Designing and Deploying 802.11n Wireless Networks

Gain a practical understanding of the underlying concepts of the 802.11n standard and the methodologies for completing a successful wireless network installation

ciscopress.com

Jim Geier

Designing and Deploying 802.11n Wireless Networks

Jim Geier

Cisco Press

800 East 96th Street

Indianapolis, IN 46240

The 802.11 standard takes into account the following significant differences between wired and WLANs:

- **Security mechanisms:** Because wireless transmit signals over much larger areas than do those using wired media, WLANs, in terms of privacy, require a much larger area to protect. Thus, 802.11 implements a variety of encryption and authentication methods.
- **Bandwidth efficiency methods:** Radio frequency spectrum offers limited bandwidth for sending signals as compared to metallic and optical fiber cabling that Ethernet users. As a result, the 802.11 MAC and PHY layers must implement specialized functions for making transmissions as efficient as possible.
- **Power management:** Because 802.11 radios are installed in smaller handheld devices, with limited battery power, 802.11 includes options for activating a power save mode that conserves battery power.

The 802.11 standard defines services that provide the functions that the LLC layer requires for sending MSDUs between two entities on the network. These services, which the MAC layer implements, fall into two categories:

- **Station services:** These include authentication, deauthentication, privacy, and MSDU delivery.
- **Distribution system services:** These include association, disassociation, distribution, integration, and reassociation.

The following sections define the station and distribution system services.

Station Services

The 802.11 standard defines services for providing functions among stations. A station might be within any wireless element on the network, such as a handheld PC or handheld scanner. Each of these client devices might have more than one station. In addition, all access points implement station services. To provide necessary functionality, these stations need to send and receive MSDUs and implement adequate levels of security.

Authentication

Because WLANs have limited physical security to prevent unauthorized access, 802.11 defines authentication services to control LAN access to a level equal to a wired link. Every 802.11 station, whether part of an independent basic service set (BSS) or an extended service set (ESS) network, must use the authentication service prior to establishing a connection (referred to as an association in 802.11 terms) with another station with which it will communicate. Stations performing authentication send a unicast management authentication frame to the corresponding station.

Deauthentication

When a station wants to disassociate from another station, it invokes the deauthentication service. Deauthentication is a notification and cannot be refused. A station performs deauthentication by sending an authentication management frame (or group of frames to multiple stations) to advise of the termination of authentication.

Privacy

With a wireless network, all stations and other devices can hear data traffic taking place within range on the network, seriously affecting the security level of a wireless link. IEEE 802.11 counters this problem by offering a privacy service option (that is, encryption) that raises the security level of the 802.11 network to that of a wired network.

Note See Chapter 6 for more information about how 802.11 provides various services.

Distribution System Services

Distribution system services, as defined by 802.11, provide functionality across a distribution system. Access points provide distribution system services. The following sections provide an overview of the services that distribution systems need to provide proper transfer of MSDUs.

Association

Each station must initially invoke the association service with an access point before it can send information through a distribution system. The association maps a station to the distribution system via an access point. Each station can associate with only a single access point, but each access point can associate with multiple stations. Association is also a first step to providing the capability for a station to be mobile between BSSs.

Disassociation

A station or access point may invoke the disassociation service to terminate an existing association. This service is a notification; therefore, neither party may refuse termination. Stations should disassociate when leaving the network. An access point, for example, might disassociate all its stations if being removed for maintenance.

Distribution

A station uses the distribution service every time it sends MAC frames across a distribution system. The 802.11 standard does not specify how the distribution system delivers the data. The distribution service provides the distribution system with only enough information to determine the proper destination BSS.

Integration

The integration service enables the delivery of MAC frames through a portal between a distribution system and a non-802.11 LAN. The integration function performs all required media or address space translations. The details of an integration function depend on the distribution system implementation and are beyond the scope of the 802.11 standard.

Reassociation

The reassociation service enables a station to change its current state of association. Reassociation provides additional functionality to support BSS-transition mobility for associated stations. The reassociation service enables a station to change its association from one access point to another. This keeps the distribution system informed of the current mapping between access point and station as the station moves from one BSS to another within an ESS. Reassociation also enables changing association attributes of an established association while the station remains associated with the same access point. The mobile station always initiates the reassociation service.

Station States and Corresponding Frame Types

The state existing between a source and destination station (see Figure 5-5) governs which IEEE 802.11 frame types the two stations can exchange.

The following types of functions can occur within each class of frame:

- Class 1 frames

Control frames:

- Request-to-send (RTS)
- Clear-to-send (CTS)
- Acknowledgment (ACK)
- Contention-free (CF)

Management frames:

- Probe request/response
- Beacon
- Authentication
- Deauthentication
- Announcement traffic indication message (ATIM)

Data frames

- Class 2 frames

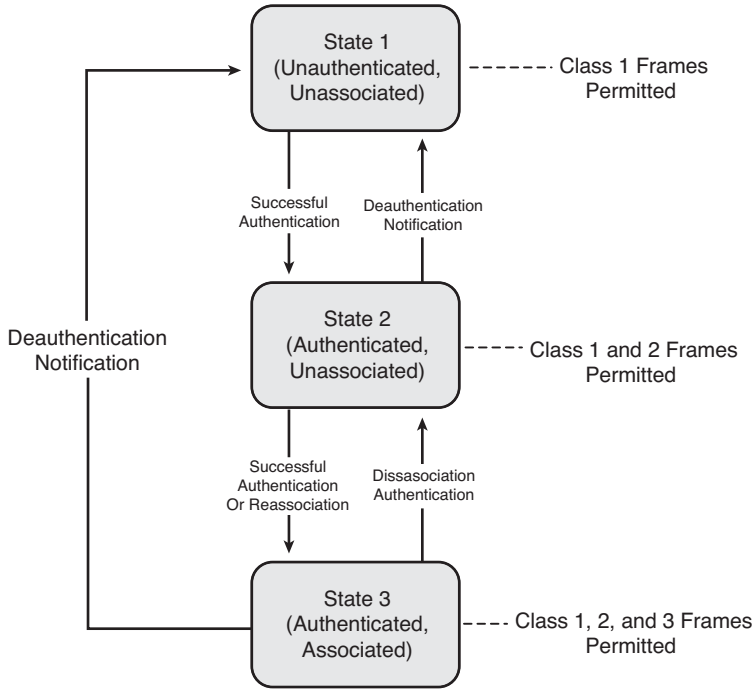

Figure 5-5 *The Operation of an 802.11 Station Depends on Its Particular State*

Management frames:

- Association request/response
- Reassociation request/response
- Disassociation

- Class 3 frames

Data frames

Management frames

- Deauthentication

Control frames

- Power Save Poll

To keep track of station state, each station maintains the following two state variables:

- **Authentication state:** Can have a value of unauthenticated and authenticated
- **Association state:** Can have a value of unassociated and associated

Note Keep up-to-date on the IEEE 802.11 Working Group activities by periodically visiting its website at http://www.ieee802.org/11/.

Summary

As mentioned in this chapter, the 802.11 WLAN standard certainly has benefits that an organization should consider when selecting components that provide LAN mobility. IEEE 802 is a solid family of standards that will provide much greater multiple-level interoperability than proprietary systems. The 802.11 standard has the backing of IEEE, having an excellent track record of developing long-lasting standards, such as IEEE 802.3 (Ethernet) and the earlier versions of 802.11.

Chapter 6

IEEE 802.11 Medium Access Control (MAC) Layer

This chapter will introduce you to:

- Primary 802.11 MAC Layer Functions
- Connectivity
- Timing and Synchronization
- RTS/CTS
- 802.11 MAC Frame Structures
- MAC Frame Types
- Interoperability

To design and implement an effective wireless LAN (WLAN), it is important to have a good understanding of the operation of the 802.11 MAC layer. The description of the MAC layer in the 802.11 standard is rather lengthy and focuses on details that developers must know when designing and implementing 802.11 radios, and it is not necessary that those deploying wireless LANs understand all the fine points. This chapter explains the parts of the 802.11 standard that you need to know to help you best configure and troubleshoot 802.11n WLANs.

Primary 802.11 MAC Layer Functions

The 802.11 standard specifies a common Media Access Control (MAC) layer, which provides a variety of functions that support the operation of 802.11-based WLANs. In general, the MAC layer manages and maintains communications between 802.11 stations (client radios and access points) by coordinating access to a shared radio channel and using protocols that enhance communications over a wireless medium. Often viewed as the "brains" of the network, the 802.11 MAC layer interfaces with a specific 802.11 physical (PHY) layer, such as 802.11a, 802.11b, 802.11g or 802.11n, to perform the tasks of