers support the APs in an enterprise, the APs can be distributed across them. As always, when clients become mobile, they roam from one AP to another—except they could also be roaming from one controller to another, depending on how neighboring APs are assigned to the controllers. As a network grows, AP roaming can scale too by organizing controllers into mobility groups.

Before an Intercontroller Roam

When a client roams from one AP to another and those APs lie on two different controllers, the client makes an intercontroller roam.

Figure 19-6 shows a simple scenario prior to a roam. Controller WLC 1 has one association in its database—that of Client 1 on AP 1.

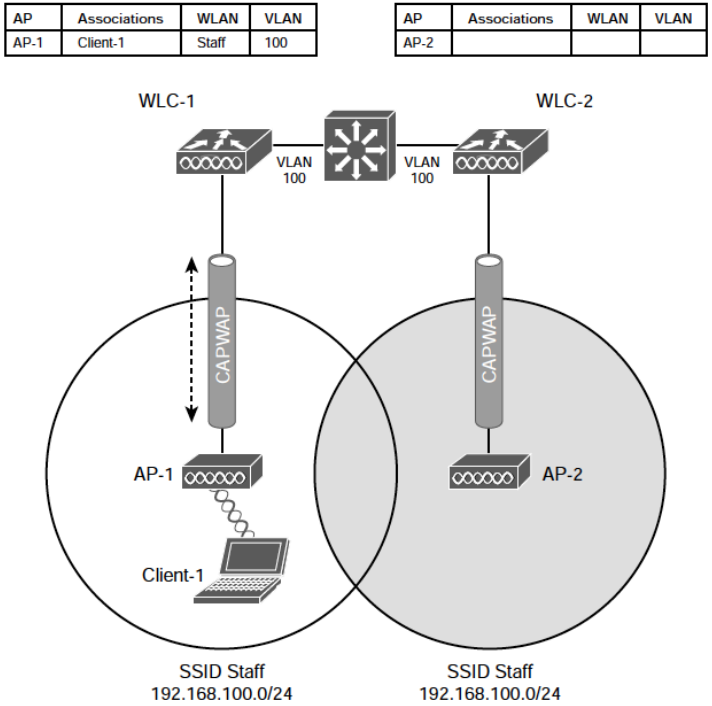

Figure 19-6 *Before an Intercontroller Roam*

After an Intercontroller Roam

When the client roams to a different AP, it can try to continue using its existing IP address or work with a DHCP server to either renew or request an address.

Figure 19-7 shows the client roaming to AP 2, where WLAN Staff is also bound to the same VLAN 100 and 192.168.100.0/24 subnet. Because the client has roamed between APs but stayed on the same VLAN and subnet, it has made a Layer 2 intercontroller roam.

Key Topic

AP	Associations	WLAN	VLAN

AP	Associations	WLAN	VLAN
AP-2	Client-1	Staff	100

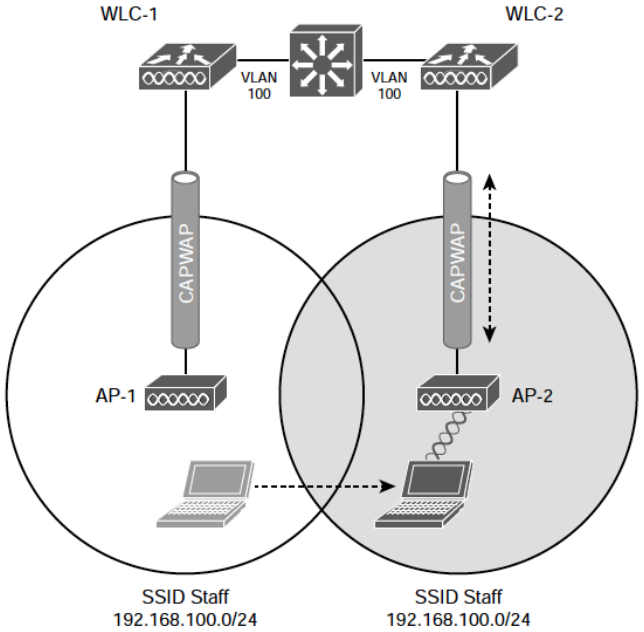

Figure 19-7 *After an Intercontroller Roam*

Before a Layer 3 Intercontroller Roam

When a client initiates an intercontroller roam, the two controllers involved can compare the VLAN numbers that are assigned to their respective WLAN interfaces. If the two VLAN IDs differ, the controllers arrange a Layer 3 roam that will allow the client to keep using its IP address.

Figure 19-8 illustrates a simple wireless network containing two APs and two controllers.

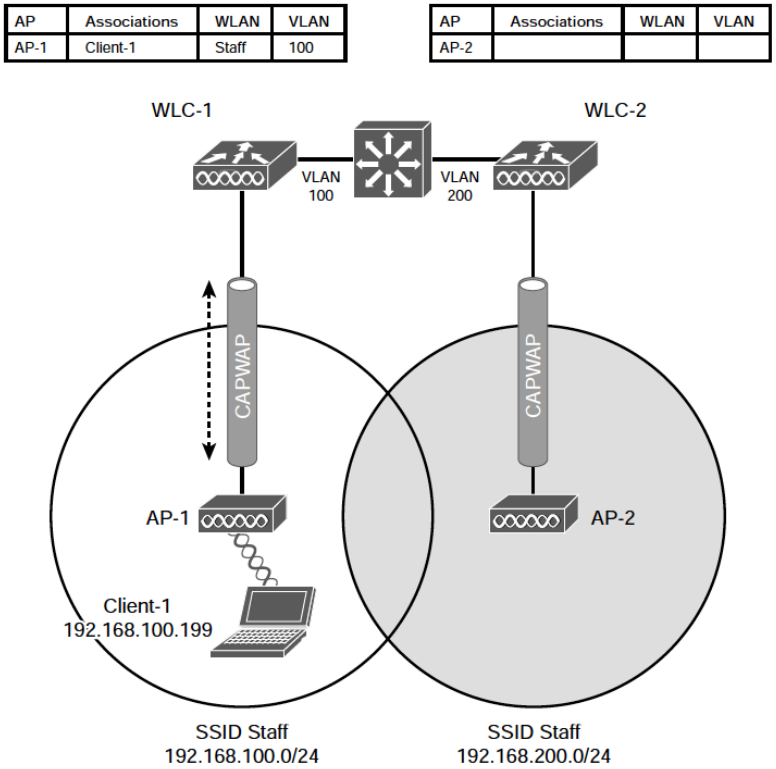

Figure 19-8 *Before a Layer 3 Intercontroller Roam*

After a Layer 3 Intercontroller Roam

A Layer 3 intercontroller roam consists of an extra tunnel that is built between the client's original controller and the controller it has roamed to. The tunnel carries data to and from the client as if it is still associated with the original controller and IP subnet.

Figure 19-9 shows the results of a Layer 3 roam.

The original controller (WLC 1) is called the anchor controller, and the controller with the roamed client is called the foreign controller.

Key Topic

AP	Associations	WLAN	VLAN
WLC-2	Client-1 (Mobile)	Staff	100

AP	Associations	WLAN	VLAN
AP-2	Client-1	Staff	

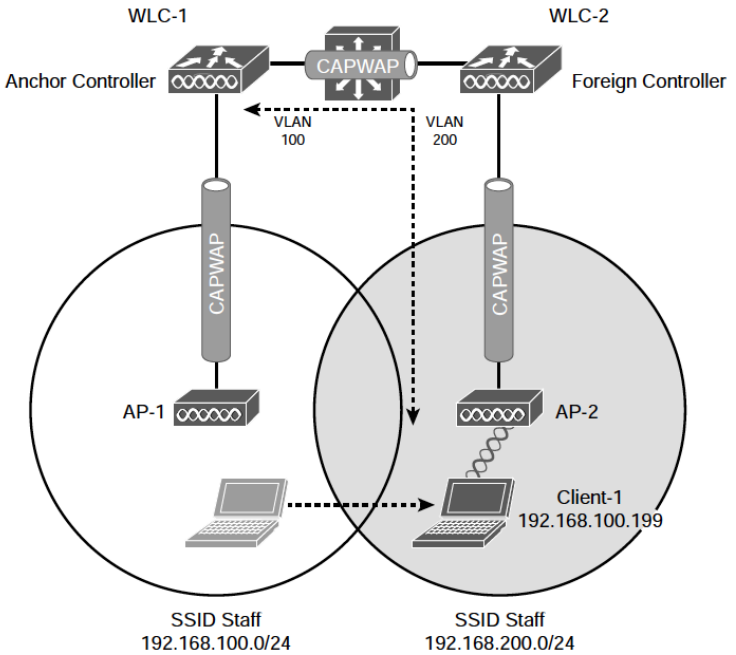

Figure 19-9 *After a Layer 3 Intercontroller Roam*

Scaling Mobility with Mobility Groups

Cisco controllers can be organized into mobility groups to facilitate intercontroller roaming.

If two centralized controllers are configured to belong to the same mobility group, clients can roam quickly between them.

If two controllers are assigned to different mobility groups, clients can still roam between them, but the roam is not very efficient. Credentials are not cached and shared, so clients must go through a full authentication during the roam.

Mobility Group Hierarchy

Mobility groups have an implied hierarchy, as shown in Figure 19-10.

Each controller maintains a mobility list that contains its own MAC address and the MAC addresses of other controllers. Each controller in the list is also assigned a mobility group name.

The mobility list gives a controller its view of the outside world; it knows of and trusts only the other controllers configured in the list.

Key Topic

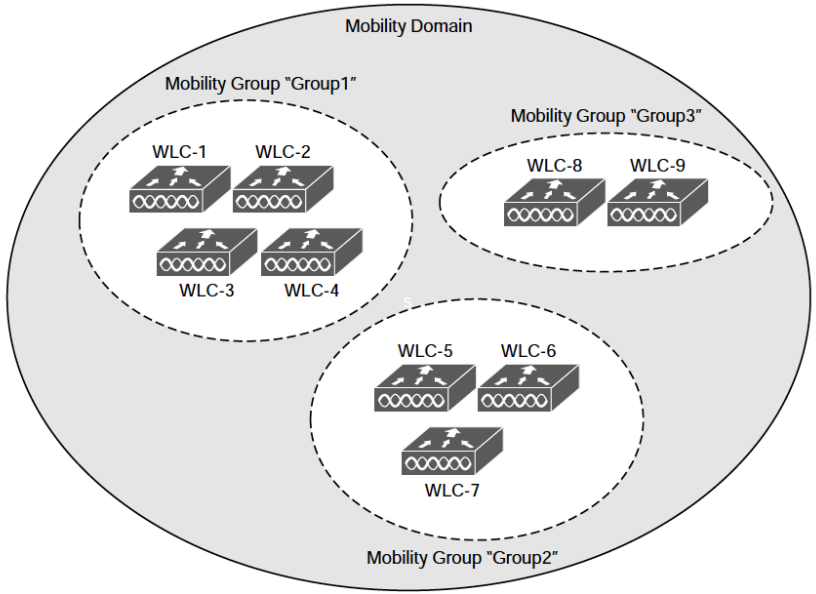

Figure 19-10 *Mobility Group Hierarchy*

Locating Devices in a Wireless Network

- Wireless networks are usually designed to provide coverage and connectivity in all areas where client devices are expected to be located. For example, a hospital building will likely have seamless wireless coverage on all floors and in all areas where users might go. Locating a user or device is important in several use cases, and a wireless network can be leveraged to provide that information.

Locating a Wireless Device with One AP or Three APs

A client's distance from an AP can be computed from its RSS. If the distance is measured from a single AP only, it is difficult to determine where the client is situated in relation to the AP. Obtain the same measurement from three or more APs, then correlate the results and determine where they intersect.

Figure 19-11 illustrates the difference in determining a client's location with a single and multiple APs.

Key Topic

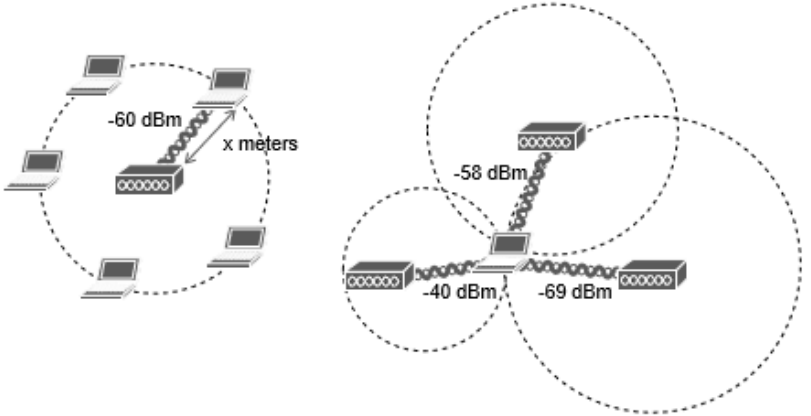

Figure 19-11 *Locating a Wireless Device with One AP (left) and Three APs (right)*

Real Time Location Data for Tracked Devices

The most intuitive way to interpret location data is to view devices on a map that represents the building and floor where they are located.

Figure 19-12 shows an example map of one floor of a building from Cisco DNA Spaces. The square icons represent AP locations, which were manually entered on the map. One device has been selected in the figure causing lines to be drawn to some of the APs that overheard the device.

Key Topic

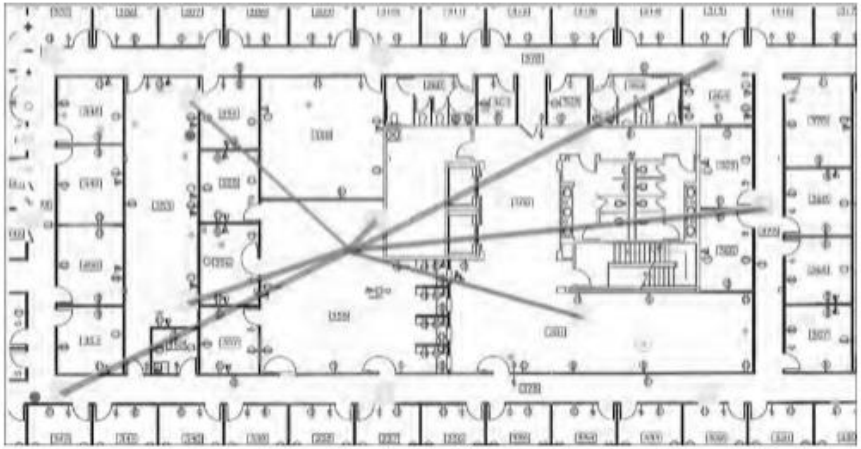

Figure 19-12 *An Example Map Showing Real Time Location Data for Tracked Devices*

Real Time Location for Other Tracked Devices

The same real-time location service also supports wireless devices that might never actually associate with an AP. For example, you might be interested in locating or tracking a potential customer's smartphone as he walks through a store. As long as Wi-Fi is enabled on the device, it will probably probe for available APs.

RFID tags are another type of device that can be attached to objects so that they can be tracked and located. Some RFID tags can actively join a wireless network to exchange data, while others are meant to simply "wake up" periodically to send 802.11 Probe Requests or multicast frames to announce their presence.

Another interesting use case is locating rogue devices and sources of Wi-Fi interference. Rogue devices will likely probe the network and can be discovered and located. Interference sources, such as cordless phones, wireless video cameras, and other transmitters, might not be compatible with the 802.11 standard at all.

Prepare for the Exam

Prepare for the Exam

Key Topics for Chapter 19

Description
After Roaming Between Autonomous APs
Cisco Wireless Network After an Intracontroller Roam
After an Intercontroller Roam
After a Layer 3 Intercontroller Roam
Mobility Group Hierarchy
Locating a Wireless Device with One AP (left) and Three APs (right)
An Example Map Showing Real Time Location Data for Tracked Devices

Prepare for the Exam

Key Terms for Chapter 19

Key Terms	
Author controller	Mobility controller (MC)
Foreign controller	Mobility domain
Intercontroller roaming	Mobility group
Intracontroller roaming	Point of attachment (PoA)
Layer 2 roam	Point of presence (PoP)
Layer 3 roam	Received signal strength (RSS)
Mobility agent (MA)	RF fingerprinting


CISCO