Guide to Wireless Communications, Third Edition

Chapter 8
High-Speed WLANs and WLAN Security

Objectives

- Describe how IEEE 802.11a networks function and how they differ from 802.11 networks
- Outline how 802.11g enhances 802.11b networks
- Discuss the 802.11n, 802.11ac, and 802.11ad amendments to the standard
- Explain how the use of wireless bridges and wireless switches expands the functionality and management of WLANs
- List the security features and issues with IEEE 802.11 networks

IEEE 802.11a

- 802.11a standard maintains the same medium access control (MAC) layer functions as 802.11b WLANs
  - Differences are confined to the physical layer
- 802.11a achieves its increase in speed and flexibility over 802.11b through:
  - Its multiplexing technique
  - A more efficient error-correction scheme

U-NII Frequency Band

- IEEE 802.11a uses the Unlicensed National Information Infrastructure (U-NII) band
  - Intended for devices that provide short-range, high-speed wireless digital communications
- U-NII spectrum is segmented into four bands
  - Each band has a maximum power limit
- Outside the United States
  - 5 GHz band is allocated to users and technologies other than WLANs

Unlicensed Band	Frequency Bands	WLAN Standard	Total Bandwidth
Industrial, Scientific, and Medical (ISM)	2.4–2.4835 GHz 5.725–5.875 GHz	802.11b, 802.11g, 802.11n 802.11n	83.5 MHz 150 MHz
Unlicensed National Information Infrastructure (U-NII)	5.15–5.25 GHz 5.25–5.35 GHz 5.47–5.725 GHz 5.725–5.825 GHz	802.11a, 802.11n, 802.11ac	100 MHz 100 MHz 255 MHz 100 MHz

Table 8-1 ISM vs. U-NII

U-NII Band	Frequency (GHz)	Maximum Power Output (mW)
U-NII-1	5.15–5.25	40
U-NII-2	5.25–5.35	200
U-NII-2 Extended	5.47–5.725	200
U-NII-3	5.725–5.825	800

Table 8-2 U-NII bands

Channel Allocation in 802.11a

- Channel allocation
  - With 802.11b, the available frequency spectrum is divided into 11 channels in the United States
    - Only three non-overlapping channels are available for simultaneous operation
  - In 802.11a, eight frequency channels operate simultaneously
    - In the Low Band (5.15 to 5.25 GHz) and Middle Band (5.25 to 5.35 GHz)
    - 23 channels are available
    - Within each frequency channel there is a 20 MHz-wide channel that supports 52 subcarrier frequencies

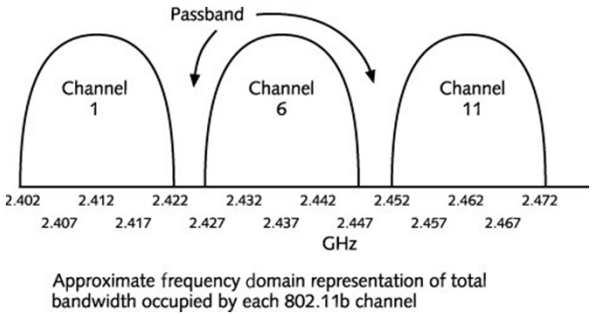

Figure 8-1 802.11b channels

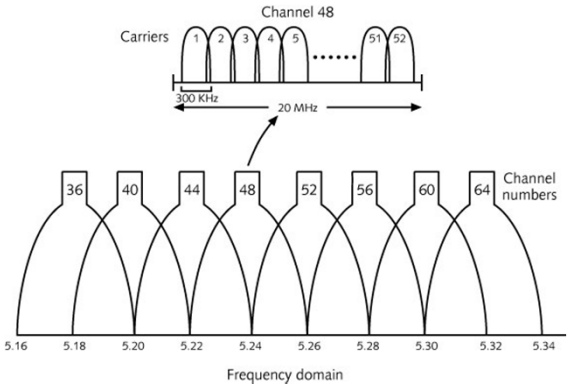

Figure 8-2 802.11a channels

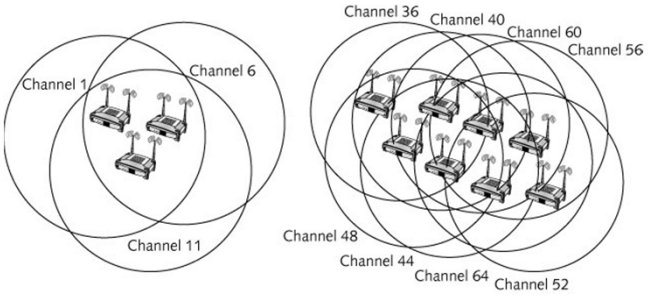

Figure 8-3 802.11b vs. 802.11a channels

Orthogonal Frequency Division Multiplexing

- Multipath distortion
  - Receiving device gets the signal from several different directions at different times
    - Must wait until all reflections are received
- 802.11a solves this problems using OFDM
- Orthogonal Frequency Division Multiplexing (OFDM)
  - Splits a high-speed digital signal into several slower signals running in parallel
  - Sends the transmission in parallel across several lower-speed, narrower frequency channels

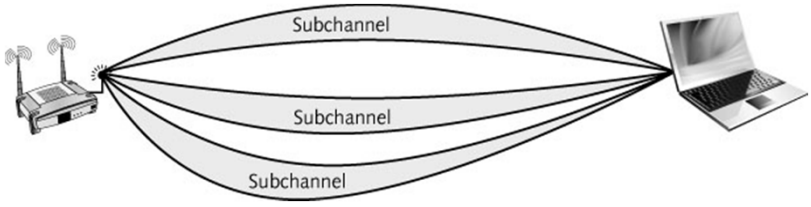

Figure 8-4 Transmitting on multiple subchannels simultaneously

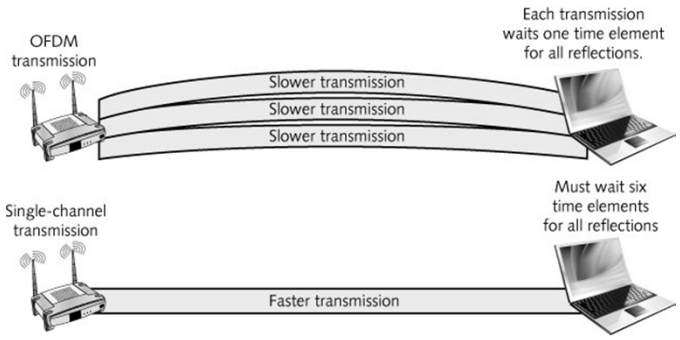

Figure 8-5 Comparison of OFDM and single channel transmission

Orthogonal Frequency Division Multiplexing

- OFDM uses 48 of the 52 subchannels for data
- Modulation techniques
  - At 6 Mbps, phase shift keying (PSK)
  - At 12 Mbps, quadrature phase shift keying (QPSK)
  - At 24 Mbps, 16-level quadrature amplitude modulation (16-QAM)
  - At 54 Mbps, 64-level quadrature amplitude modulation (64-QAM)

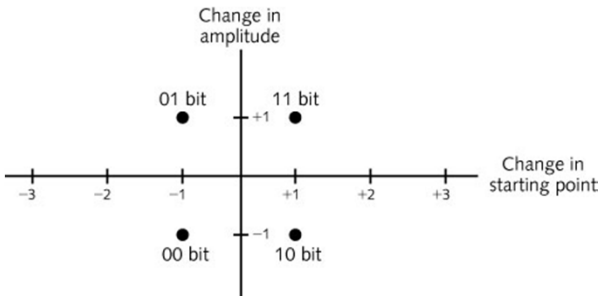

Figure 8-6 Quadrature amplitude modulation

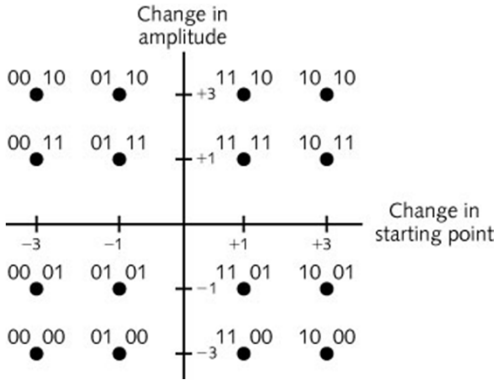

Figure 8-7 16-level quadrature amplitude modulation (16-QAM)

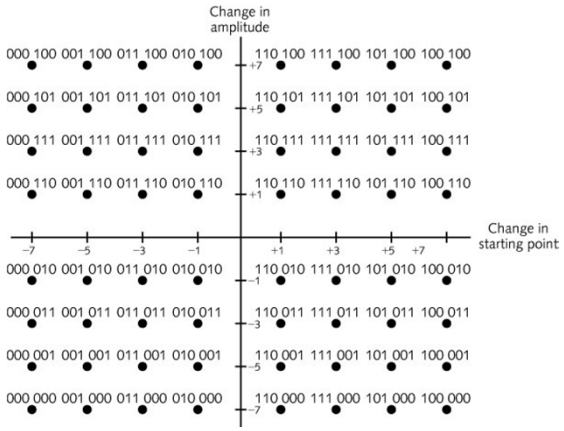

Figure 8-8 64-level quadrature amplitude modulation (64-QAM)

Error Correction in 802.11a

- Number of errors is significantly reduced
  - Due to the nature of 802.11a transmissions
- Because transmissions are sent over parallel subcarriers
  - Radio interference from outside sources is minimized
- Forward Error Correction (FEC) transmits extra bits per byte of data
  - Eliminates the need to retransmit if an error occurs, which saves time, increases throughput

802.11a PHY Layer

- The 802.11a PHY layer is divided into two parts
  - Physical Medium Dependent (PMD) sublayer
    - Defines the characteristics of the wireless medium
    - Defines the method for transmitting and receiving data through that medium
  - Physical Layer Convergence Procedure (PLCP)
    - Based on OFDM instead of DSSS
    - Reformats the data received from the MAC layer into a frame that the PMD sublayer can transmit
    - Determines when the medium is free so data can be sent

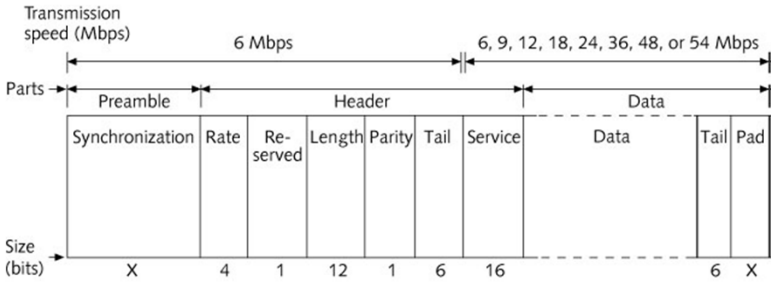

Figure 8-9 802.11a PLCP frame

802.11a PHY Layer

- 802.11a networks have a shorter range of coverage
  - Approximately 225 feet
  - Compared to 375 feet for an 802.11bWLAN

IEEE 802.11g

- Operates in the same frequency band as 802.11b
- Follows the same specifications for 802.11b
- Standard outlines two mandatory transmission modes along with two optional modes
- Mandatory transmission modes
  - Same mode used by 802.11b and must support the rates of 1, 2, 5.5, and 11 Mbps
  - Same OFDM mode used by 802.11a but in the same frequency band used by 802.11b
- Number of channels available with 802.11g is three
  - Compared with eight channels for 802.11a

IEEE 802.11g

- Optional transmission modes
  - PBCC (Packet Binary Convolutional Coding) and can transmit at 22 or 33 Mbps
  - DSSS-OFDM, which uses the standard DSSS preamble of 802.11b
    - Transmits the data portion of the frame using OFDM
- Optional modes are required to maintain backward compatibility with 802.11b

IEEE 802.11g

- Signal timing differences
  - When device transmits at a higher rate than 802.11b
    - A 6-microsecond quiet time of no transmission is added
      - At the end of the data portion of every frame
  - Short interframe space (SIFS) timing
    - Affected by the addition of the quiet time
    - Overall performance is lower than that of 802.11a due to the added ‘quiet time’ when 802.11b devices are present
    - An all-80211.g network does not require the quiet time
- PLCP frame formats used in 802.11g are the same as for 802.11b

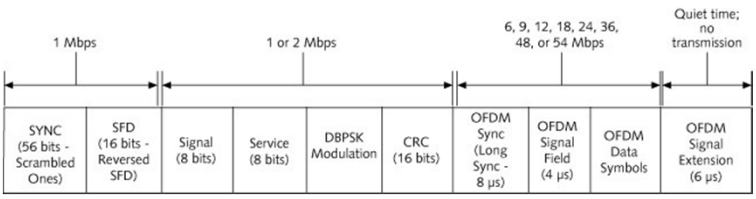

Figure 8-10 802.11g PLCP frame

IEEE 802.11g

- When both 802.11b and 802.11g devices share the same network
  - Standard defines how the frame header is transmitted at 1 or 2 Mbps using DSSS
- The optional 22 Mbps rate is achieved by using the PBCC encoding method
- Modulation is binary phase shift keying (BPSK)

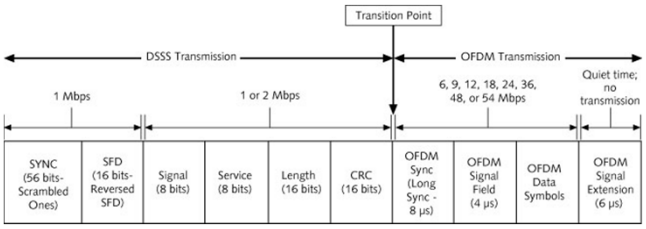

Figure 8-11 802.11b (DSSS) to 802.11g (OFDM) transition after the frame header

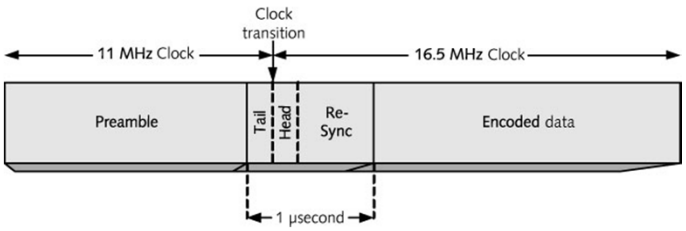

Figure 8-12 Clock switching during transition from 22 Mbps to 33 Mbps

IEEE 802.11n and Other Amendments

- IEEE 802.11n
  - Ratified end of 2009
  - Uses multiple radios and antennas in each device
  - Works in 2.4 and 5 GHz bands; backward compatible with 802.11

IEEE 802.11n

- Multiple-input and multiple-output (MIMO)
  - Based on using multiple radios and antennas
  - Prior to 802.11n, two antennas were used for **antenna diversity** – antenna with the strongest signal is used
  - 802.11n MIMO devices employ beamforming to direct transmissions to the device from which a frame was received
  - 802.11n MIMO also uses **spatial multiplexing** - frames are broken up and sent in multiple parts from different radios

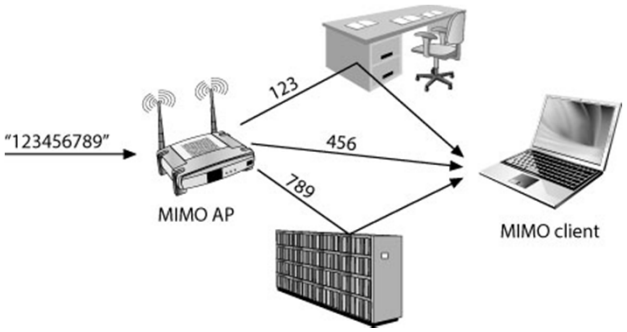

Figure 8-13 Spatial multiplexing sending multiple (spatial) streams of data

IEEE 802.11n

- Up to four transmitters and four receivers
  - Max transmission speed of 600 Mbps
  - Configurations such as 2x3 (2 transmitters and 3 receivers) and 3x3 (3 of each) exist

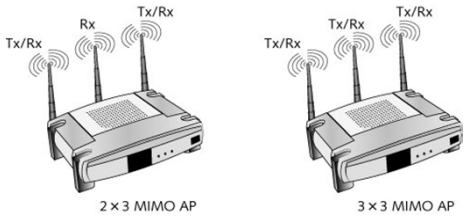

Figure 8-14 802.11n MIMO devices

IEEE 802.11n

- Channel configuration
  - Uses more bandwidth than other standards
    - Can use 20 or 22 MHz to communicate with 802.11b or 802.11g devices
    - Uses 40 MHz for high throughput (HT); 300 to 600 Mbps
  - Support DSSS and OFDM
  - 802.11n supports channel bonding – two channels are combined into on 40 MHz channel

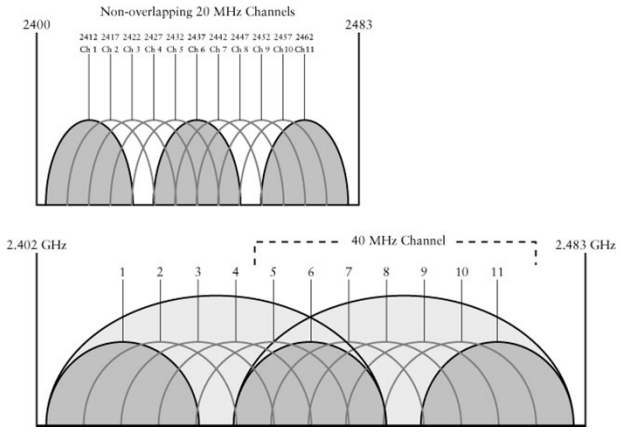

Figure 8-15 Channel bonding in 802.11n

IEEE 802.11n

- Guard interval
  - In non-HT transmissions, delay is required at the end of each frame to allow reflected signals to arrive
    - The delay is called the **guard interval**
    - Prevents **intersymbol interference (ISI)**
- Modulation and coding scheme
  - Nine different factors define the data rates
- HT PHY Layer
  - Supports three frame formats
    - 1 – when communicating with 802.11a/g devices
    - 2 – when used in mixed HT and legacy devices
    - 3 – 802.11n only (greenfield mode)

IEEE 802.11n

- MT MAC Sublayer
  - Enhancements to increase throughput and power management
    - Frame aggregation – combines multiple MAC frames into one PHY frame to reduce overhead
    - Two new power management methods
      - Spatial multiplexing power save mode (SMPS)
      - Power save multi-poll (PSMP)

IEEE 802.11n

- Reduced interframe space (RIFS)
  - Allowed only in greenfield mode
    - Shorter 2-microsecond interframe space
    - Less timing overhead (normal SIFS interval is 10 microseconds)

IEEE 802.11n

- HT operating modes
  - Allows 802.11n to coexist with non-HT devices
  - Mode 0 – greenfield mode, supports only HT-capable devices using 20 or 40 MHz channels
  - Mode 1 – an HT mode but prevents interference from non-HT devices by using protection mechanisms
  - Mode 2 – supports either 20 or 40 MHz channels
  - Mode 3 – non-HT mixed mode; supports devices at 20 or 40 MHz

IEEE 802.11e

- Approved for publication in November 2005
- Defines enhancements to the MAC layer of 802.11
  - To expand support for LAN applications that require Quality of Service (QoS)
- 802.11e allows the receiving device to acknowledge after receiving a burst of frames
- Enables prioritization of frames in distributed coordinated function (DCF) mode

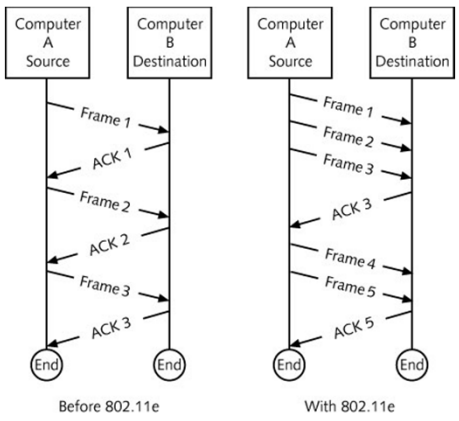

Figure 8-16 802.11e frame acknowledgements

IEEE 802.11e

- Implements two new coordination functions
  - Enhanced DCF (EDCF)
    - Station with higher priority traffic waits less to transmit
  - Hybrid coordination function (HCF)
    - Combination of DCF and point coordination function (PCF)
- Supports traffic prioritization based on QoS (quality-of-service); improves security features for mobile and nomadic users
- Nomadic user
  - Moves frequently but does not use the equipment while in motion

IEEE 802.11r

- Amount of time required by 802.11 devices to associate and disassociate
  - It is in the order of hundreds of milliseconds
- Support voice over wireless LAN (VoWLAN) in a business environment with multiple access points
  - 802.11 standard needs a way to provide quicker handoffs
- 802.11 MAC protocol
  - Does not allow a device to find out if the necessary QoS resources are available at a new AP

IEEE 802.11r

- 802.11r is designed to resolve these issues
  - In addition to security concerns regarding the handoff
- 802.11r is expected to enhance the convergence of wireless voice, data, and video

IEEE 802.11s

- Hard-to-do task
  - Deploy a wireless network over the entire downtown area of a medium-sized city
  - Provide seamless connectivity to all city employees
- Ideal solution
  - Connect the wireless APs to each other over the wireless communications channels
- 802.11s provides the solution – wireless mesh network

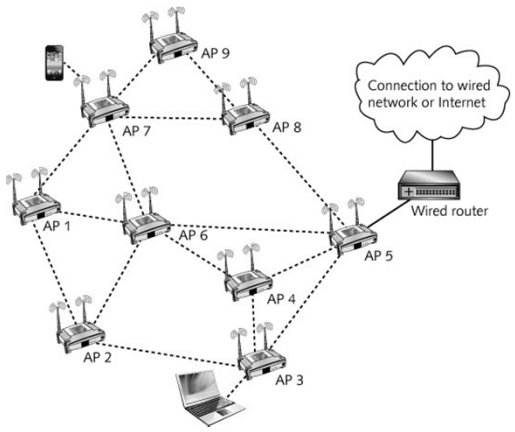

Figure 8-17 Wireless APs connected in a mesh network

802.11ac and 802.11ad

- 802.11ac and 802.11ad are under development
  - Ratification expected late 2013
  - Achieves data rates from 433 Mbps to almost 7 Gbps
  - Allows between two and eight radios
  - 802.11ac works only in the 5 GHz U-NII band
  - 802.11ad goal is to expand the 802.11 standard to work in the 60 GHz band while maintaining backward compatibility

Expanding WLAN Functionality

- Devices
  - Wireless bridges
    - Connect two wired networks or extend the range of a WLAN

Wireless Bridges and Repeaters

- Ideal solution for connecting remote sites when the sites are separated by obstacles
  - That make using a wired connection impractical or very expensive
- 802.11b bridges can transmit up to 18 miles (29 kilometers) at 11 Mbps
  - Or up to 25 miles (40 kilometers) at 2 Mbps
- 802.11a bridges can transmit up to 8.5 miles (13.5 kilometers) at 54 Mbps
  - Or 28 Mbps at up to 20 miles (32 kilometers)

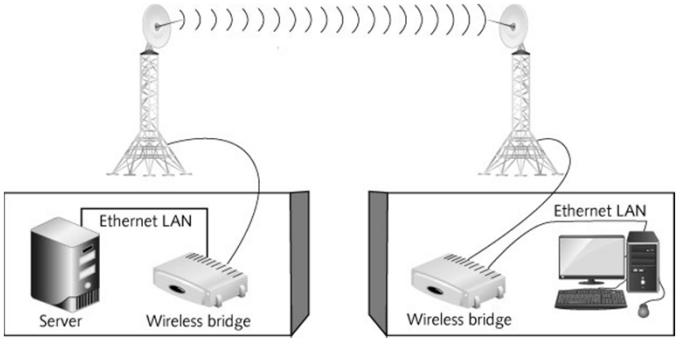

Figure 8-18 Wireless bridging of two LANs

Wireless Bridges and Repeaters

- WLAN extension
  - Wireless bridges can extend range of a WLAN
  - Bridge can be configured to connect to an AP as a repeater in point-to-multipoint mode
  - Client devices can associate with the bridge
- Keep in mind the amount of extra delay introduced in WLAN extension applications

Wireless Controllers

- Managing AP devices remotely can be difficult
- Wireless controllers
  - Incorporate most of the functions of an AP but do not have radios
  - Connect multiple, less-complex APs via cable connection or logical network connection
- Quality of Service (QoS) features make it easier to deploy voice over wireless LAN (VoWLAN)

Other WLAN Expansion Hardware

- Devices for the wireless home and office
  - Most specialized devices for distributing media or connecting computers are being discontinued due to WMM specification from the Wi-Fi Alliance

WLAN Security

- Broadcasting network traffic over the airwaves
  - Has created an entirely new set of issues for keeping data transmissions secure
  - Security implementations are analogous to those in Ethernet
  - WLANs are far more exposed to intrusion because the medium is not contained

Attacks Against WLANs

- Some of the most dangerous attacks
  - Hardware theft
    - Device may contain information that can assist someone in breaking into the network
  - AP impersonation
    - A rogue AP can impersonate a valid device
  - Passive monitoring
    - Data transmissions can be monitored
  - Denial of service (DoS)
    - Flood the network with transmissions and deny others access to the AP

802.11 Security

- Authentication
  - Process that verifies that the client device has permission to access the network
  - Each WLAN client can be given the SSID of the network manually or automatically
  - Turning off SSID broadcast can only protect your network against someone finding it unintentionally
- Privacy
  - Ensures that transmissions are not read by unauthorized users
  - Accomplished with data encryption

802.11 Security

- Wired Equivalent Privacy (WEP)
  - Data encryption specification for wireless devices
  - Two versions: 64-bit and 128-bit encryption
  - Attackers can decrypt a 128-bit WEP key in minutes
  - Uses weak RC4 implementation
  - Seldom used today except in some home networks

802.11 Security

- Wi-Fi Protected Access
  - Standard for network authentication and encryption
    - Introduced by the Wi-Fi Alliance in response to the weaknesses in WEP
  - Uses a 128-bit pre-shared key (PSK)
  - WPA-PSK uses a different encryption key for each client device, for each packet, and for each session
  - WPA employs temporal key integrity protocol (TKIP)
    - Which provides per-packet key-mixing
  - TKIP also provides message integrity check (MIC)
  - TKIP uses a 48-bit hashed initialization vector

802.11 Security

- Wi-Fi Protected Access
  - WPA2: version of WPA that has been certified by the IEEE to be compatible with IEEE 802.11i
- IEEE 802.11i and IEEE 802.1x
  - Define a robust security network association (RSNA)
  - Provide
    - Mutual authentication between client devices and AP
    - Controlled access to the network
    - Establishment of security keys
    - Key management

802.11 Security

- IEEE 802.11i and IEEE 802.1x
  - Client device must be authenticated on the network by an external authentication server
    - Remote Authentication Dial In User Service (RADIUS)
    - Or by AP itself
  - All communication between the client device and the AP is blocked
    - Until the authentication process is completed
  - 802.1x uses the Extensible Authentication Protocol (EAP)
    - For relaying access requests between a wireless device, the AP, and the RADIUS server

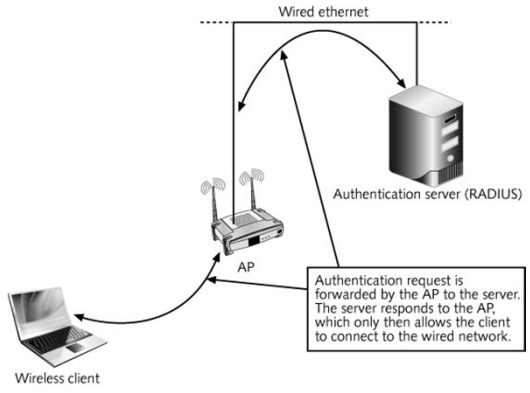

Figure 8-19 Securing a wireless network using a RADIUS server

802.11 Security

- Push-Button Wireless Security
  - New method of configuring wireless devices
  - Automatically configures the security settings
- Virtual Private Networks (VPNs)
  - Use an encrypted connection to create a virtual tunnel between two points
    - Across a public or corporate network
  - VPNs using strong encryption algorithms
    - Most secure method of implementing a wireless network

Additional WLAN Security Strategies

- Additional strategies
  - Reduce WLAN transmission power
  - Change the default security settings on the APs
  - Antivirus and antispyware software
  - Separate WLAN transmissions from wired network traffic
    - Place a firewall between the WLAN and the wired LAN

Summary

- Operating in the 2.4 GHz ISM frequency range, 802.11b has a maximum data rate of 11 Mbps
- The 802.11a has a maximum rated speed of 54 Mbps
- IEEE 802.11a networks use the Unlicensed National Information Infrastructure (U-NII) band
- In 802.11a, 23 frequency channels can operate simultaneously
- IEEE 802.11b WLAN reception is slowed down by multipath distortion
  - 802.11a solves this problem using OFDM

Summary

- OFDM uses 48 of the 52 subchannels for data, while the remaining four are used for error correction
  - Number of errors in an 802.11a transmission is significantly reduced
- The 802.11a standard made changes only to the physical layer (PHY layer)
  - Of the original 802.11 and 802.11b standard
- 802.11g preserves the features of 802.11b but increases the data transfer rates to those of 802.11a
- 802.11e standard adds QoS to 802.11 standards

Summary

- The 802.11n amendment increases the data rate up to 600 Mbps using either the 2.4 GHz ISM or the 5 GHz U-NII band
- The 802.11r amendment enables fast roaming and reduces the time required for a device to associate with a new AP
- The 802.11s amendment enables APs to communicate and pass traffic from one to the other
- The 802.11ac amendment boosts the speed of WLANs up to nearly 7 Gbps

Summary

- The new 802.11ad amendment operates in the 60 GHz band for short-range connections at up to 7 Gbps
- WLANs can suffer a range of security attacks
- WLANs can be protected through the use of VPNs, 802.11i authentication, and 802.1X privacy