CHAPTER 5

Wireless LAN Topologies

Up to this point, this book has discussed radio frequency (RF) signals as they travel from a transmitter to a receiver. As Figure 5-2 shows, the transmitter can contact the receiver at any and all times, as long as both devices are tuned to the same frequency (or channel) and use the same modulation and coding scheme. That all sounds simple, except that it is not really practical.

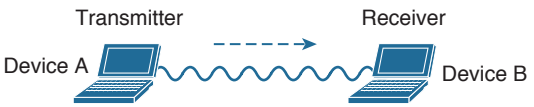

Figure 5-2 *Unidirectional Communication*

To fully leverage wireless communication, data should travel in both directions, as shown in Figure 5-3. Sometimes Device A needs to send data to Device B, while Device B would like to take a turn to send at other times.

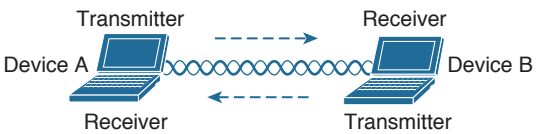

Figure 5-3 *Bidirectional Communication*

Because the two devices are using the same channel, two phrases in the preceding sentence become vitally important: *take a turn* and *send at other times*. As you learned in previous chapters, if multiple signals are received at the same time, they interfere with each other. The likelihood of interference increases as the number of wireless devices grows. For example, Figure 5-4 shows four devices tuned to the same channel and what might happen if some or all of them transmit at the same time.

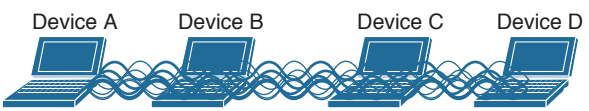

Figure 5-4 *Interference from Simultaneous Transmissions*

All this talk about waiting turns and avoiding interference should remind you of an Ethernet LAN, where multiple hosts can share common bandwidth and a collision domain. To use the media effectively, all the hosts must operate in half-duplex mode so that they avoid colliding with other transmissions. The side effect is that no host can transmit and receive at the same time on a given frequency.

Tip IEEE 802.11 WLANs are always half duplex because transmissions between stations use the same frequency. Only one station can transmit at any time; otherwise, collisions occur. To achieve full-duplex mode, one station's transmission would have to occur on one frequency while it receives over a different frequency—much like full-duplex Ethernet links work. Although this is certainly possible and practical, the 802.11-2012 standard does not permit full-duplex operation. The 802.11ac amendment will somewhat ease that restriction in its "Wave 2" implementation, through the use of downstream multi-user MIMO (MU-MIMO).

A wireless LAN is similar. Because multiple hosts can share the same channel, they also share the "airtime" or access to that channel at any given time. Therefore, to keep everything clean, only one device should transmit at any given time. To contend for use of the channel, devices based on the 802.11 standard have to determine whether the channel is clear and available before transmitting anything. This process is described in more detail in Chapter 6, "Understanding 802.11 Frame Types."

At the most basic level, there is no inherent organization to a wireless medium or any inherent control over the number of devices that can transmit and receive frames. Any device that has a wireless network adapter can power up at any time and try to communicate. At a minimum, a wireless network should have a way to make sure that every device using a channel can support a common set of parameters, including data rates, 802.11 modulation types, channel width, and so on. Beyond that, there should be a way to control which devices (and users) are allowed to use the wireless medium, and the methods that are used to secure the wireless transmissions.

Basic Service Set

The solution is to make every wireless service area a closed group of mobile devices that forms around a fixed device—before a device can participate, it must advertise its capabilities and then be granted permission to join. The 802.11 standard calls this a *basic service set* (BSS). At the heart of every BSS is a wireless *access point* (AP), as shown in Figure 5-5. The AP operates in *infrastructure mode*, which means it offers the services that are necessary to form the infrastructure of a wireless network.

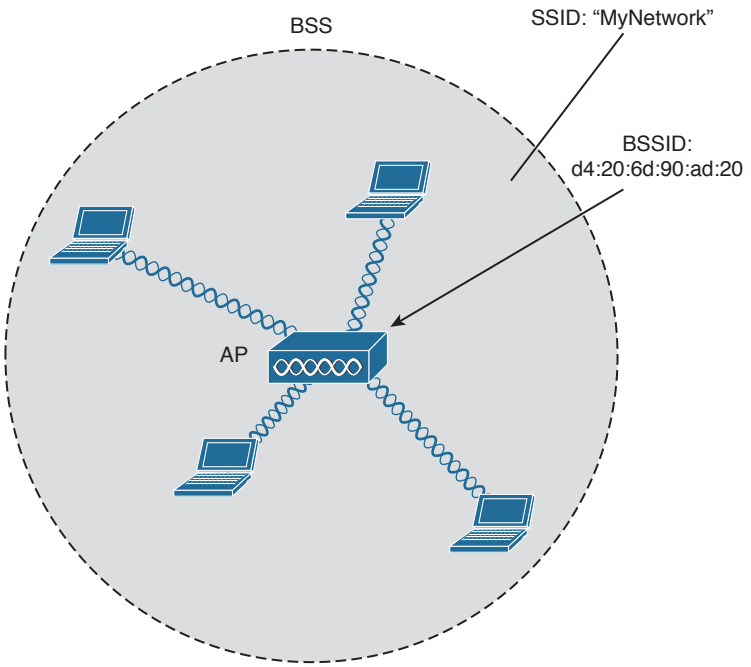

Figure 5-5 *802.11 Basic Service Set*

Because the operation of a BSS hinges on the AP, the BSS is bounded by the area where the AP's signal is usable. This is known as the *basic service area* (BSA) or *cell*. In Figure 5-5, the cell is shown as a simple circular area that might result from the radiation pattern of an omnidirectional antenna. Cells can have other shapes too, depending on the antenna that is connected to the AP and on the physical surroundings.

The AP serves as a single point of contact for every device that wants to use the BSS. It advertises the existence of the BSS so that devices can find it and try to join. To do that, the AP uses a unique BSS identifier (BSSID) that is based on the AP's own radio MAC address.

In addition, the AP advertises the wireless network with a service set identifier (SSID), which is a text string containing a logical name. Think of the BSSID as a machine-readable name tag that uniquely identifies the BSS ambassador (the AP), and the SSID as a non-unique, human-readable name tag that identifies the wireless service.

Membership with the BSS is called an *association*. A device must send an association request and the AP must either grant or deny the request. Once associated, a device becomes a client, or an 802.11 *station* (STA), of the BSS. What then? As long as a wireless client remains associated with a BSS, most communications to and from the client must pass *through* the AP, as indicated in Figure 5-6. By using the BSSID as a source or destination address, data frames can be relayed to or from the AP.

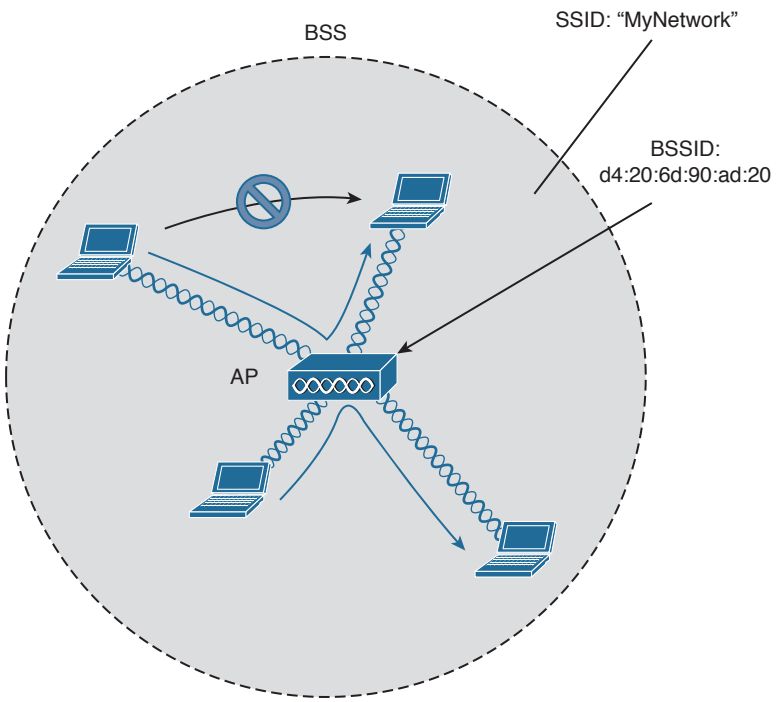

Figure 5-6 *Traffic Flows Within a BSS*

You might be wondering why all client traffic has to traverse the AP at all. Why cannot two clients simply transmit data frames directly to each other and bypass the middleman? If clients are allowed to communicate directly, then the whole idea of organizing and managing a BSS is moot. By sending data through the AP first, the BSS remains stable and under control. The 802.11z amendment, along with a few other Wi-Fi Alliance peer-to-peer mechanisms like Wi-Fi Direct and Near-me Area Network (NAN), provide an exception to the rule, which permits two clients to communicate directly without having to pass through an AP.

Tip Even though data frames are meant to pass through an AP, keep in mind that other devices in the same general area that are listening on the same channel can overhear the transmissions. After all, frames are freely available over the air to anyone that is within range to receive them. If the frames are unencrypted, then anyone may inspect their contents. Only the BSSID value contained within the frames indicates that the intended sender or recipient is the AP.

Distribution System

Notice that a BSS involves a single AP and no explicit connection into a regular Ethernet network. In that setting, the AP and its associated clients make up a standalone network. But the AP’s role at the center of the BSS does not just stop with managing the BSS—sooner or later, wireless clients will need to communicate with other devices that are not members of

the BSS. Fortunately, an AP can also uplink into an Ethernet network because it has both wireless and wired capabilities. The 802.11 standard refers to the upstream wired Ethernet as the *distribution system* (DS) for the wireless BSS, as shown in Figure 5-7.

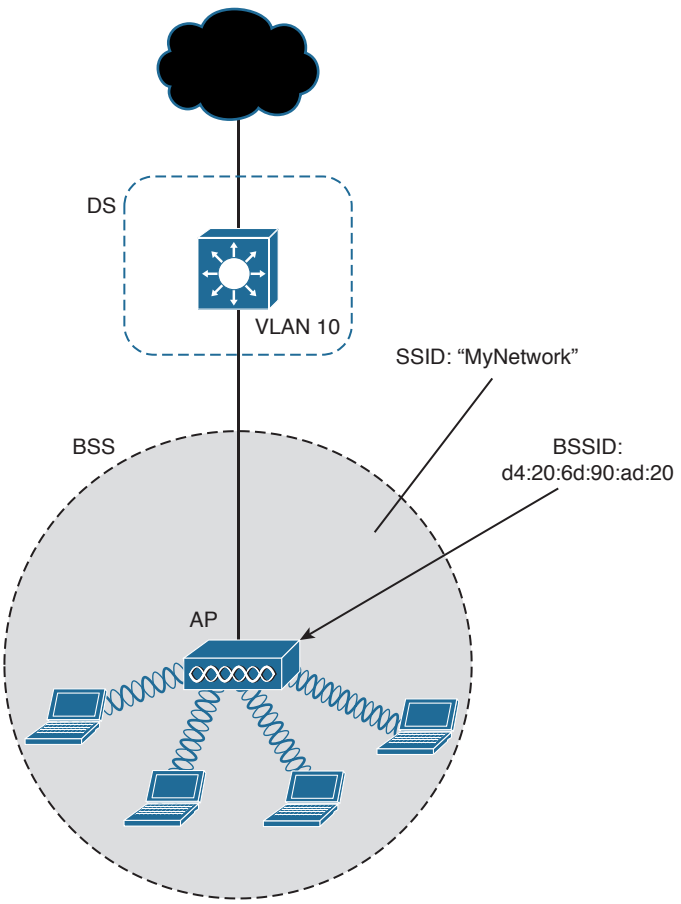

Figure 5-7 *Distribution System Supporting a BSS*

You can think of an AP as a translational bridge, where frames from two dissimilar media (wireless and wired) are translated and then bridged at Layer 2. In simple terms, the AP is in charge of mapping a virtual local-area network (VLAN) to an SSID. In Figure 5-7, the AP maps VLAN 10 to the wireless LAN using SSID "MyNetwork." Clients associated with the "MyNetwork" SSID will appear to be connected to VLAN 10.

This concept can be extended so that multiple VLANs are mapped to multiple SSIDs. To do this, the AP must be connected to the switch by a trunk link that carries the VLANs. In Figure 5-8, VLANs 10, 20, and 30 are trunked to the AP over the DS. The AP uses the 802.1Q tag to map the VLAN numbers to the appropriate SSIDs. For example, VLAN 10 is mapped to SSID "MyNetwork," VLAN 20 is mapped to SSID "YourNetwork," and VLAN 30 to SSID "Guest."

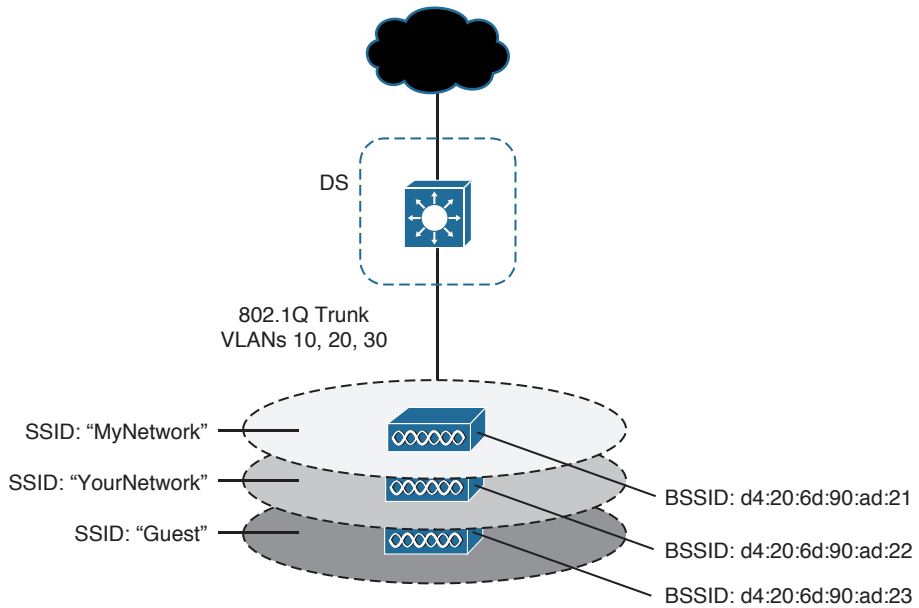

Figure 5-8 *Supporting Multiple SSIDs on One AP*

In effect, when an AP uses multiple SSIDs, it is trunking VLANs over the air to wireless clients. The clients must use the appropriate SSID that has been mapped to the respective VLAN when the AP was configured. The AP then appears as multiple logical APs—one per BSS—with a unique BSSID for each. With Cisco APs, this is usually accomplished by incrementing the last digit of the radio’s MAC address for each SSID.

Even though an AP can advertise and support multiple logical wireless networks, each of the SSIDs covers the same geographic area. That is because the AP uses the same transmitter, receiver, antennas, and channel for every SSID that it supports. Beware of one misconception though: Multiple SSIDs can give an illusion of scale. Even though wireless clients can be distributed across many SSIDs, all of those clients must share the same AP’s hardware and must contend for airtime on the same channel.

Extended Service Set

Normally, one AP cannot cover the entire area where clients might be located. For example, you might need wireless coverage throughout an entire floor of a business, hotel, hospital, or other large building. To cover more area than a single AP’s cell, you simply need to add more APs and spread them out geographically.

When APs are placed at different geographic locations, they can all be interconnected by a switched infrastructure. The 802.11 standard calls this an extended service set (ESS), as shown in Figure 5-9.

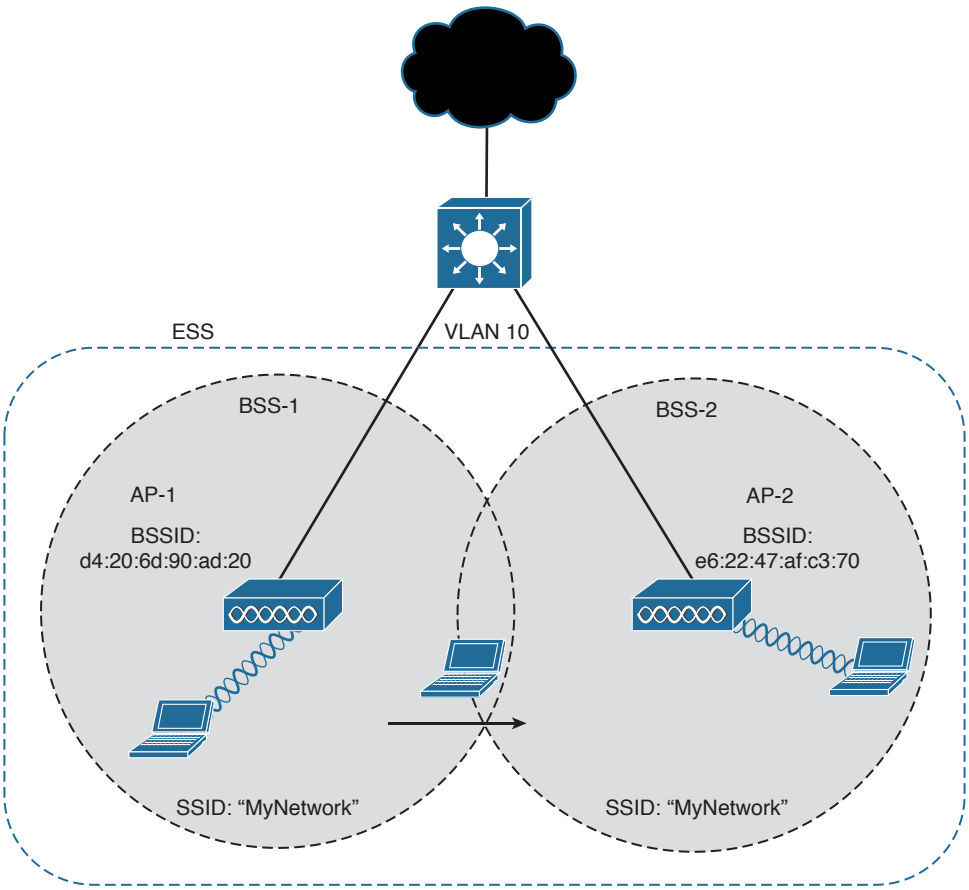

Figure 5-9 *Scaling Wireless Coverage with an 802.11 Extended Service Set*

Tip Chapter 7, "Planning Coverage with Wireless APs," discusses AP and cell placement in greater detail.

The idea is to make multiple APs cooperate so that the wireless service is consistent and seamless from the client's perspective. Ideally, any SSIDs that are defined on one AP should be defined on all the APs in an ESS; otherwise, it would be very cumbersome and inconvenient for a client to be reconfigured each time it moves into a different AP's cell.

Notice that each cell in Figure 5-9 has a unique BSSID, but both cells share one common SSID. Regardless of a client's location within the ESS, the SSID will remain the same but the client can always distinguish one AP from another.

In an ESS, a wireless client can associate with one AP while it is physically located near that AP. If the client later moves to a different location, it can associate with a different nearby AP automatically. Passing from one AP to another is called *roaming* and is covered in Chapter 6.

Independent Basic Service Set

Usually a wireless network leverages APs for organization, control, and scalability. Sometimes that is not possible or convenient in an impromptu situation. For example, two people who want to exchange electronic documents at a meeting, might not be able to find a BSS available or might want to avoid having to authenticate to a production network. In addition, many personal printers have the capability to print documents wirelessly, without relying on a regular BSS or AP.

The 802.11 standard allows two or more wireless clients to communicate directly with each other, with no other means of network connectivity. This is known as an *ad hoc* wireless network, or an *independent basic service set* (IBSS), as shown in Figure 5-10. For this to work, one of the devices must take the lead and begin advertising a network name and the necessary radio parameters. Any other device can then join as needed. IBSSs are meant to be organized in an impromptu, distributed fashion; therefore, they do not scale well beyond eight to ten devices.

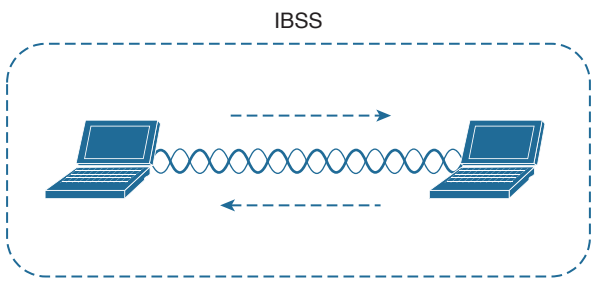

Figure 5-10 *802.11 Independent Basic Service Set*

Other Wireless Topologies

Wireless APs can be configured to operate in noninfrastructure modes when a normal BSS cannot provide the functionality that is needed. The following sections cover the most common modes.

Repeater

Normally, each AP in a wireless network has a wired connection back to the DS or switched infrastructure. To extend wireless coverage, additional APs and their wired connections are added. In some scenarios, it is not possible to run a wired connection to a new AP because the cable distance is too great to support Ethernet communication.

In that case, you can add an additional AP that is configured for *repeater mode*. A wireless repeater takes the signal it receives and repeats or retransmits it. The idea is to move the repeater out away from the AP so that it is still within range of both the AP and the distant client, as shown in Figure 5-11.

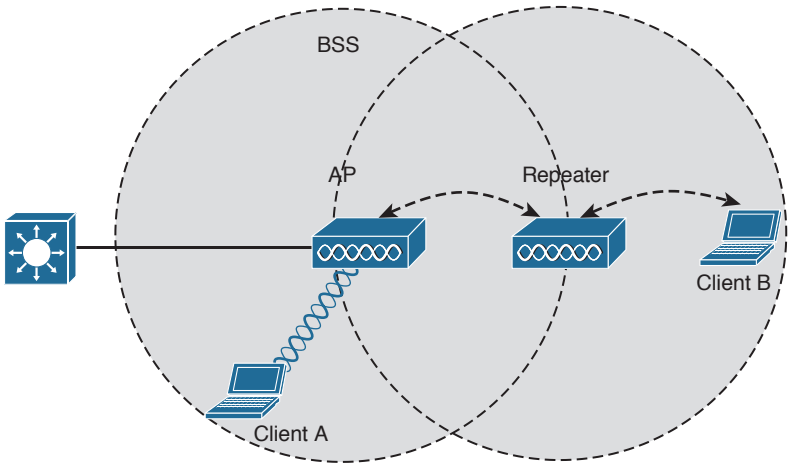

Figure 5-11 *Extending the Range of an AP with a Wireless Repeater*

If the repeater has a single radio, there is a possibility that the AP's signal will be received and retransmitted by the repeater, only to be received again by the AP—halving the effective throughput. As a remedy, some repeaters can use two radios to keep the original and repeated signals isolated. One radio is dedicated to signals in the AP's cell, while the other radio is dedicated to signals in the repeater's own cell.

Workgroup Bridge

Suppose you have a device that supports a wired Ethernet link but is not capable of having a wireless connection. You can use a workgroup bridge (WGB) to connect the device's wired network adapter to a wireless network.

Rather than providing a BSS for wireless service, a WGB becomes a wireless client of a BSS. In effect, the WGB acts as an external wireless network adapter for a device that has none. In Figure 5-12, an AP provides a BSS; Client A is a regular wireless client, while Client B is associated with the AP through a WGB.

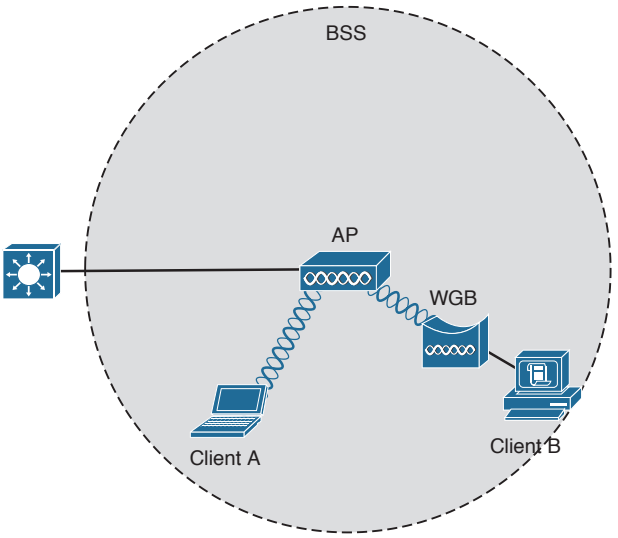

Figure 5-12 *Nonwireless Device Connecting Through a Workgroup Bridge*

You might encounter two types of workgroup bridges:

- **Universal workgroup bridge (uWGB)**—A single wired device can be bridged to a wireless network.
- **Workgroup bridge (WGB)**—A Cisco-proprietary implementation that allows multiple wired devices to be bridged to a wireless network.

Outdoor Bridge

An AP can be configured to act as a bridge to form a single wireless link from one LAN to another over a long distance. Outdoor bridged links are commonly used for connectivity between buildings or between cities.

If the LANs at two locations need to be bridged, a point-to-point bridged link can be used. One bridge mode AP is needed on each end of the wireless link. Directional antennas are normally used with the bridges to maximize the link distance, as shown in Figure 5-13.

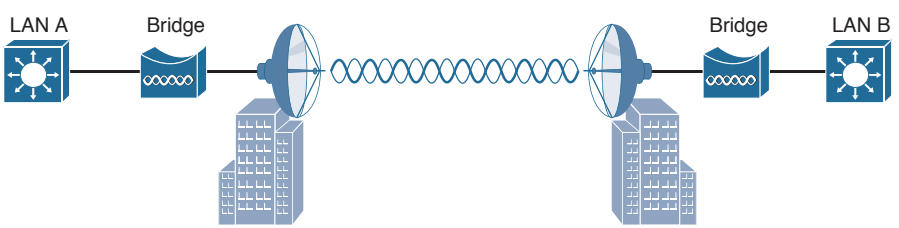

Figure 5-13 *Point-to-Point Outdoor Bridge*

Sometimes the LANs at multiple sites need to be bridged. A point-to-multipoint bridged link allows a central site to be bridged to several other sites. The central site bridge is

connected to an omnidirectional antenna so that its signal can reach the other sites simultaneously. The bridges at each of the other sites can be connected to a directional antenna aimed at the central site. Figure 5-14 shows the point-to-multipoint scenario.

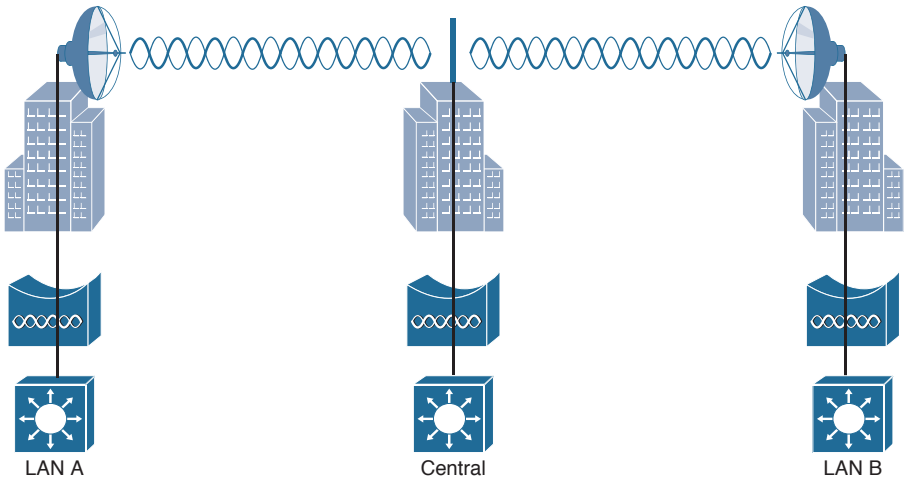

Figure 5-14 *Point-to-Multipoint Outdoor Bridge*

Mesh Network

To provide wireless coverage over a large area, it is not always practical to run Ethernet cabling to every AP that is needed. Instead, you could use multiple APs configured in mesh mode. In a mesh topology, traffic is bridged from AP to AP, in a daisy-chain fashion.

Mesh APs can leverage dual radios—one in the 2.4-GHz band and one in the 5-GHz band. Each mesh AP usually maintains a BSS on a 2.4-GHz channel, with which wireless clients can associate. Client traffic is then usually bridged from AP to AP over 5-GHz channels as a backhaul network. At the edge of the mesh network, the backhaul traffic is bridged to the wired LAN infrastructure. Figure 5-15 shows a typical mesh network. With Cisco APs, you can build a mesh network indoors or outdoors. The mesh network runs its own dynamic routing protocol to work out the best path for backhaul traffic to take across the mesh APs.

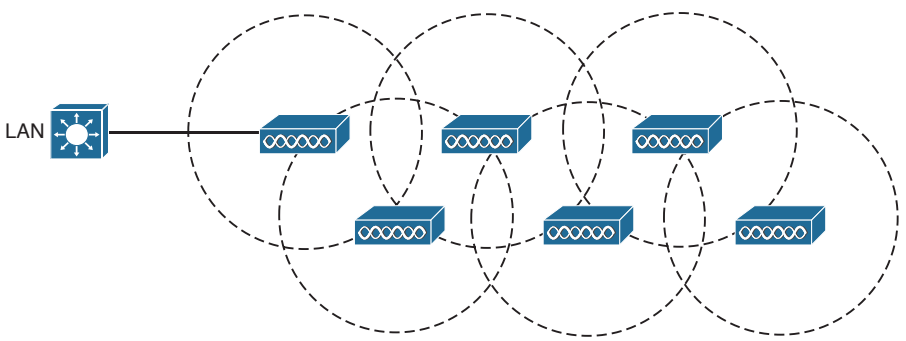

Figure 5-15 *Typical Wireless Mesh Network*