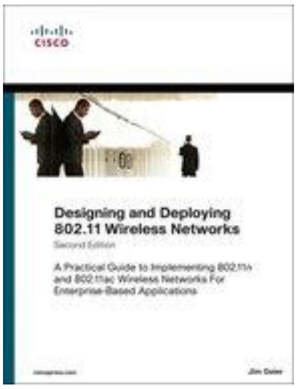


- **Designing and Deploying 802.11 Wireless Networks: A Practical Guide to Implementing 802.11n and 802.11ac Wireless Networks, Second Edition**
- **By:** Jim Geier

- **Publisher:** Cisco Press
- **Pub. Date:** May 18, 2015
- **Print ISBN-10:** 1-58714-430-1
- **Print ISBN-13:** 978-1-58714-430-1
- **Web ISBN-10:** 0-13-389143-7
- **Web ISBN-13:** 978-0-13-389143-0
- **Pages in Print Edition:** 600

About This eBook

ePUB is an open, industry-standard format for eBooks. However, support of ePUB and its many features varies across reading devices and applications. Use your device or app settings to customize the presentation to your liking. Settings that you can customize often include font, font size, single or double column, landscape or portrait mode, and figures that you can click or tap to enlarge. For additional information about the settings and features on your reading device or app, visit the device manufacturer's Web site.

Many titles include programming code or configuration examples. To optimize the presentation of these elements, view the eBook in single-column, landscape mode and adjust the font size to the smallest setting. In addition to presenting code and configurations in the reflowable text format, we have included images of the code that mimic the presentation found in the print book; therefore, where the reflowable format may compromise the presentation of the code listing, you will see a "Click here to view code image" link. Click the link to view the print-fidelity code image. To return to the previous page viewed, click the Back button on your device or app.

Designing and Deploying 802.11 Wireless Networks

A Practical Guide to Implementing 802.11n and 802.11ac Wireless Networks For Enterprise-Based Applications

Second Edition

Jim Geier

800 East 96th Street
Indianapolis, IN 46240

Designing and Deploying 802.11 Wireless Networks

Second Edition

Jim Geier

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

ISBN-13: 978-1-58714-430-1

ISBN-10: 1-58714-430-1

Printed in the United States of America

First Printing May 2015

Library of Congress Control Number: 2015936629

Warning and Disclaimer

This book is designed to provide information about wireless networking, which includes Cisco products. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an “as is” basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

Corporate and Government Sales

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact: **U.S. Corporate and Government Sales** 1-800-382-3419corpsales@pearsontechgroup.com

For sales outside the United States, please contact: **International Sales** international@pearsoned.com

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers’ feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through e-mail at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher: Paul Boger

Associate Publisher: Dave Dusthimer

Technical Editors: Jonathan Christman and George Stefanick

Copy Editor: Kitty Wilson

Indexer: Brad Herriman

Proofreader: Debbie Williams

Book Designer: Mark Shirar

Business Operation Manager, Cisco Press: Jan Cornelssen

Executive Editor: Mary Beth Ray

Managing Editor: Sandra Schroeder

Senior Development Editor: Eleanor C. Bru

Project Editor: Seth Kerney

Editorial Assistant: Vanessa Evans

Composition: Trina Wurst

Americas Headquarters
Cisco Systems. Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices**.

About the Author

Jim Geier has 30 years’ experience planning, designing, analyzing, and implementing communications systems, wireless networks, and mobile devices. Jim is founder and principal consultant of Wireless-Nets, Ltd., providing wireless analysis and design services to product manufacturers. He is also president and CEO and co-founder of Health Grade Networks, providing wireless network solutions to hospitals, airports, and manufacturing facilities. Jim is the author of more than a dozen books on mobile and wireless topics, including *Designing and Deploying 802.11n Wireless Networks*(Cisco Press), *Implementing 802.1X Security Solutions* (Wiley), *Wireless Networking Handbook* (New Riders), and *Network Re-engineering* (McGraw-Hill). He has been an active participant in IEEE standards organizations, such as the IEEE 802.11 Working Group and the Wi-Fi Alliance. He has served as chairman of the IEEE Computer Society, Dayton Section, and various conferences. He has served as a testifying expert for patent litigation cases focusing on technologies dealing with wireless networking and cellular systems.

You can e-mail Jim Geier at jimgeier@wireless-nets.com.

About the Technical Reviewers

Jonathan E. Christman is vice-president of technology and co-founder at Health Grade Networks. He has more than 25 years of networking experience with more than 20 years dedicated to healthcare IT. He holds numerous certifications, including Cisco CCNP-Wireless, CCNA Routing and Switching, and CCDA, as well as other vendor-specific and vendor-neutral certifications. For the past 10 years, Jon has been working exclusively with wireless technologies, RFID/RTLS systems, and VoIP and VoWiFi systems in healthcare. Jon lives in the Firelands area of north-central Ohio with his beautiful wife and has two grown daughters.

George M. Stefanick, Jr. is a wireless architect employed by the Houston Methodist Hospital, where he manages 7 wireless distributions, 3,500 access points, and 30,000 wireless clients. George has been in wireless communications since 1997 and holds various vendor-specific and vendor-neutral certifications. George focuses on high-density indoor deployments in the healthcare vertical, leveraging his hands-on experience in site survey, RFID, and voice designs. George has consulted internationally and on many *Fortune 500* accounts. George was a Cisco Support Community VIP in 2012, 2013, and 2014, and an Aruba MVP in 2014 and 2015.

Dedication

I dedicate this book to my wife, Debbie.

Acknowledgments

I want to thank the Pearson production team for their time and effort with creating this book.

I also want to thank Jon Christman and George Stefanick for providing technical feedback on the many topics that this book covers.

Contents at a Glance

Introduction

Part I: Fundamental Concepts

Chapter 1 Introduction to Wireless LANs

Chapter 2 Radio Wave Fundamentals

Chapter 3 Wireless LAN Types and Components

Chapter 4 Wireless LAN Implications

Part II: The 802.11 Standard

Chapter 5 Introduction to IEEE 802.11 and Related Standards

Chapter 6 IEEE 802.11 Medium Access Control (MAC) Layer

Chapter 7 IEEE 802.11 Physical (PHY) Layers

Part III: Wireless Network Design

Chapter 8 Planning a Wireless LAN Deployment

Chapter 9 Defining Requirements for a Wireless LAN

Chapter 10 System Architecture Considerations

Chapter 11 Range, Performance, and Roaming Considerations

Chapter 12 Radio Frequency Considerations

Chapter 13 Security Considerations

Part IV: Wireless Network Installation and Testing

Chapter 14 Test Tools

Chapter 15 Performing a Wireless Site Survey

Chapter 16 Installing and Configuring a Wireless LAN

Chapter 17 Testing a Wireless LAN

Part V: Operational Support Considerations

Chapter 18 Managing a Wireless LAN

Chapter 19 Troubleshooting a Wireless LAN

Chapter 20 Preparing Operational Support Staff

Glossary

Index

Contents

Introduction

Part I: Fundamental Concepts

Chapter 1 Introduction to Wireless LANs

Wireless LAN Markets and Applications

Retail

Warehousing

Healthcare

Hospitality

Voice over WLAN

Video Surveillance

Home and Small Office

General Enterprise Systems

Location-Aware Wireless Applications

Benefits of Wireless Networks

Mobility

Installation in Difficult-to-Wire Areas

Increased Reliability

Reduced Installation Time

Long-Term Cost Savings

Productivity Gain Is the Answer

Wireless LAN Technologies

Initial 802.11

802.11a

802.11b

802.11g

Current Standards: 802.11n and 802.11ac

Comparison of 802.11 Standards

Wi-Fi Certification

Wireless LANs: A Historical Perspective

The Early Days

Initial 802.11 Standardization

802.11n and 802.11ac Standardization

Summary

Chapter 2 Radio Wave Fundamentals

Radio Wave Attributes

Amplitude

Frequency

Phase

RF System Components

RF Transceiver

RF Modulation

Amplitude-Shift Keying

Frequency-Shift Keying

Phase-Shift Keying

Quadrature Amplitude Modulation

Spread Spectrum

Orthogonal Frequency-Division Multiplexing

RF Signal Propagation

Attenuation

Free Space Loss

Physical Obstacles

Multipath Propagation

Noise and Signal-to-Noise Ratio

RF Mathematics

Converting Units

Summary

Chapter 3 Wireless LAN Types and Components

Types of Wireless LANs

Ad Hoc Wireless LANs

Infrastructure Wireless LANs

Wireless Mesh Networks

Wireless LAN Components

Client Devices

Client Radio

Industry Standard Architecture

Peripheral Component Interconnect

Mini-PCI

PC Card

ExpressCard

CompactFlash

Universal Serial Bus

Access Points

Autonomous Access Points

Controller-Based Access Points

Wi-Fi Routers

Mesh Nodes

Antennas

RF Amplifiers

Repeaters

Bridges

Network Infrastructure Components

Network Distribution Systems

Switches

Optical Fiber

Power over Ethernet

Application Connectivity Software

Terminal Emulation

Browser-Based Approaches

Direct Database Interfaces

Wireless Middleware

Summary

Chapter 4 Wireless LAN Implications

Security Vulnerabilities

Passive Monitoring

Unauthorized Access

Unauthorized Access Leads to Compromise of Financial Data

Denial-of-Service Attacks

Radio Signal Interference

Microwave Oven Interference

Cordless Phone Interference

Bluetooth Interference

Neighboring Wireless LAN Interference

Impacts of Multipath Propagation

Roaming Issues

Battery Limitations

Interoperability Problems

Installation Issues

Summary

Part II: The 802.11 Standard

Chapter 5 Introduction to IEEE 802.11 and Related Standards

The Importance of Standards

Types of Standards

Institute of Electrical and Electronics Engineers

Benefits of the 802.11 Standard

Appliance Interoperability

Fast Product Development

Stable Future Migration

Price Reductions

Avoiding Silos

The IEEE 802 LAN Standards Family

802.11 MAC Sublayer

802.11 Physical Layer

IEEE 802.2

Unacknowledged Connectionless Service

Connection-Oriented Service

Continuous ARQ

Stop-and-Wait ARQ

Acknowledged Connectionless Service

IEEE 802.11 Features

Station Services

Authentication

Deauthentication

Privacy

Distribution System Services

Association

Disassociation

Distribution

Integration

Re-association

Station States and Corresponding Frame Types

Summary

Chapter 6 IEEE 802.11 Medium Access Control (MAC) Layer

Primary 802.11 MAC Layer Functions

Data Delivery

Medium Access

Distributed Coordination Function

Hybrid Coordination Function

Error Recovery

Data Frame Acknowledgements

Dynamic Rate Switching

Data Frame Aggregation

MSDU Aggregation

MPDU Aggregation

Data Frame Fragmentation

Encryption

Wired Equivalent Privacy

Temporal Key Integrity Protocol

CCMP

Multicasting

Connectivity

Scanning for Networks

Authentication

Open System Authentication

Shared Key Authentication

IEEE 802.1X Port-Based Authentication

Associating with the Access Point

4-Way Handshake

Timing and Synchronization

Short IFS

PCF IFS

    - DCF IFS
    - Extended IFS
- RTS/CTS
    - Power Management
- 802.11 MAC Frame Structures
    - Protocol Version Field
    - Type Field
        - *Subtype Field*
    - To DS Field
    - From DS Field
    - More Frag Field
    - Retry Field
    - Power Management Field
    - More Data Field
    - Protected Frame Field
    - Order Field
    - Duration/ID Field
    - Address 1, 2, 3, and 4 Fields
    - Sequence Control Field
    - QoS Control Field
    - HT Control Field
    - Frame Body Field
    - Frame Check Sequence Field
- MAC Frame Types
    - Management Frames
        - *Association Request Frame*
        - *Association Response Frame*
        - *Re-association Request Frame*
        - *Re-association Response Frame*
        - *Probe Request Frame*
        - *Probe Response Frame*
        - *Beacon Frame*
        - *ATIM Frame*
        - *Disassociation Frame*
        - *Authentication Frame*

Deauthentication Frame

Action Frame

Action No ACK Frame

Management Frame Body Contents

Control Frames

Control Wrapper Frame

Block ACK Request Frame

Block ACK Frame

Power-Save Poll Frame

Request-to-Send Frame

Clear-to-Send Frame

Acknowledgement Frame

Contention-Free End Frame

CF End + CF ACK Frame

Data Frames

Interoperability

Summary

Chapter 7 IEEE 802.11 Physical (PHY) Layers

802.11 Physical Layer Architecture

PLCP Sublayer

PMD Sublayer

802.11 Physical Layer Functions

Carrier Sense Function

Transmit Function

Receive Function

Legacy 802.11 Physical Layers

Frequency-Hopping Spread Spectrum PHY

Direct-Sequence Spread Spectrum PHY

Infrared PHY

Orthogonal Frequency-Division Multiplexing PHY (802.11a)

High-Rate Direct-Sequence Spread Spectrum PHY (802.11b)

Extended-Rate PHY (802.11g)

High-Throughput (802.11n)

MIMO Concepts

Transmit Beamforming

Spatial Multiplexing
Channel Bonding
802.11n Modulation
Interoperability
Very High-Throughput 6 GHz (802.11ac)
RF Channel Bandwidth
Multi-User MIMO
Interoperability
Summary

Part III: Wireless Network Design

Chapter 8 Planning a Wireless LAN Deployment

Project Management Principles
Wireless LAN Deployment Planning Steps
Step 1: Defining the Project Scope
Project Charter
Assumptions
Constraints
Step 2: Developing the Work Breakdown Structure
Requirements Definition Phase
Design Phase
Implementation Phase
Operations and Maintenance Phase
Step 3: Identifying Staffing
Step 4: Creating a Schedule
Step 5: Developing a Budget
Preliminary Requirements and Design
Hardware and Software Costs
Deployment Services Costs
Ongoing Operations and Maintenance Costs
Step 6: Evaluating Risks
Step 7: Analyzing Feasibility
Costs
Benefits
Impacts on Users
Impacts on Existing Systems

Making the Decision to Proceed
Executing the Project
The Kickoff Meeting
Evaluating the Outcome of the Project
Summary

Chapter 9 Defining Requirements for a Wireless LAN

Requirements Attributes
Requirements Definition Steps
Step 1: Gathering Information
Interviewing Users
Interviewing IT Staff
Reviewing the Existing Infrastructure and Systems
Step 2: Analyzing Requirements
Application Requirements
Client Device Requirements
Signal Coverage Requirements
Utilization Requirements
Mobility Requirements
Security Requirements
Scalability Requirements
Existing Network Infrastructure Requirements
Environmental Requirements
Aesthetic Requirements
Step 3: Documenting Requirements
Step 4: Obtaining Requirements Approval
Summary

Chapter 10 System Architecture Considerations

Architectural Considerations
Wireless Access Networks
Autonomous Access Point Architecture
Controller-Based Access Point Architecture
Mesh Network Architecture
Ad Hoc Architecture
2.4-GHz Versus 5-GHz

Geographic Location Considerations

Performance Considerations

Existing Client Device Considerations

Facility Size Considerations

Radio Signal Interference Considerations

Hybrid Frequency Band Considerations

Common Infrastructure Considerations

Migration Considerations

Redundancy Considerations

Controller Redundancy

Access Point Redundancy

Distribution Systems

Switch Considerations

PoE Considerations

Voice over WLAN Systems

Single-Site Architecture

Multisite WAN with Centralized Call Processing

Multisite WAN with Distributed Call Processing

Application Connectivity

Terminal Emulation Considerations

Browser-Based Connectivity Considerations

Direct Database Considerations

Wireless Middleware Considerations

Summary

Chapter 11 Range, Performance, and Roaming Considerations

Range Versus Performance

Range Considerations

Signal Coverage Requirements

Radio Frequency Bands

Transmit Power Settings

Transmission Channel Settings

Data Rate Settings

Antennas

Amplifiers

Repeaters

- Physical Obstacles
- Radio Signal Interference

Performance Considerations

- Throughput Versus Data Rate
- Radio Frequency Bands
- Transmit Power Settings
- Transmission Channel Settings
- Data Rate Settings
- Antennas
- Amplifiers
- Radio Signal Interference
- Channel Width Settings
- Signal Coverage
- Fragmentation Settings
- RTS/CTS Settings
- Bandwidth Control Mechanisms
- Microcell Deployment Strategies

Roaming Considerations

- Roaming Levels
  - *Access Point Roaming*
  - *Subnet Roaming*
  - *Wireless ISP Roaming*
- Wireless IP Phone Roaming
- Mobility Settings

Summary

Chapter 12 Radio Frequency Considerations

Frequency Band Selection

- 2.4-GHz Frequency Band
- 5-GHz Frequency Band

Transmission Channel Settings

- Manual Channel Settings
  - *Single-Level Facilities*
  - *Multilevel Facilities*
- Adaptive Channel Settings

Difficult-to-Cover Areas

- Signal Coverage in Elevators
- Signal Coverage in Stairwells
- Signal Coverage in Parking Areas

Radio Signal Interference Reduction

Summary

Chapter 13 Security Considerations

Security Elements

Encryption

Authentication

- EAP Methods
- Authentication Servers
- Guest Access

Rogue Access Point Detection

RF Shielding

Wireless Security Policies

Summary

Part IV: Wireless Network Installation and Testing

Chapter 14 Test Tools

Tool Considerations

Spectrum Analyzers

- Real-Time Fast Fourier Transform
- FFT Duty Cycle
- Swept Spectrogram
- Active Devices
- Recording Spectrum Data

Signal Coverage Testers

- Heat Maps
- Positioning
- Passive Versus Active Modes
- Simulation
- Free Signal Coverage Tester: NetStumbler

Wireless Protocol Analyzers

- Filtering Frames
- Recording Traces

Free Protocol Analyzer: WireShark

Summary

Chapter 15 Performing a Wireless Site Survey

Wireless Site Survey Considerations

Reviewing Requirements

Selecting Site Survey Tools

Obtaining Floor Diagrams

Inspecting the Facility

Assessing the Existing Network Infrastructure

Communications Rooms

Switches and Power over Ethernet

WAN

Identifying Potential Radio Signal Interference

Defining Signal Values for Acceptable Signal Coverage

Minimum Received Signal Strength

Minimum SNR

Uplink Versus Downlink Signal Values

Identifying Optimum Access Point Antenna Installation Locations

Propagation Testing

Test Access Point Configuration

Antenna Considerations

Identifying Test Locations

Measuring Test Signals

Assessing Propagation Test Results

Cell Overlap Considerations

Annotating Access Point Antenna Installation Locations

Writing an RF Site Survey Report

Summary

Chapter 16 Installing and Configuring a Wireless LAN

Wireless LAN Installation Considerations

Planning the Installation

Developing an Installation Plan

Points of Contact

Safety Tips

Installation Procedures
Required Facility Changes
Tools
References to Design Documentation
Schedule
Resources
Budget
Risks
Coordinating the Installation
Staging the Components
Installing Access Points
Mounting Practices
Antenna Alignment
Configuring Access Points
Configuration Setting Access
Firmware
Access Point Configuration Settings
802.11n/ac Enable
SSID
Beacon Interval
Radio Frequency Bands
Transmit Power
Transmission Channel
Data Rates
Antenna Diversity
Channel Width
Fragmentation Threshold
RTS/CTS Threshold
Testing the Installation
Documenting the Installation
Summary
Chapter 17 Testing a Wireless LAN
Wireless LAN Testing Considerations
Signal Coverage Testing
Wireless Site Survey Coverage Testing

As-Installed Coverage Testing
Considering Beacon Rates
Performance Testing
Association Tests
Registration Tests
Authentication Tests
Network Connection Tests
Application Connection Tests
Application Tests
Load Tests
In-Motion Testing
Security Vulnerability Testing
Security Settings Verification
Penetration Testing
Private-Side Testing
Public-Side Testing
Acceptance/Verification Testing
Simulation Testing
Prototype Testing
Pilot Testing
Test Documentation
Summary

Part V: Operational Support Considerations

Chapter 18 Managing a Wireless LAN

Operational Support Considerations
Help Desk
Connection Problems
Poor Signal Coverage
Poor Performance
System Status
Additional Considerations
Network Monitoring
Performance Monitoring
Access Point Monitoring

- Configuration Monitoring
- Security Policy Management
  - *Installation Control Policies*
  - *Monitoring Policies*
  - *Periodic Testing Policies*

Maintenance
- Inoperative Access Points
- Poor Performance
- Poor Signal Coverage
- Broken Hardware
- Firmware Updates
- Signal Coverage Verification
- Access Point Inspections
- Troubleshooting

Sparing

Engineering
- Advanced Problem Resolution
- Coverage Expansion
- Capacity Increases
- Firmware Review
- Technology Upgrades
- Design Review

Configuration Management
- Change-Control Processes

Security Management
- Reviewing Existing Security Policies
- Reviewing the System Architecture
- Reviewing Management Tools and Procedures
- Interviewing Users
- Verifying Configurations of Wireless Devices
- Investigating Physical Installations of Access Points
- Identifying Rogue Access Points
- Performing Penetration Tests
- Analyzing Security Gaps
- Recommending Improvements

- Trouble Ticket Coordination
    - Help Desk Group
    - Desktop Support Group
    - Network Support Group
- Preparing for the Transfer to Operational Mode
- Summary

Chapter 19 Troubleshooting a Wireless LAN

- Troubleshooting Methodology
    - Identifying the Problem
    - Identifying the Underlying Cause of the Problem
    - Fixing the Problem
- Connection Problems
    - Insufficient Signal Coverage
    - Radio Signal Interference
    - Access Point Failure
    - Incompatible Client Radio
    - Faulty Firmware
    - Incorrect Client Radio Configuration
- Performance Problems
    - Insufficient Signal Coverage
    - Radio Signal Interference
    - Faulty Firmware
    - Non-optimal Client Radio Configuration
    - Non-optimal Access Point Configuration
    - Misaligned Antennas
    - High Utilization
- Summary

Chapter 20 Preparing Operational Support Staff

- Support Staff Considerations
- Availability of Existing Staff
- Experience Requirements
- Education and Training Requirements
    - Vendor-Neutral Training
    - Vendor-Specific Training

College Education

Certifications

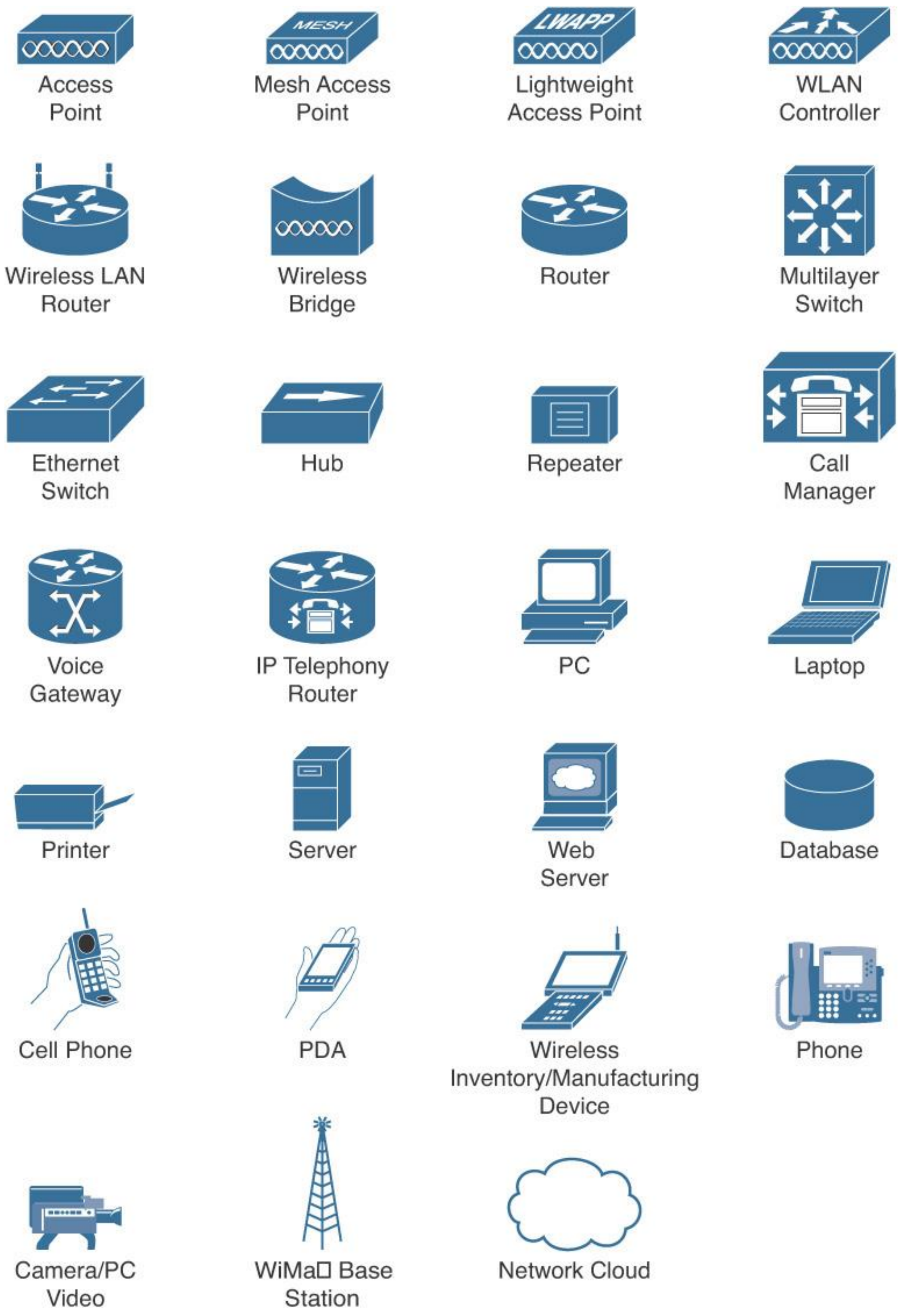
Staffing Sources

Summary

Glossary

Index

Icons Used in This Book



Introduction

The 802.11ac amendment to the IEEE 802.11 wireless LAN (WLAN) standard was ratified in 2013, enabling 802.11 systems to provide significantly higher performance in the 5-GHz band. Network equipment manufacturers now offer 802.11ac-compliant equipment in addition to 802.11n (2.4 GHz) as their primary WLAN solutions. WLANs based on earlier versions of the standard (802.11a, 802.11b, and 802.11g) are considered "legacy," and there is significant risk that these existing non-802.11n/ac systems will become obsolete. As a result, organizations deploying new WLANs should definitely implement 802.11ac and 802.11n-compliant equipment. In addition, organizations with existing non-802.11n/ac WLANs should begin planning the migration to 802.11ac and 802.11n-compliant networks.

This book focuses on planning, designing, installing, testing, and supporting 802.11ac and 802.11n wireless networks for a variety of applications. The methods, recommendations, and tips in this book are based on the author's many years of practical experience deploying WLANs. Organizations with no existing wireless network and those migrating from legacy wireless networks to 802.11ac- and 802.11n-compliant networks will find this book to be a valuable guide.

Goals and Methods

The overall goal of this book is to guide you through the steps of deploying an 802.l1n WLAN. To accomplish this, the book includes the following elements:

Step-by-step approach: The book breaks each phase of WLAN deployment into clearly defined steps that provide the basis for understanding and planning the details of the phase.

Case studies: The book includes several case studies that provide explanations of concepts and methods as they are practiced in actual deployments.

Hands-on exercises: The book includes exercises that make use of free and inexpensive tools that help you gain practical experience with concepts described in the chapter.

Notes: Concise notes are distributed throughout the book and provide insightful information related to deploying WLANs.

Who Should Read This Book?

This book is intended for a variety of people, from someone with basic knowledge of networking to those who have years of experience working with WLANs but have little or no experience implementing 802.11 networks.

How This Book Is Organized

Although this book can be read cover to cover, it is designed to be flexible and allow you to easily move between chapters and sections of chapters to learn just the information that you need.

This book covers the following topics:

Part I, "Fundamental Concepts": This part of the book includes chapters that cover important underlying concepts that must be understood before deploying an 802.11 wireless network. Readers already familiar with WLANs may be able to skip one or more of the chapters in this part of the book.

Chapter 1, "Introduction to Wireless LANs": This chapter defines the markets and applications of WLANs and the wireless technologies that support them.

Chapter 2, "Radio Wave Fundamentals": This chapter explains radio wave fundamentals so that you have a basis for understanding the complexities of deploying WLANs.

Chapter 3, "Wireless LAN Types and Components": This chapter describes ad hoc, mesh, and infrastructure WLAN types and various components, such as access points, controllers, client radios, and amplifiers.

Chapter 4, "Wireless LAN Implications": This chapter explains the impacts of radio signal interference, security vulnerabilities, multipath propagation, roaming, and battery limitations on WLANs.

Part II, "The 802.11 Standard": This part of the book provides in-depth coverage of the most current medium access and physical layers of the IEEE 802.11 standard (including 802.11ac and 802.11n functionality). The focus here is on the elements of the standard that you should know to be successful at deploying and supporting 802.11 wireless networks.

Chapter 5, "Introduction to IEEE 802.11 and Related Standards": This chapter provides background on the 802.11 standards and an overview of the 802.11 standard and related standards, such as IEEE 802.2.

Chapter 6, "IEEE 802.11 Medium Access Control (MAC) Layer": This chapter explains details of the 802.11 standard that you need to know to help you best configure and troubleshoot 802.11 WLANs.

Chapter 7, "IEEE 802.11 Physical (PHY) Layers": This chapter describes the modulation functions that are part of the 802.11 physical layers.

Part III, "Wireless Network Design": This part of the book includes chapters that cover steps necessary to design an 802.11 wireless network for various scenarios.

Chapter 8, "Planning a Wireless LAN Deployment": This chapter provides an overview of the steps you need to complete when deploying a WLAN and details on defining the project scope, developing a work breakdown structure, identifying staffing, creating a schedule, developing a budget, evaluating risks, and analyzing feasibility.

Chapter 9, "Defining Requirements for a Wireless LAN": This chapter explains how to gather, analyze, and document requirements for an 802.11 WLAN.

Chapter 10, "System Architecture Considerations": This chapter explains what to consider when designing the access network and distribution system for an 802.11 WLAN.

Chapter 11, "Range, Performance, and Roaming Considerations": This chapter explains the various trade-offs for enhancing the range, performance, and roaming capabilities of an 802.11 wireless LAN.

Chapter 12, "Radio Frequency Considerations": This chapter covers important radio frequency (RF) design considerations for 802.11 WLANs, such as frequency band selection, transmission channel settings, difficult-to-cover areas, and radio signal interference reduction techniques.

Chapter 13, "Security Considerations": This chapter explains important methods and techniques for securing a WLAN, including encryption, authentication, rogue access point detection, RF shielding, and security policies.

Part IV, "Wireless Network Installation and Testing": This part of the book explains the steps necessary to install and test an 802.11 wireless network.

Chapter 14, "Test Tools": This chapter describes the tools that you need to effectively design and support an 802.11 WLAN.

Chapter 15, "Performing a Wireless Site Survey": This chapter explains the steps and techniques, such as inspecting the existing network, analyzing radio signal interference, and performing signal propagation testing, that are needed to determine the optimum installation locations for access points.

Chapter 16, "Installing and Configuring a Wireless LAN": This chapter explains how to plan the installation, stage the components, install the access points, and document the installation of a WLAN.

Chapter 17, "Testing a Wireless LAN": This chapter describes the steps and techniques necessary to test a wireless LAN, including signal coverage testing, performance testing, in-motion testing, security testing, acceptance testing, simulation testing, prototype testing, and pilot testing.

Part V, "Operational Support Considerations": This part of the book explains what to consider when supporting an 802.11 wireless network. Readers will learn how to establish specialized support for wireless networks and perform help desk operations, network monitoring, and troubleshooting.

Chapter 18, "Managing a Wireless LAN": This chapter describes important operations and maintenance functions that you should consider when supporting a WLAN, including help desk, network monitoring, maintenance, engineering, configuration management, security management, trouble ticket coordination, operational support tools, and operational support transfer preparation.

Chapter 19, "Troubleshooting a Wireless LAN": This chapter explains how to identify problems, such as connectivity and performance issues, and determine the underlying causes.

Chapter 20, "Preparing Operational Support Staff": This chapter describes what you should consider when evaluating the experience and education of staff for supporting a wireless LAN.

Glossary: The glossary defines terms that this book uses.

Hands-on Exercises

As mentioned in the "Goals and Methods" section, this book includes exercises that make use of free and inexpensive tools that help you gain practical experience with the concepts described. You can find these exercises on the following pages:

Chapter 4

Hands-on Exercise: Passively Monitor a Wireless LAN—78

Hands-on Exercise: Understand Basic Performance Impacts of Radio Signal Interference—94

Chapter 6

Hands-on Exercise: Observing 802.11 Dynamic Rate Shifting—130

Hands-on Exercise: Observing 802.11 Active Scanning—139

Hands-on Exercise: Observing the 802.11 Connection Process—143

Hands-on Exercise: Observing 802.11 Beacons—158

Hands-on Exercise: Observing 802.11 Frames Resulting from Typical User Traffic—164

Chapter 7

Hands-on Exercise: Understanding Performance Impacts of Increasing 802.11n Spatial Streams—182

Hands-on Exercise: Understanding Performance Impacts of 802.11n Channel Bonding—183

Chapter 11

Hands-on Exercise: Analyzing Impacts on Range Using Different Data Rate Settings—293

Part I: Fundamental Concepts

Chapter 1. Introduction to Wireless LANs

This chapter will introduce you to:

Wireless LAN Markets and Applications

Benefits of Wireless Networks

Wireless LAN Technologies

Wireless LANs: A Historical Perspective

Applications of wireless local-area networks (WLANs) have become commonplace in many markets throughout the world. Newer WLANs based on the 802.11n and 802.11ac standards now offer the performance needed to effectively support a high density of users and a broad range of high-end applications, such as voice, video, and image processing. This chapter defines the markets and applications of WLANs and the wireless technologies that support them.

Wireless LAN Markets and Applications

In general, WLANs are applicable to all markets with a need for user mobility or when the installation of physical media is not feasible. WLANs are especially useful when employees must process information on the spot via electronic-based forms and interactive menus. Wireless networking makes it possible to place portable computing devices in the hands of mobile users, such as doctors, nurses, warehouse clerks, inspectors, claims adjusters, real estate agents, and salespeople.

The implementation of portable devices with wireless connectivity facilitates access to a common database and applications that meet the needs of users, eliminate unnecessary paperwork, decrease errors, reduce processing costs, and improve overall efficiency. It also introduces user mobility by allowing the user to move from one WLAN to another seamlessly. The alternative to this, which many companies still employ today, is using paperwork to update records, process inventories, and file claims. This method processes information much more slowly, produces redundant data, and is subject to input errors caused by illegible handwriting. The approach to mobile computing over a WLAN using a centralized database enhances productivity and is clearly a superior approach.

The sections that follow provide a general description of the WLAN market and applications within that market. This will help stimulate ideas with regard to how WLANs will benefit your company or organization.

Retail

Retail organizations need to order, price, sell, and manage inventories of merchandise. A wireless network in a retail environment enables clerks and storeroom personnel to perform their functions directly from the sales floor. Salespeople are equipped with a pen-based computer or a small computing device with bar code reading and printing capabilities, while connected to the store’s database via the WLAN. They can then complete transactions such as pricing, labeling bins, placing special orders, and taking inventory from anywhere within the store.

When printing price labels that will be affixed to items or shelves, retailers often use a handheld bar code scanner and printer to produce bar coded or human-readable labels. A database or file contains the price information located either on the handheld device, often called a batch device, or on a server somewhere in the store. In batch mode, the price clerk scans the bar code (typically the product code) located on the item or shelf edge, the application software uses the product code to look up the new price, and then the printer produces a new label that the clerk affixes to the item.

In some cases, the batch-based scanner/printer has enough memory to store all the price information needed to perform the pricing functions throughout a shift or an entire day. This situation makes sense if the user needs to update pricing information in the database through the day, typically during the evening. The clerks load the data onto the device at the beginning of their shifts and then walk throughout the store, pricing items. However, if the memory in the device is not large enough to store all the data or if updates to the server need to be done in real time, a wireless network is necessary. If the handheld unit is equipped with a wireless network connection, the handheld can be configured for a WLAN, and data can be stored on a centralized server and accessed each time an item’s bar code is scanned. In addition, a wireless network–based solution has merit if downloading information to a batch device is too time consuming.

Warehousing

Warehouse staff must manage the receiving, shelving, inventorying, picking, and shipping of goods. These responsibilities require the staff to be mobile. Warehouse operations traditionally have been paper intensive and time consuming. An organization can eliminate paper, reduce errors, and decrease the time necessary to move items in and out by giving each warehouse employee a mobile handheld computing device with an Intermec bar code scanner, for example, connected via a wireless network to a warehouse inventory system.

Upon receiving an item for storage within the warehouse, a clerk can scan the item's bar coded item number and enter other information from a small keypad into the database via the handheld device. The system can respond with a location by printing a put-away label. A forklift operator can then move the item to a storage place and account for the procedure by scanning the item's bar code. The inventory control system keeps track of all transactions, making it very easy to produce accurate inventory reports. In addition, the online interaction with a database will identify mistakes immediately, enabling the operator to correct a mistake before it becomes a problem.

As shipping orders enter the warehouse, the inventory system produces a list of the items and their locations. A clerk can view this list from the database via a handheld device and locate the items needed to assemble a shipment. As the clerk removes the items from the storage bins, the database can be updated via the handheld device. All these functions depend heavily on wireless networks to maintain real-time access to data stored in a central database.

Warehouses involve a host of functions where the use of wireless IP phones can provide significant benefits. Clerks end up being scattered throughout the warehouse facility, which can be quite expansive, and communications with other clerks and managers is essential to perform various functions. In most cases, it is not practical for the clerks and managers to meet face to face to communicate. In fact, it is often not possible for them to even find each other because of the numerous rows of bins and products. For example, an order may come in for the shipment of a particular item to a customer. Rather than wait for a clerk to return to the main office, it is much faster and productive for the shipping department to call a clerk directly and have the clerk pick the item.

Wireless Bar Code System for Warehouses

A manufacturer in North America is a leading provider of bar code printers and supplies. As part of the company's goal to streamline processes within its manufacturing plant and warehouse, a process improvement team applied the use of mobile handheld bar code scanning and printing devices with the support of a WLAN within its central distribution center (CDC).

Before the system was implemented, the CDC was experiencing inefficiencies because clerks needed to walk back and forth between stacks of finished goods and a desktop terminalused to determine a warehouse storage location for the items. The clerks would collect information from the finished goods by writing it down on a piece of paper, and then they would walk to the terminal to query the company's warehouse management system for a recommended storage location. The clerk would write this location information on a large label, walk back to the product, and affix the label to the product's container. Later, a forklift operator would come by and place the container in the correct location on the warehouse floor. The process of walking back and forth between the products and the terminal made inefficient use of the clerk's time, which slowed the movement of products through the plant.

The solution to this problem consists of a bar code scanner equipped with a radio card and a WLAN. 802.11 access points throughout the warehouse connect to an Ethernet network that interfaces to a server running a warehouse management system. The clerk can now scan the finished product's bar code, which is used to query the warehouse management system for a valid put-away location. The system then prints a label on a printer connected to the bar code scanner indicating the applicable location information.

Through the use of this scan, print, and apply function, the solution eliminates the need for the clerk to walk back and forth to the terminal, increasing productivity by 50 percent. In addition, the solution provides significant gains in accuracy through the elimination of human error.

Many warehouses already have existing WLANs; however, because these wireless networks primarily support relatively low-performance bar code solutions for implementing inventory management functions, such an existing WLAN will likely not have enough capacity to support a large number of wireless IP phones. In most cases, the much higher capacity of 802.11n and 802.11ac networks is necessary to support voice applications in warehouses.

Healthcare

Healthcare centers, such as hospitals and doctor's offices, must maintain accurate records to ensure effective patient care. A simple mistake can cost someone's life. As a result, doctors and nurses must carefully record test results, physical data, pharmaceutical orders, and surgical procedures. This paperwork often overwhelms healthcare staff, taking 50 percent to 70 percent of their time.

Doctors and nurses are also extremely mobile, going from room to room as they care for patients. The use of electronic patient records, with the capability to input, view, and update patient data from anywhere in the hospital, increases the accuracy and speed of healthcare. This improvement is made possible by providing each nurse and doctor with a wireless pen-based computer, coupled with a wireless network connected to databases that store critical medical information about the patients.

A doctor caring for someone at the hospital, for example, can place an order for a blood test by keying the request into a handheld computer. The laboratory will receive the order electronically and dispatch a lab technician to draw blood from the patient. The laboratory will run the tests requested by the doctor and enter the results into the patient's electronic medical record. The doctor can then check the results via the handheld appliance from anywhere in the hospital.

Wireless LANs also help patients in hospitals. Patient monitoring devices, such as those from Draeger and Mindray, monitor the vital signs of patients and wirelessly send the information to monitors located in the patient rooms and nursing stations. This allows patients to get out of bed and move around their room without the nuisance of cables attaching them to monitoring equipment.

Another application for wireless networks in hospitals is the tracking of pharmaceuticals. The use of mobile handheld bar code printing and scanning devices dramatically increases the efficiency and accuracy of all drug transactions, such as receiving, picking, dispensing, inventory taking, and tracking of drug expiration dates. Most importantly, though, it ensures that hospital staff is able to administer the right drug to the right person at the right time. This would not be possible without the use of wireless networks to support a centralized database and mobile data collection devices.

Hospitals were some of the first users of wireless IP phones, mainly because of the significant needs for effective communications among high-valued medical staff. The ability for doctors and nurses to respond quickly with verbal instructions is crucial in saving the lives of patients. Patients receive a higher level of care, which leads to faster recovery.

Wireless IP phones allow hospital staff to not waste time looking for a phone to use.

An issue with deploying voice over wireless solutions in hospitals, however, is the difficulty in providing adequate WLAN coverage. Hospitals include x-ray rooms surrounded by lead, irregular metal objects, and unpredictable traffic flows of people. This leads to significant attenuation and multipath propagation. In addition, radio frequency (RF) interference from other wireless systems operating in the 2.4-GHz band, such as frequency-hopping spread spectrum devices, can cause degradation in performance. As a result, a wireless site survey is absolutely necessary to ensure that the network fully meets all requirements.

Hospitality

Hospitality establishments check customers in and out and keep track of needs such as room service orders and laundry requests. Restaurants need to keep track of the names and numbers of people waiting for entry, table status, and drink and food orders. Restaurant staff must perform these activities quickly and accurately to avoid making patrons unhappy. Wireless networking satisfies these needs very well.

Wireless computers are very useful in situations where there is a large crowd, such as a sports bar restaurant. For example, someone can greet a restaurant patron at the door and enter his name, the size of the party, and smoking preferences into a common database via a wireless device. The greeter can then query the database and determine the availability of an appropriate table. Those who oversee the tables use a wireless device to update the database to show whether the table is occupied, being cleaned, or available. After obtaining a table, the waiter transmits the order to the kitchen via the wireless device, eliminating the need for paper order tickets. Keep in mind, however, that the wireless network approach in finer restaurants may not be appealing to patrons. In that case, the patrons may expect waiters to memorize their orders.

Voice over WLAN

Voice over WLAN (VoWLAN) systems are an extension to wired VoIP systems and an alternative to traditional analog and digital voice communications. VoWLANs offer significant benefits of providing mobility and wirelessly converging voice with data applications. With VoWLANs, hospitals, enterprises, retail stores, warehouses, and homeowners can reduce telephony costs and enable mobile applications.

Examples of the systems that VoWLANs can replace include the following:

- Wired telephones
- Cellular telephones
- Two-way radios

With VoWLANs, individuals and teams can use VoWLAN phones to communicate by voice over the WLAN to others inside and outside a facility. The experience is similar to using a traditional wired telephone; however, the user is free to roam about the building where Wi-Fi has been deployed. Furthermore, a VoWLAN phone can operate from many of the growing number of Wi-Fi hotspots, allowing a person to make use of the same mobile phone while within or away from the office or home. Some cellular phones incorporate VoWLAN capability, which allows users to make calls over traditional cellular networks when no WLAN is available and then switch to a WLAN seamlessly when the user roams onto the Wi-Fi-enabled network.

Figure 1-1 illustrates the basic usage models of a VoWLAN system. The optimum approach depends on user requirements and existing telephone hardware.

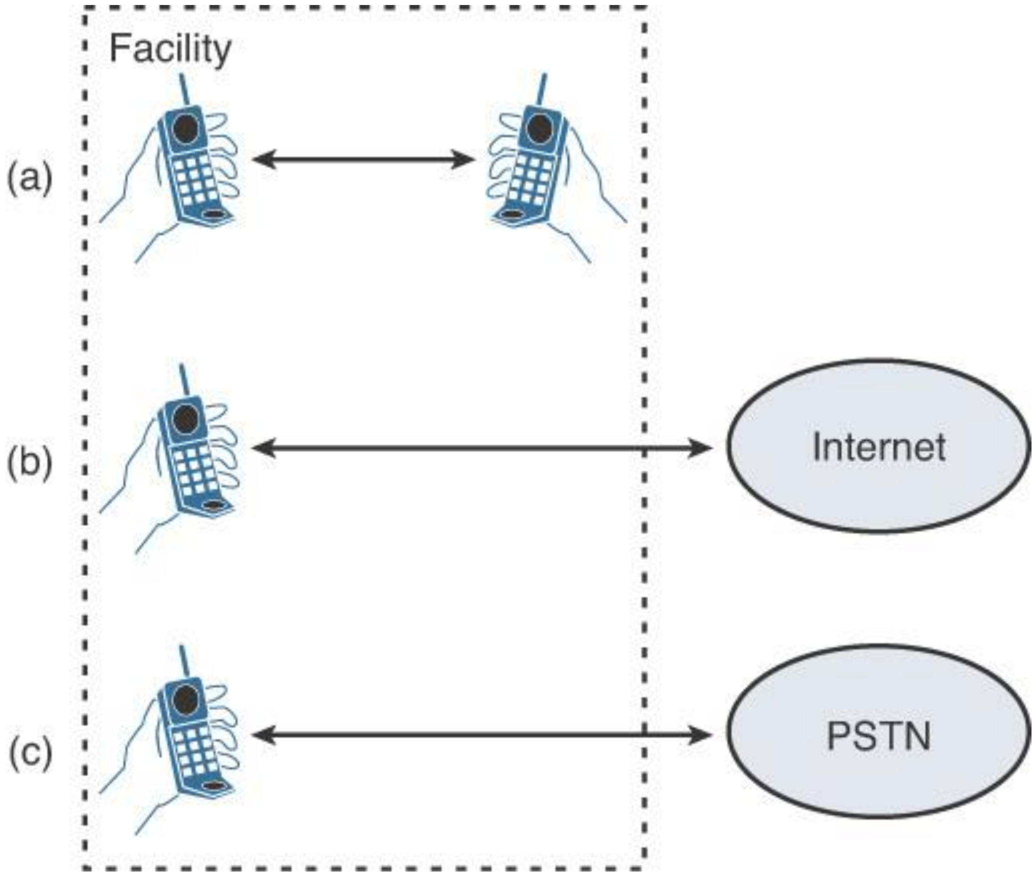


Figure 1-1 *VoWLAN Usage Models: (a) Local-Only, (b) Telephone via Internet, (c) Telephone via PSTN*

Video Surveillance

Several companies sell small video cameras that relay moving images to monitors and recording devices over WLANs. The installation of these cameras is much easier than with traditional ones because there is no need to run wires between the cameras and the company’s network. The video signals flow over a WLAN and into a video server or PC. As a result, a company can set up a Wi-Fi video surveillance system much faster and in scenarios where it is not feasible to install traditional wired cameras.

Wireless video surveillance is beneficial for many industries. For example, the San Mateo County Courthouse installed Wi-Fi video cameras. With this system, security officials could keep a continual eye on crowds and their behavior. In addition, public facilities, such as hotels and shopping malls, use Wi-Fi cameras to watch over shopping areas, inside elevators, and near exit doors. Enterprises are also taking advantage of Wi-Fi cameras to monitor lobby entrances and parking lots.

Home and Small Office

With a WLAN, employees can bring laptops home from work and continue working just as they do from their offices. For many professions, this makes it possible for people to work from home more effectively, whether it is to spend a few more hours researching on the Internet or to enable telecommuting on a daily basis.

Of course with a wireless laptop, a person can truly work from any place in the house. There is nothing tying you down to a desk in a particular room. You are free to use the Internet or access files on other computers while relaxing in a comfy chair in front of a TV, lounging on the patio breathing fresh air, or sitting at a desk in a quiet bedroom.

WLANs at home are good for PCs, too. Unlike in companies, most homes are not wired with Ethernet cabling. That makes wireless the best way to connect stationary PCs to the network. You will have much more flexibility in locating a PC to any part of the house without being near the broadband modem.

Many homes now have more than one computer. After purchasing a new PC, homeowners will generally hold on to the older PC. It might not be the best for running some of the newer games, but it still offers a good station for browsing the web and interacting with e-mail. Of course, some people will also bring a laptop home from work or purchase one instead of upgrading to a newer PC.

With multiple computers, it is extremely beneficial for home users to connect to the same broadband connection. Because of the ease of installation, a WLAN is the best solution for sharing access to the Internet and other PCs in the home. Just be sure to install a WLAN router (not an access point) to ensure that you have Network Address Translation (NAT) and Dynamic Host Configuration Protocol (DHCP) services, which are necessary for all the computers to share a single official IP address supplied by your Internet service provider.

Without a WLAN, most home users must cable their printer directly to a PC or the Ethernet connector on a broadband modem. This limits the number of places that the printer can reside. Generally, it must sit within a few feet of the PC or modem.

A Wi-Fi print server, however, enables the printer to be accessible over the WLAN. This makes printer placement extremely flexible. For example, you might find it most useful to have the printer in the family room, where you do most of your laptop computing. Or it might make more sense to have the printer just inside the door that leads to your patio. You can also easily move a Wi-Fi-connected printer to new locations whenever you want to.

General Enterprise Systems

In the past, the implementation of a WLAN was relatively expensive compared to the implementation of higher-performing Ethernet networks. This required a WLAN application to provide a tremendous gain in efficiency to make it cost effective. As a result, many existing applications of WLANs are in markets such as healthcare, warehousing, and retail, where mobility provided efficiency gains capable of significantly lowering operational costs. With WLAN prices continuing to drop and performance increasing with 802.11n and 802.11ac, though, many enterprise information system managers are beginning to seriously consider the use of WLANs rather than traditional Ethernet. The benefits are provision of mobile and portable access to general network functions such as e-mail, Internet browsing, access to databases, and so on and elimination of the time and expense of installing and supporting physical cable. Thus, WLANs are now effectively satisfying applications in horizontal markets.

An oil exploration company operating in Colombia, South America, experienced high expenses when relocating its drilling rigs. The oil-drilling setup required two control rooms in portable sheds separated 5,000 feet from the drilling platform to provide 500 Kbps computer communication between the sheds and the drilling rig. The existing communications system consisted of Ethernet networks at each of the three sites. Each shed had four PCs running on the network, and the drilling site had one PC for direct drilling-control purposes.

Every time the oil company needed to move to a different drilling site, which occurred four or five times each year, it had to spend between $50,000 and $75,000 to reinstall optical fiber through the difficult terrain between the sheds and the drilling platform. With rewiring expenses reaching as high as $375,000 per year, the onsite system engineer designed a wireless point-to-point system to accommodate the portability requirements to significantly reduce the cost of relocating the drilling operation. The solution includes a spread-spectrum radio-based wireless system that uses directional antennas to establish point-to-point communication between the sheds and the drilling platform.

The cost of purchasing the wireless network components was approximately $10,000. Wherever the oil company now moves its drilling operation, it will save the costs of laying a new cabling infrastructure between the sites.

Location-Aware Wireless Applications

More and more companies are beginning to apply location-based services over wireless networks to enable rather interesting enhancements to applications. In general, a location-based system (LBS) keeps track of the position of users on the network as they roam throughout the facility. A centralized system collects and integrates this positioning information to drive additional functions that identify the position of users in relation to the facility and pertinent areas, such as information booths, emergency centers, stores, products, and so on.

Within healthcare facilities, doctors, nurses, and, sometimes, patients are very mobile. As a result, many hospitals have WLANs to support patient monitoring, electronic patient records, and narcotics tracking. In this situation, an LBS can also track doctors throughout the hospital, which enables a nurse to know whether a particular doctor is nearby and able to take care of a specific emergency.

In addition, an LBS enables hospital staff to track the whereabouts of patients, and if they go astray or anything adverse happens to them, an alarm system will alert the closest doctors and nurses. For example, some homes for the elderly implement LBSs over WLANs to trigger an alarm when patients try to leave the facility.

Hospitals also need to track expensive equipment that is often required to save lives. An LBS enables hospital administration to know the exact location of this equipment for accountability and usability purposes. If a nurse needs a specific portable x-ray machine in the emergency room, stat, the LBS can display where to find it. If it leaves the facility, chokepoints can be installed in major corridors or exits, showing when a piece of equipment or a user leaves a given area of the hospital or passes through an exit where a chokepoint is installed.

Department stores and shopping malls can reap huge benefits from LBSs. A customer can use his or her smart phone to download an interactive store map and find the exact location of any item within the store. By entering a few search criteria, the smart phone can provide a description of where the item has been moved on the WLAN. The same concept also applies to shopping malls. A WLAN can cover the entire parking lot and the inside of a large shopping mall, and customers using a smart phone are able to more easily find stores. Once a customer is in the mall, a real-time map constantly shows the shopper where each store is in relation to his/her position. The LBS can also send promotions from specific stores as shoppers pass by them.

An LBS also provides convenience to people in large public areas. In a convention center, for example, a wireless user can take advantage of moving maps that identify meeting rooms, positions of vendors on a tradeshow floor, and emergency exits in relation to the position of the user.

As a patron using a smart phone passes a specific display case at a museum, an LBS can download voice and possibly video information describing the contents of the display. The user can move about the museum and receive location-based information, which enhances the learning and enjoyment of the visitor.

Similar to a convention center, in an airport, wireless users can also easily find their way around by using an LBS solution. For example, the LBS can display routes to various locations, such as restaurants, coffee shops, and emergency exits. Tenants within the airport can also display location-aware advertisements, which offer the airport a revenue stream for advertising in addition to network access.

An LBS can make the job of security guards immensely easier. The security control room can constantly track the position of every guard and alert others when there is an incident occurring in an area. All of this traverses the WLAN. Of course, this means that the WLAN requires enhanced security mechanisms to ensure that this information is not available to thieves.

Because of the vast amounts of data, such as maps and tracking updates, that an LBS generates, the higher performance and reliability of 802.l1n and 802.11ac are imperative. This is especially true when supporting LBS in addition to other wireless applications, such as voice.

Case Study 1-1: Acme Healthcare Is Ready to Go Wireless

Acme Healthcare is a fictitious 250-bed acute care hospital that surfaces throughout this book to emphasize the primary considerations when deploying an 802.11 wireless network.

Acme Healthcare serves the healthcare needs of a medium-sized community in the United States. The hospital has very few wireless networks, which are mainly operated independently by several of the clinics. The existing networks are a mix of 802.11g and 802.11n networks, and they primarily serve connections between laptops and the hospital’s healthcare information system.

The hospital CIO, Arthur, has attended a couple of healthcare conferences and learned that many of the other hospitals are in the process of deploying WLANs to support mobile applications, such as voice communications, electronic medical records, x-ray image distribution, video surveillance, asset tracking, patient monitoring, and foreign language translator systems. Arthur envisions similar applications and substantial resulting benefits for his hospital. With the masses of baby boomers getting older, Acme Hospital’s profit has been increasing steadily over the past few years, and Arthur is now ready to move forward with a hospital-wide wireless system.

Note

Upgrade your existing network to all 802.11n and 802.11ac to support higher-speed mobile applications and avoid implications of the legacy WLANs (802.11a, 802.11b, 802.11g) that have become obsolete.

Benefits of Wireless Networks

The emergence and continual growth of WLANs are being driven by the need to lower the costs associated with network infrastructures and to support mobile networking applications that offer gains in process efficiency, accuracy, and lower business costs. The following sections explain the mobility and cost-saving benefits of WLANs so that you can better justify the expense of deploying a WLAN.

Mobility

Mobility enables users to move physically while using an appliance, such as a wireless laptop, smart phone, or data collector. Many employers require their employees to be mobile in an effort to increase efficiency. Inventory clerks, healthcare workers, police officers, and emergency care specialists, for example, are ideal candidates who can benefit from wireless mobility.

Of course, wired networks require a physical tether between a user’s workstation and a network’s resources, which makes access to these resources impossible while roaming about their work environment. Wireless mobility increases the users’ freedom of movement and results in significant return on investment because of gains in efficiency.

Mobile applications requiring wireless networking include those that depend on real-time access to data, which is usually stored in centralized databases. If your applications require mobile users to be aware immediately of changes made to data, or if information put into the system must immediately be available to others, you have a definite need for wireless networking. For accurate and efficient price markdowns, for example, many retail stores use wireless networks to interconnect handheld bar code scanners and printers to databases containing current price information. This enables the printing of the correct prices on the items, making both the customer and the business owner more satisfied.

Installation in Difficult-to-Wire Areas

The implementation of wireless networks offers many tangible cost savings when performing installations in difficult-to-wire areas. If rivers, freeways, or other obstacles separate buildings you want to connect, a wireless solution may be much more economical than installing physical cable or leasing communications circuits, such as T1 service. Some organizations spend thousands or even millions of dollars on installing physical links with nearby facilities. 802.11n bridges, coupled with directional antennas, can easily provide wireless connectivity over thousands of feet, depending on obstacles along the path.

The asbestos found in older facilities is another problem that many organizations encounter. The inhalation of asbestos particles is extremely hazardous to your health; therefore, you must take great care when installing network cabling within these areas. When taking necessary precautions, the resulting cost of cable installations in these facilities can be prohibitive.

Some organizations, for example, remove the asbestos, making it safe to install cabling. This process is very expensive because you must protect the building's occupants from breathing the asbestos particles agitated during removal. The cost of removing asbestos covering just a few flights of stairs can be tens of thousands of dollars. Obviously, the advantage of wireless networking in asbestos-contaminated buildings is that you can avoid the asbestos removal process, resulting in tremendous cost savings.

In some cases, it might be impossible to install cabling. Some municipalities, for example, might restrict you from permanently modifying older facilities with historical value. This could limit the drilling of holes in walls during the installation of network cabling and outlets. In such a situation, a wireless network might be the only solution. Right-of-way restrictions within cities and counties might also block the digging of trenches in the ground to lay optical fiber for networked sites. Again, in this situation, a wireless network might be the best alternative.

Increased Reliability

A problem inherent in wired networks is downtime because of cable faults. Moisture erodes metallic conductors via water intrusion during storms and accidental spillage or leakage of liquids. With wired networks, a user might accidentally break his/her network connector when trying to disconnect his/her PC from the network to move it to a different location. Imperfect cable splices can cause signal reflections that result in unexplainable errors. The accidental cutting of cables can bring down a network immediately. Wires and connectors can easily break through misuse and normal use. These problems interfere with users' ability to use network resources, causing havoc for network managers. An advantage of wireless networking, therefore, results from the use of less cable. This reduces the downtime of the network and the costs associated with replacing cables.

Reduced Installation Time

The installation of cabling is often a time-consuming activity. For LANs, installers must pull twisted-pair wires or optical fiber above the ceiling and drop cables through walls to network outlets that they must affix to the wall. These tasks can take days or weeks, depending on the size of the installation. The installation of optical fiber between buildings within the same geographic area consists of digging trenches to lay the fiber or pulling the fiber through an existing conduit. You might need weeks or possibly months to receive right-of-way approvals and dig through ground and asphalt.

The deployment of wireless networks greatly reduces the need for cable installation, making the network available for use much sooner. Thus, many countries that lack network infrastructure have turned to wireless networking as a method of providing connectivity among computers without the expense and time associated with installing physical media. This is also necessary within the United States to set up temporary offices and rewire renovated facilities.

Long-Term Cost Savings

Companies reorganize, resulting in the movement of people, new floor plans, office partitions, and other renovations. These changes often require rewiring the network, incurring both labor and material costs. In some cases, the rewiring costs of organizational changes are quite substantial, especially with large enterprise networks. A reorganization rate of 15 percent each year can result in yearly reconfiguration expenses as high as $750,000 for networks that have 6,000 interconnected devices. The advantage of wireless networking is again based on the lack of cable: You can move the network connection by just relocating an employee’s PC or IP phone.

Productivity Gain Is the Answer

For compelling reasons to install WLANs, you need to show continual productivity benefits. For example, consider using 802.11-equipped laptops. This enables users to read and respond to e-mail and browse the Internet during office meetings, assuming that the user can be responsive when needed at the meeting while plunking away at a laptop. Even though this seems trivial, the productivity gains can be significant.

Assume that a person attends three hours of meetings each day. If the user spends approximately 15 minutes per hour responding to e-mail and other Internet-related tasks during each meeting, the user will have 45 more minutes each day to work on other tasks. This seems pretty reasonable, considering the average person and office setting.

A 45-minute productivity gain equates to company cost savings that depend on the person's cost per hour. At $50 per hour, the savings will be $37.50 per person-day. A smaller company with 20 users will save $750 per day, $15,000 per month, $180,000 per year, and so on. After including WLAN installation costs, you may see a positive ROI in just a few months. Even if you factor in the cost of new laptops for everyone, you should still see a positive ROI in less than a year.

As a result, the use of WLANs can prove financially beneficial in common office environments, even if it only enables people to make better use of their time during meetings. Once a WLAN is in place, however, you will surely think of additional productivity-enhancing applications.

Determining Benefits of a VoWLAN System

The calculation of savings resulting from a VoWLAN solution includes the combination of quantitative and qualitative benefits. Let's take a look at each of these types of benefits and see how they can help justify VoWLAN costs.

Quantitative Benefits

The quantitative benefits comprise the actual dollar savings resulting from the deployment of a VoWLAN solution. This is generally cash that a company avoids paying for particular services, but it can also include sales of hardware that the

VoWLAN system is replacing. The following are the types of quantitative benefits that you can realize with a VoWLAN solution:

Reduced long-distance telephone charges: The routing of inter-company VoIP telephone calls is nearly free; therefore, a VoWLAN system can eliminate the long-distance charges (toll bypass) associated with each VoWLAN user.

Fewer wired telephone lines: A company can eliminate the need for a wired telephone line for each VoWLAN user, which saves any associated fees. Because VoWLAN users are wireless, there is no need to rewire telephone lines when changes are made to the workforce.

Increased productivity: This one is somewhat difficult to define in some cases, but it allows employees to complete work faster and better server customers. This results in higher revenues for the company, which is certainly a benefit.

Qualitative Benefits

Qualitative benefits enhance the operation of the company, but they do not result in definable dollar savings. These types of benefits often lean management toward funding the project when quantitative benefits are marginal or not well defined. The following are the types of qualitative benefits that you should consider when performing an ROI study for a VoWLAN solution:

Improved safety: This is certainly important to any company. In some cases, the regular use of VoWLAN phones can provide vital and immediate communications in emergency situations.

Better image to customers: With the use of VoWLAN phones, customers will see company employees getting things done faster and more efficiently, which makes the customer more inclined to do business with the company.

Increased employee morale: Employees equipped with VoWLAN handsets have less frustration because they don’t have to deal with telephone tag or search for phones when they need them.

Note

For details on implications of WLANs, such as radio frequency interference and security issues, refer to Chapter 4, "Wireless LAN Implications."

Wireless LAN Technologies

Wireless LAN technologies offer wireless connectivity in building, campus, and city-wide environments. Figure 1-2 illustrates the basic concept of a WLAN. The 802.11 standard has been evolving for more than a decade, resulting in today's 802.11n and 802.11ac and several legacy standards (see Figure 1-3).

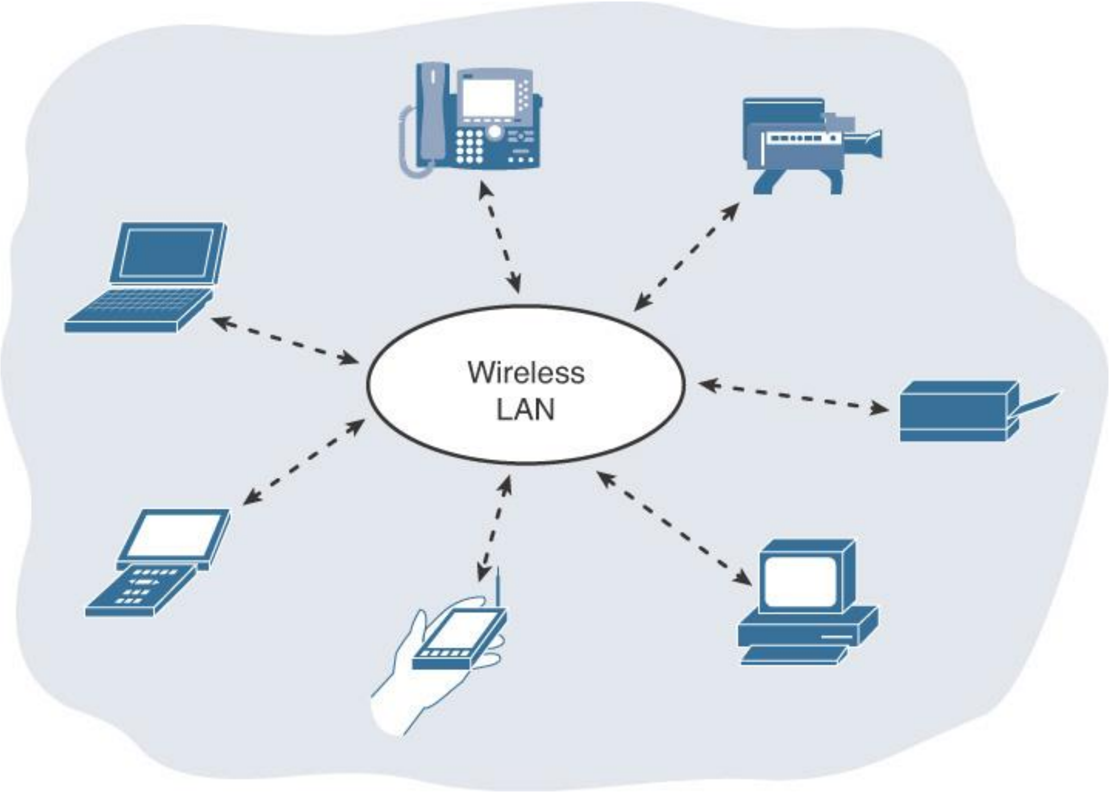


Figure 1-2 *Wireless LANs Support Wireless Communications Among a Variety of Client Devices*

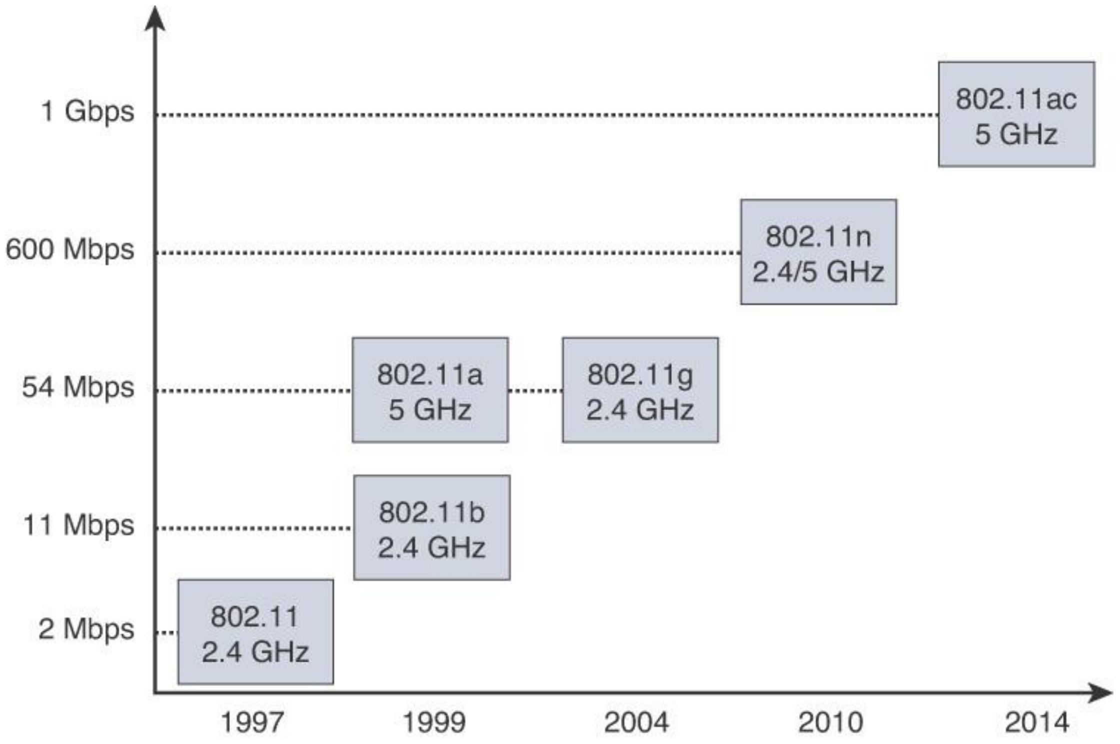


Figure 1-3 *IEEE 802.11 Standardization Has Led to Higher Performance*

In most cases, a standards organization defines the specific protocols and radio technology, and an industry group certifies the products based on the standard. For example, the IEEE 802.11 Working Group defines the 802.11 standard for WLANs, and the Wi-Fi Alliance provides interoperability testing for 802.11 products.

Note

802.11a, 802.11b, and 802.11g are considered legacy WLAN technologies because they have become obsolete.

Several different types of WLANs exist in companies and organizations. As a result, it is important that you understand the different WLAN types and their capabilities. In most cases, especially if there is an existing wireless network, it will be cost-effective to deploy an 802.11n or 802.11ac WLAN and make use of the existing legacy networks by configuring the access points to allow connections for older clients (e.g., 802.11g). Over time, as the needs arise and the funding is available, you should focus on migrating all users and applications to only 802.11n and 802.11ac.

The following sections provide a brief overview of the WLAN standards. The emphasis of this book is on IEEE 802.11–compliant WLANs because

802.11 is expected to continue being the preferred standard for supporting WLAN application. Other technologies, such as 802.16 (WiMAX), 802.15.3 (Bluetooth), and 802.15.4 (ZigBee), may better suit your needs in some situations, however. For example, WiMAX may be best for providing networking over large areas, such as cities. Bluetooth is the predominant technology for personal area networks, and ZigBee is ideal for very-low-power applications.

Initial 802.11

The initial IEEE 802.11 WLAN standard, ratified in 1997, specifies the use of both direct-sequence spread spectrum (DSSS) and frequency-hopping spread spectrum (FHSS) for delivering 1-Mbps and 2-Mbps data rates in the 2.4-GHz band. DSSS and FHSS are different forms of transmitting data over a WLAN.

The lower data rate provided by the initial 802.11 standard was more than enough bandwidth at the time to support bar code applications, which were the first commercial uses of WLAN technology. In general, however, the products based on this initial standard did not proliferate because of their high costs. In addition, some of the wireless data collector vendors were reluctant to move from proprietary wireless technologies to 802.11-based devices, primarily because they wanted to continue selling their own wireless base stations and only allow their data collectors to operate on them.

802.11a

In 1999, the 802.11 group ratified the 802.11a standard, which offers data rates up to 54 Mbps in the 5-GHz band, using orthogonal frequency-division multiplexing (OFDM). Even though the 802.11a standard was available in 1999, 802.11a access points and radio cards did not become commercially available until several years later. The primary reasons for the delay to market were the difficulties in developing 5-GHz, 802.11 hardware and the weak market potential for WLAN components that did not interoperate with the existing 2.4-GHz WLANs. 802.11a products had been available for several years, but their use was somewhat limited to specialized applications, especially where high performance was necessary (and interoperability with 2.4-GHz systems was not necessary).

A significant advantage of 802.11a is that it offers very high capacity compared to other legacy WLANs. The reason is that the 802.11a, 5-GHz spectrum defines a greater number of RF channels that do not overlap in frequency. Another advantage of 802.11a is that it operates in the 5-GHz band, which is mostly free from sources of RF interference. Microwave ovens, Bluetooth devices, most cordless phones, and the majority of neighboring WLANs operate in the 2.4-GHz band of frequencies. The lower noise floor in the 5-GHz band affords lower retransmission rates and higher resulting throughput compared to 802.11b and 802.11g systems.

802.11b

To provide higher data rates when operating in the 2.4-GHz band, the 802.11 group also ratified the 802.11b physical layer in 1999, enhancing the initial DSSS physical layer to include additional 5.5-Mbps and 11-Mbps data rates. The 802.11b access points were backward compatible with original 802.11 DSSS client devices. Soon after ratification of the 802.11b standard, 802.11b access points and radio cards began shipping with those improvements. It was a fairly easy modification to existing 802.11 DSSS devices to become 802.11b compliant. In fact, most users could upgrade their existing access points and radio cards with simple firmware upgrades. For several years, 802.11b devices proliferated throughout the industry and became the most commonly installed WLAN hardware.

Unfortunately, a great deal of RF interference resides in the 2.4-GHz band, which impacts 802.11b, 802.11g, and 2.4-GHz 802.11n users. A microwave oven can cause significant degradation in throughput because radio waves from a microwave oven can block 802.11b (and 802.11g) radio cards from accessing the medium or create bit errors in the 802.11 frames in transit. The potential for RF interference in the 2.4-GHz band is one reason a company would strongly consider using 5-GHz solutions.

A limiting factor of 802.11b is that it supports only up to three non-overlapping radio cells in the same area. The 2.4-GHz frequency spectrum is roughly 90-MHz wide, and an 802.11b radio card or access point uses approximately 30 MHz when transmitting. To avoid inter-access point interference (also referred to as co-channel interference), 802.11b access points must be set to specific channels. For example, access points in the United States can be set to channels 1, 6, and 11 to avoid overlap and mutual interference. This is especially important if there are many active wireless users. As a result of this frequency plan and limited data rates, 802.11b has limited capacity (and data rates).

802.11g

802.11g, ratified in 2004, further enhances 802.11b to include data rates up to 54-Mbps in the 2.4-GHz band, using OFDM. 802.11g is backward compatible with 802.11b, which is referred to as 802.11b/g mixed-mode operation. For example, an 802.11b radio card can associate with an 802.11g access point. Because of its support for data rates up to 54-Mbps, 802.11g offers higher performance than 802.11b systems. Capacity is still somewhat limited, however, because 802.11g operates in the 2.4-GHz band, which still limits the number of non-overlapping channels to 1, 6, and 11, as with 802.11b. As a result, 802.11g systems have less capacity than 802.11a WLANs. 802.11g, for example, can have up to three non-overlapping channels with 54 Mbps per channel.

A single 802.11b station associating with an 802.11g access point invokes the use of protection mechanisms, such as request-to-send/clear-to-send (RTS/CTS). The reason this is necessary is that 802.11b and 802.11g use different modulation, which means that they cannot interoperate and coordinate transmissions according to the 802.11 protocol. The access point informs all stations that an 802.11b station is present by setting an applicable bit in the body of each beacon frame. As a result, all stations begin using protection mechanisms.

The RTS/CTS protection mechanism requires each station to implement the entire RTS/CTS process for each data frame needing transmission. The problem with this requirement is that throughput suffers because of the RTS and CTS frames. As a result, some 802.11 stations are designed to implement a CTS-to-self mechanism as a protection. In this case, a station needing to send data first transmits a CTS frame to itself, using a modulation type understandable by all stations and indicating to other stations how long the sending station will need to access the medium in order to send a data frame. This may decrease the number of frame transmissions, but it still introduces a considerable amount of overhead. Thus, a mixed environment of 802.11b and 802.11g users significantly degrades the throughput of the WLAN, often by as much as 30 percent, which reduces the number of simultaneous voice calls that the network can support.

This is why most vendors allow administrators to configure access points to allow only 802.11g station associations, referred to as 802.11g-only mode. Of course the problem with this is that all users must have 802.11g radio cards. 802.11b-equipped devices will not be able to associate with the access point. But at least the throughput will remain relatively high.

Some vendors also allow you to disable protection mechanisms in mixed mode, which supports both 802.11b and 802.11g connections. This is a good approach if there are a limited number of active users because the probability of 802.11b and 802.11g devices transmitting at the same time is minimal.

Many 802.11g implementations use 802.11b-only mode to avoid interoperability issues and maximize range. Sometimes 802.11b client radios have trouble connecting to 802.11g access points, and administrators often fix the problem by switching the 802.11g access points to b-only mode. 802.11b also has slightly better range because of lower minimum data rates. 802.11b can operate with data rates as low as 1 Mbps, whereas 802.11g can operate only as low as 6 Mbps. The lower minimum data rate operation of 802.11b allows longer-range operation compared to 802.11g.

In addition, most 802.11g access points set to b-only mode will send beacons as 1 Mbps instead of 2 Mbps (which is what 802.11g generally uses). This extends the reach of 802.11b access points beyond 802.11g access points. In addition, the use of b-only mode eliminates the need for the access point to use protection mechanisms since users are all 802.11b and not a mix of 802.11b and 802.11g.

Current Standards: 802.11n and 802.11ac

The 802.11n standard, ratified in 2009, specifies data rates well above 100 Mbps and at much better throughput than legacy systems. In 2008, the Wi-Fi Alliance started certifying WLAN products based on Draft 2.0 of the 802.11n standard, which offers a solid technology that requires only software upgrades to be compatible with the ratified version of the 802.11 standard. Draft 2.0 802.11n differs from earlier pre-802.11n, which was based on several earlier and differing 802.11n drafts. A problem is that most of the pre-802.11n products do not interoperate between vendors. As a result, it is likely not possible to upgrade pre-802.11n products to the Draft 2.0 or ratified versions of the standard.

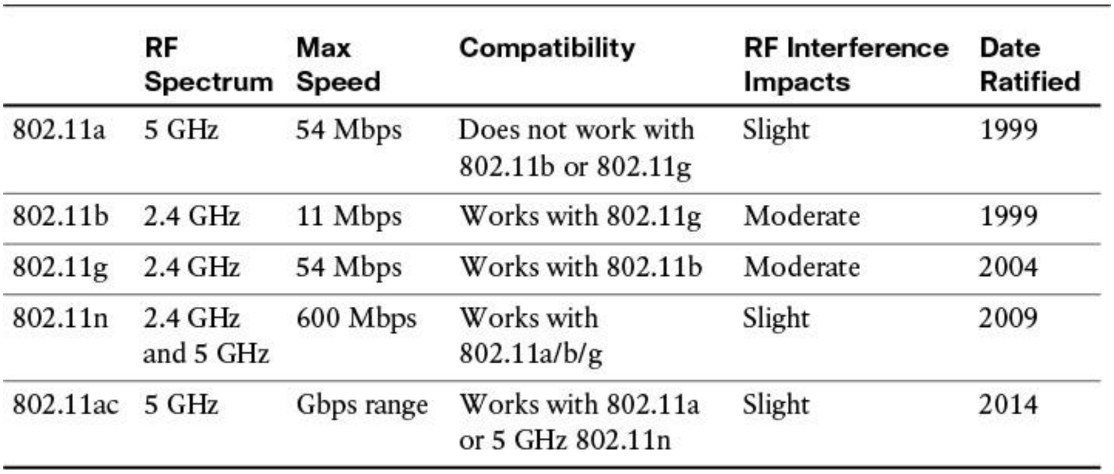
802.11n supports operation in both the 2.4-GHz and 5-GHz bands, which provides flexibility for satisfying a multitude of wireless requirements. In addition, 802.11n is backward compatible with 802.11g and 802.11a legacy WLANs, and protection mechanisms are necessary to coordinate access to the network, similar to 802.11b/g mixed-mode operation. Of course, protection mechanisms impose a great detail of overhead, which hampers throughput. The backward compatibility makes it possible to continue use of existing legacy WLAN devices; however, to achieve the full performance potential of 802.11n, you should implement 802.11n-only client devices.

802.11n does a better job than legacy systems (802.11a, 802.11b, and 802.11g) at providing higher performance, availability, and predictability of the network because of multiple-input multiple-output (MIMO) operation, channel bonding, and more efficient protocols, such as packet aggregation. With 802.11n, usage of the wireless network is comparable to wired Ethernet connections. In addition, support costs are relatively low because there isn’t as much need to continually fine-tune the network as there is in legacy networks. The MIMO technology of 802.11n overcomes interference issues, which improves reliability and reduces the time needed to troubleshoot related problems.

802.11ac was ratified in 2014 and is an enhancement to the 802.11n standard in the 5-GHz band. 802.11ac increases data rates in the Gbps range to play effectively with Gigabit Ethernet. 802.11ac provides higher data rates through wider RF channels, more spatial streams, and higher-order modulation. Typical dual-band access points today implement 802.11n in the 2.4-GHz band and 802.11ac in the 5-GHz band. This combination of technologies offers substantial performance for meeting the needs of a wide variety of wireless applications and utilization levels today and in the foreseeable future.

Comparison of 802.11 Standards

Table 1-1 provides a comparison of the different characteristics of the 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac standards.



	RF Spectrum	Max Speed	Compatibility	RF Interference Impacts	Date Ratified
802.11a	5 GHz	54 Mbps	Does not work with 802.11b or 802.11g	Slight	1999
802.11b	2.4 GHz	11 Mbps	Works with 802.11g	Moderate	1999
802.11g	2.4 GHz	54 Mbps	Works with 802.11b	Moderate	2004
802.11n	2.4 GHz and 5 GHz	600 Mbps	Works with 802.11a/b/g	Slight	2009
802.11ac	5 GHz	Gbps range	Works with 802.11a or 5 GHz 802.11n	Slight	2014

Table 1-1 *802.11 Standards Comparison*

Wi-Fi Certification

The Wi-Fi Alliance (which was originally known as the Wireless Ethernet Compatibility Alliance [WECA]) is an international nonprofit organization focusing on the manufacturing, marketing, and interoperability of 802.11 WLAN products. The Wi-Fi Alliance pushes the term (actually brand) “Wi-Fi” to cover all forms of 802.11-based wireless networking (whether 802.11a, b, g, n, or ac); it is also the group behind Wi-Fi Protected Access (WPA), the stepping-stone between the much-criticized WEP and the 802.11i security standard.

Note

For a current list of certified Wi-Fi equipment, refer to the Wi-Fi Alliance website, at www.wi-fi.org.

The Wi-Fi Alliance has the following goals:

- Promote Wi-Fi certification worldwide by encouraging manufacturers to follow standardized 802.11 processes in the development of WLAN products

- Market Wi-Fi-certified products to consumers in the home, small office, and enterprise markets

Wi-Fi certification is a process that assures interoperability between 802.11 WLAN equipment, including access points and radio cards complying with a variety of form factors. After completing a testing program, WLAN vendors receive Wi-Fi certification for their products. All Wi-Fi-certified products include a label, as shown in Figure 1-4.

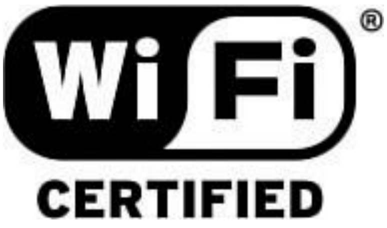


Figure 1-4 *A Product Bearing This Label Verifies Compliance with Wi-Fi Standards*

The Wi-Fi Alliance follows an established testing program to certify that products are interoperable with other Wi-Fi-certified products. Certification consists of independent testing labs located in North America, Europe, and Asia. After a product successfully passes every test, the manufacturer is granted the right to use the Wi-Fi Certified logo on that particular product and its corresponding support material, such as packaging and manuals.

For a manufacturer, the main reason to obtain Wi-Fi certification is that it helps sell products. Wi-Fi certification is meant to give consumers confidence that they are purchasing WLAN products that have met multivendor interoperability requirements. A Wi-Fi Certified logo on the product means that it has met interoperability testing requirements and will definitely work with other vendors' Wi-Fi-certified products. If a product says Wi-Fi Certified, consumers should feel confident that it will work.

There is certainly merit in having products guaranteed to interoperate with those from other vendors. IT managers generally deploy access points from a single vendor, but they often do not have control over the use of different vendors for radio cards found in user devices. This can pose compatibility issues unless all devices undergo interoperability testing, such as the Wi-Fi certification process. Thus, Wi-Fi certification enables WLAN sales because IT managers are more likely to buy certified devices than ones that do not have Wi-Fi certification.

The 802.11 standard enables significant interoperability; however, there are no conformance mandates to ensure that a particular vendor follows all the rules precisely. IT managers realize this and therefore see the value in the conformance that Wi-Fi demands. In fact, the general public is starting to recognize Wi-Fi as a brand and buzzword that is more significant than 802.11 alone.

With this said, a company wanting to sell mainstream WLAN products needs Wi-Fi certification to be competitive. The importance of Wi-Fi certification will only grow as more and more mixed-vendor WLANs proliferate in public markets.

Note

Refer to Chapters 5, “Introduction to IEEE 802.11 and Related Standards,” 6, “IEEE 802.11 Medium Access Control (MAC) Layer,” and 7 “IEEE 802.11 Physical (PHY) Layers,” for more details on the IEEE 802.11 standard.

Case Study 1-2: Acme Healthcare Chooses 802.11n and 802.11ac

Acme Healthcare, the fictitious hospital introduced earlier in this chapter, decided that 802.11n and 802.11ac will best meet the hospital’s wireless networking needs. Arthur, the hospital CIO, consulted with several of his IT staff, and the consensus was that the higher throughput and reliability of 802.11n and 802.11ac as compared to the legacy 802.11 systems is absolutely necessary to support demanding applications that the hospital plans to deploy. It will be imperative that the wireless network be able to effectively support a relatively large number of time-sensitive applications, such as voice communications and patient monitoring, as well as currently unknown applications that the hospital may implement in the future. In addition, the surge of hospital workers having multiple wireless computing devices, such as smart phones and laptops, has increased potential utilization to levels that the legacy technologies will not support.

Note that this case study surfaces throughout this book to emphasize the primary considerations in deploying an 802.11n and 802.11ac wireless network.

Wireless LANs: A Historical Perspective

You may be interested in knowing how WLAN technologies got started and how they have developed over the years. The evolution of WLANs has been taking place for decades, leading to continual gains in performance, security, and reliability. This section starts with the historical roots and then explores what has led to the 802.11n and 802.11ac standards.

The Early Days

Network technologies and radio communications were brought together for the first time in 1971 at the University of Hawaii as a research project called ALOHANET. The ALOHANET system enabled computer sites at seven campuses spread out over four islands to communicate with the central computer on Oahu without using the existing unreliable and expensive phone lines. ALOHANET offered bidirectional communications in a star topology between the central computer and each of the remote stations. The remote stations had to communicate with each other via the centralized computer.

In the 1980s, amateur radio hobbyists, hams, kept radio networking alive in the United States and Canada by designing and building terminal node controllers (TNCs) to interface their computers through ham radio equipment. A TNC acts much like a telephone modem, converting the computer's digital signal into a signal that a ham radio can modulate and send over the airwaves by using a packet-switching technique. In fact, the American Radio Relay League (ARRL) and the Canadian Radio Relay League (CRRL) have been sponsoring the Computer Networking Conference since the early 1980s to provide a forum for the development of wireless WANs. Thus, hams have been using wireless networking for years, much earlier than the commercial market.

In 1985, the FCC made possible the commercial development of radio-based LAN components by authorizing the public use of the Industrial, Scientific, and Medical (ISM) bands. These frequencies reside between 902 MHz and 5.85 GHz, just above the cellular phone operating frequencies. The ISM band is attractive to wireless network vendors because it provides a part of the spectrum on which to base their products, and end users do not have to obtain FCC licenses to operate the products. The ISM band allocation has had a dramatic effect on the wireless industry, prompting the development of WLAN components. Without a standard, however, vendors began developing proprietary radios and access points.

Initial 802.11 Standardization

In the late 1980s, the Institute of Electrical and Electronics Engineers (IEEE) 802 Working Group, responsible for the development of LAN standards such as Ethernet and Token Ring, began development of standards for WLANs. Under the chairmanship of Vic Hayes from NCR, the IEEE 802.11 Working Group developed the Wireless LAN Medium Access Control and Physical Layer specifications. Before the ratification of the standard, companies began shipping proprietary WLAN radio cards and access points operating in the 902-MHz ISM band. In the early 1990s, the first WLAN products, NCR WaveLAN and Motorola Altair, appeared on the market. At that time, there were no applicable standards, and prices were relatively high, at around $1,500 per wireless adapter. As a result, only companies having applications with significant benefits from wireless connectivity, such as inventory management and price marking, could afford to deploy WLAN solutions.

The IEEE Standards Board approved the standard on June 26, 1997, and the IEEE published the standard on November 18, 1997. The finalization of this standard prompted vendors to release 1-Mbps and 2-Mbps 802.11-compliant radio cards and access points throughout 1998. Proliferation of WLANs at that point was slow, mainly because performance of the initial 802.11 devices was slow (and pricing was still high) compared to wired Ethernet networks. In addition, there was significant criticism of the security of 802.11 networks because of issues with the Wired Equivalent Privacy (WEP) encryption protocol.

In December 1999, the IEEE released supplements to the 802.11 standard to increase performance of WLANs. 802.11a provided up to 54 Mbps in the 5-GHz band, and 802.11b offered up to 11 Mbps in the 2.4-GHz band. Vendors began shipping 802.11b devices throughout 2000 at prices of less than $200 per radio card. This caused 802.11b sales to skyrocket. The 54-Mbps 802.11a WLANs did not become available for a couple years after 802.11b products. As a result, the proliferation of 802.11a was very low because of the significant installed base of 802.11b (and lack of interoperability between 802.11b and 802.11a).

Later, in 2004, IEEE released 802.11g, which further extended data rates in the 2.4-GHz band to 54-Mbps, using OFDM. The higher-data-rate 802.11 standards 802.11a, 802.11b, and 802.11g offer adequate capacity for supporting most applications. 802.11a, however, provided the highest capacity, mainly because the RF channels in the 5-GHz band do not overlap with each other, as they do in the 2.4-GHz band.

Another improvement to the 802.11 standard was security; 802.11i includes much stronger encryption and authentication mechanisms than the initial standard. The use of TKIP/RC4 and CCMP/AES, along with 802.11i protocols, makes WLANs very secure. The ratification of the 802.11e standard, which offers quality of service important for VoWLAN applications, was an important step toward making 802.11 WLANs more reliable.

In the past few years, the prices for WLAN adapters have decreased to well under $100 each. This dramatic drop in prices has fueled the proliferation of WLANs for a variety of applications in all markets. The Wi-Fi Alliance has also been actively promoting WLANs through the Wi-Fi brand and mandating interoperability testing.

802.11n and 802.11ac Standardization

A major improvement to WLAN technology was the development of the 802.11n standard. The first official 802.11n development began with a presentation in January 2002 to the Wireless Next Generation Standing Committee (WNG SC) of the IEEE 802.11 Working Group. In September 2002, the High Throughput Study Group (HTSG) had its first meeting and completed the Project Authorization Request (PAR) to begin the High Throughput Task Group (TGn), which would then continue with the development of the standard. The PAR emphasized the development of an amendment to the 802.11 standard to modify the Physical (PHY) Layer and Medium Access Control (MAC) Layer specifications to satisfy high performance needs of residential, enterprise, andhotspot environments. At its first meeting in September 2003, TGn created functional requirements.

The following is a list of the key requirements that the 802.11n PAR identifies:

- At least 100-Mbps throughput in a single 20-MHz channel
- Spectral density of at least 3 bps/Hz
- Support for operation in the 5-GHz band
- Backward compatibility with 802.11a
- Integration of 802.11e within workstations

It is interesting to note that there was no initial requirement for 2.4-GHz operation, but if it were to become part of the standard (which it eventually did), it would have to be backward compatible with 802.11g.

TGn issued a call for proposals on March 17, 2004. There were several proposals, but eventually the TGn Sync and WWiSE proposals emerged. TGn Sync, founded by Intel, Cisco, Agere, and Sony, emphasized providing wireless connectivity for PCs, enterprises, and consumer electronics. WWiSE, founded by Broadcom, Conexant, and Texas Instruments, focused on a simple upgrade to 802.11a. Both proposal groups defined 40-MHz channels and MAC enhancements such as frame aggregation.

Unsuccessful attempts were made from 2005 to 2006 to confirm one particular proposal. This resulted in merging the TGn Sync and WWiSE proposals. Meanwhile, some of the first “802.11n” products were made available to the public starting in 2007, but they are more appropriately referred to as pre-N products because they are based on differing versions of draft 802.11 standards. The pre-N products do not provide guaranteed interoperability. These single-vendor systems were primarily sold to the home and small business market, where it is not as important to have interoperability.

The merged 802.11n proposal passed confirmation vote (unanimously) within TGn in January 2006, and the merged proposal was converted to a draft 802.11 standard amendment (Draft 1.0). In March 2006, Draft 1.0 of the standard (referred to as a Letter Ballot) was distributed to the entire 802.11 Working Group, but it did not receive the required 75 percent necessary for adoption. The reviewers of the draft proposal generated 6,000 comments.

Resolution of the comments began in May 2006, and TGn submitted the updated draft standard (Draft 2.0) for the Letter Ballot in February 2007. This time, the 802.11 Working Group adopted Draft 2.0 with a favorable vote of 83 percent. This process, however, generated 3,000 comments that the TGn would have to resolve. Because the 802.11 Working Group adopted Draft 2.0, the Wi-Fi Alliance started certifying 802.11n products based on Draft 2.0 of the 802.11n standard. This was done so that the vendors could start selling 802.11n products while the 802.11 Working Group was finalizing the standard. Draft 3.0 of the 802.11n standard was ready in September 2007. Instead of being a Letter Ballot, Draft 3.0 was sent to the IEEE 802.11 Working Group as a Recirculation Ballot, which required that comments only address changes that had taken place since the previous draft.

On September 11, 2009, the 802.11n amendment to the 802.11 standard was ratified.

Because of falling prices and substantial performance of 802.11n, WLANs took on a much larger role in horizontal enterprise applications. In addition, many organizations, such as hospitals and airports, began replacing existing legacy (mostly 802.11g) wireless networks with 802.11n infrastructures. During 2012, the IEEE 802.11ac Task Group produced Drafts 2.0 and 3.0 of the 802.11ac standard, with final ratification in January 2014. Soon after the drafts of the standard were released, vendors started selling 802.11ac products based on the draft standard.

Summary

Wireless LANs provide significant benefits to enterprises, hospitals, warehouses, and any other establishment where mobility is important. A host of organizations, such as hospitals, enterprises, and warehouses, have many tangible benefits based on the use of wireless IP phones and other bandwidth-intensive mobile applications. 802.11n- and 802.11ac-based WLAN solutions have the performance and reliability necessary for supporting these types of applications, especially when it’s not clear what applications may need to be supported down the road.

Chapter 2. Radio Wave Fundamentals

This chapter will introduce you to:

- Radio Wave Attributes
- RF System Components
- RF Signal Propagation
- RF Mathematics

As the basis for understanding the installation, operation, and troubleshooting of wireless LANs (WLANs), it is important that you have a good knowledge of how radio waves propagate through an environment. Every Wi-Fi deployment requires that the systems engineer understand the fundamentals of how radio waves move and react within the environment. For example, in a WLAN, radio waves carry information over the air from one point to another. Along the way, the waves encounter various obstacles or obstructions that can impact range and performance, depending on the characteristics of the radio wave. In addition, regulatory rules govern the use and limitations of radio waves. This chapter explains the fundamentals of radio waves so that you have a good basis for understanding the complexities of deploying WLANs.

Radio Wave Attributes

A radio wave is a type of electromagnetic signal designed to carry information through the air over relatively long distances. Sometimes radio waves are referred to as radio frequency (RF) signals. These signals oscillate at a very high frequency, which allows the waves to travel through the air similar to waves on an ocean.

Radio waves have been in use for many years. They provide the means for carrying music to FM radios and video to televisions. In addition, radio waves are the primary means for carrying data over a wireless network. As shown in Figure 2-1, a radio wave has amplitude, frequency, and phase elements. These attributes may be varied in time to represent information.

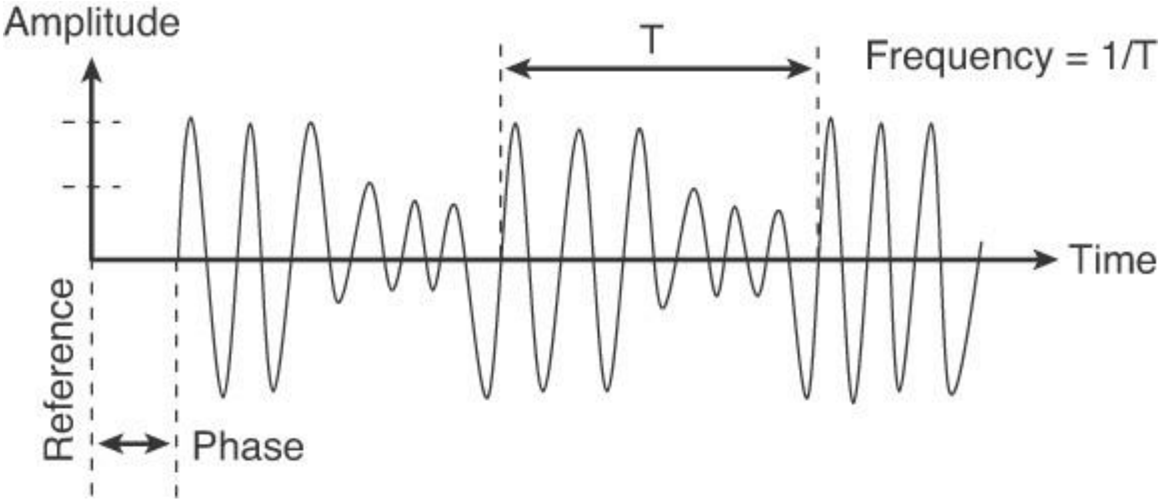


Figure 2-1 *The Amplitude, Frequency, and Phase Elements of a Radio Wave*

Amplitude

The amplitude of a radio wave indicates its strength. The measure for amplitude is generally power, which is analogous to the amount of effort a person needs to exert to ride a bicycle over a specific distance. Similarly, power in terms of electromagnetic signals represents the amount of energy necessary to push the signal over a particular distance. As the power increases, so does the range.

Radio waves have amplitudes with units of watts, which represent the amount of power in the signal. Watts have linear characteristics that follow mathematical relationships we are all very familiar with. For example, the result of doubling 10 milliwatts (mW) is 20 mW. We certainly do not need to do any serious number crunching to get that result.

As an alternative, it is possible to use dBm units (decibels referenced to 1 mW) to represent the amplitude of radio waves. The dBm is the amount of power in watts referenced to 1 mW. Zero (0) dBm equals 1 mW. By the way, the little m in dBm is a good reminder of the 1 mW reference. The dBm values are positive above 1 mW and negative below 1 mW. Beyond that, math with dBm values gets a bit harder. Refer to the section "RF Mathematics," later in this chapter, to learn how to convert between watts and dBm units and understand why it is preferable to use dBm units.

Note

You can adjust the transmit power of most client cards and access points. For example, some access points allow you to set the transmit power in increments from –1 dBm (0.78 mW) up to 23 dBm (200 mW).

Frequency

The frequency of a radio wave is the number of times per second that the signal repeats itself. The unit for frequency is Hertz (Hz), which is actually the number of cycles occurring each second. In fact, an old convention for the unit for frequency is cycles per second (cps).

802.11 WLANs use radio waves having frequencies of 2.4 GHz and 5 GHz, which means that the signal includes 2,400,000,000 cycles per second and 5,000,000,000 cycles per second, respectively. Signals operating at these frequencies are too high for humans to hear and too low for humans to see. Thus, radio waves are not noticed by humans.

The frequency impacts the propagation of radio waves. Theoretically, higher-frequency signals propagate over a shorter range than lower-frequency signals. In practice, however, the range of different frequency signals might be the same, or higher-frequency signals might propagate farther than lower-frequency signals. For example, a 5-GHz signal transmitted at a higher transmit power might go farther than a 2.4-GHz signal transmitted at a lower power, especially if electrical noise in the area impacts the 5-GHz part of the radio spectrum less than the 2.4-GHz portion of the spectrum (which is generally the case).

Phase

The phase of a radio wave corresponds to how far the signal is offset from a reference point (such as a particular time or another signal). By convention, each cycle of the signal spans 360 degrees. For example, a signal might have a phase shift of 90 degrees, which means that the offset amount is one-quarter (90/360 = 1/4) of the signal.

RF System Components

Figure 2-2 illustrates a basic RF system that enables the propagation of radio waves. The transceiver and antenna can be integrated inside the client device or can be an external component. The transmission medium is primarily air, but there might be obstacles, such as walls and furniture.

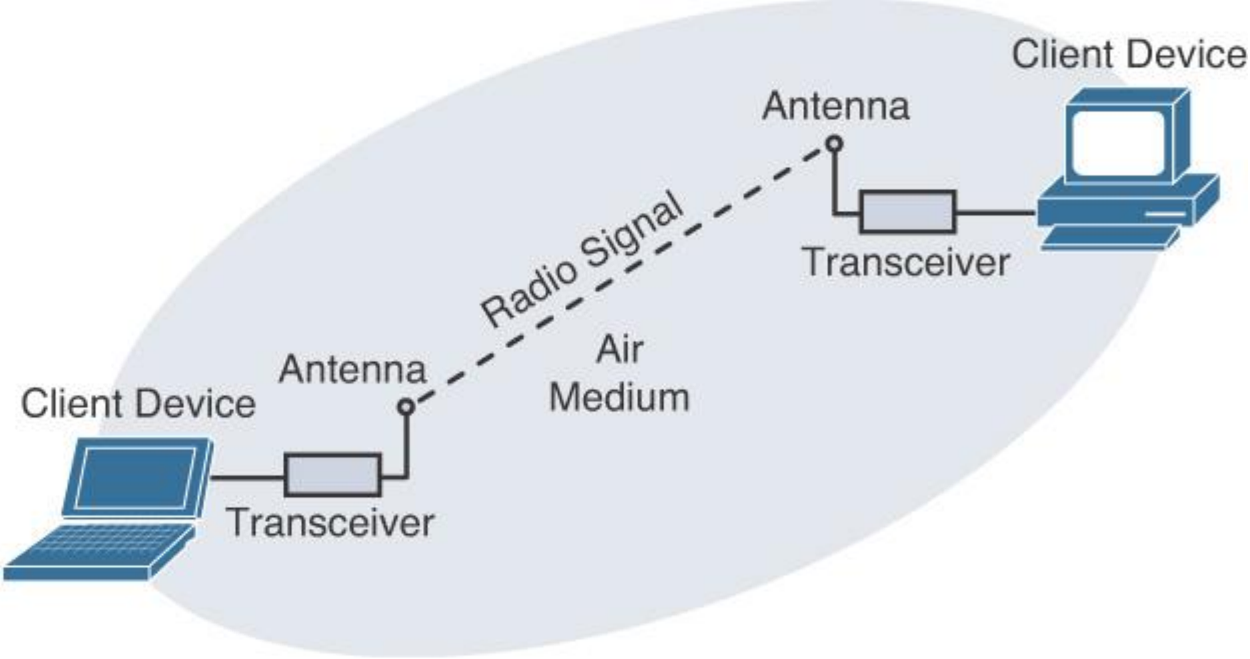


Figure 2-2 *An RF System Consists of RF Transceivers, Antennas, and a Transmission Medium*

RF Transceiver

A key component of a WLAN is the RF transceiver, which consists of a transmitter and a receiver. The transmitter transmits the radio wave on one end of the system (the "source"), and the receiver receives the radio wave on the other side (the "destination") of the system. The transceiver is generally composed of hardware that is part of the wireless client radio device (sometimes referred to as a client card).

Figure 2-3 shows the basic components of a transmitter. A process known as *modulation* converts electrical digital signals that represent information (data bits, 1s and 0s) inside a computer into radio waves at the desired frequency, which propagate through the air medium. Refer to the section "RF Modulation" for details on how modulation works. The amplifier increases the amplitude of the radio wave signal to a desired transmit power prior to being fed to the antenna and propagating through the transmission medium (consisting primarily of air in addition to obstacles, such as walls, ceilings, chairs, and so on).

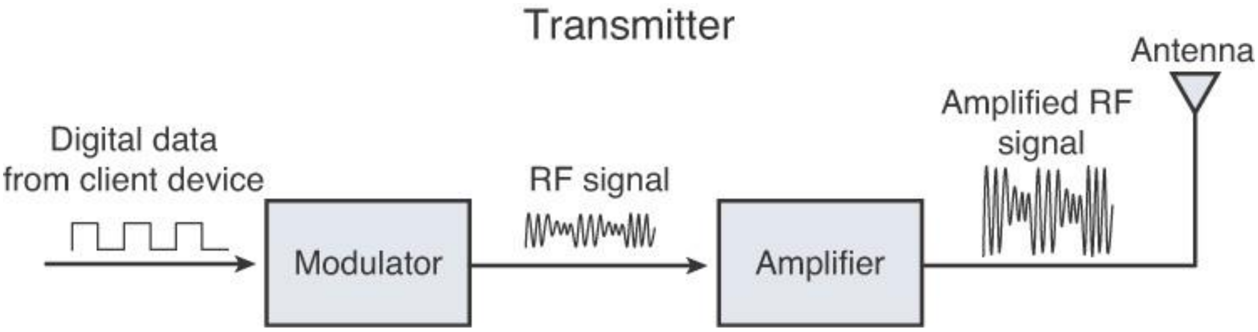


Figure 2-3 *A Transmitter Consists of a Modulator, an Amplifier, and an Antenna*

At the destination, a receiver (see Figure 2-4) detects the relatively weak RF signal and demodulates it into data types applicable to the destination computer. The radio wave at the receiver must have amplitude that is above the receiver sensitivity of the receiver; otherwise, the receiver will not be able to "interpret" the signal, or decode it. The minimum receiver sensitivity depends on the data rate. For example, say that the receiver sensitivity of an access point is –69 dBm for 300 Mbps (802.11n) and –90 dBm for 1 Mbps (802.11b). The amplitude of the radio wave at the receiver of this access point must be above –69 dBm for 300 Mbps or above –90 dBm for 1 Mbps before the receiver will be able to decode the signal.

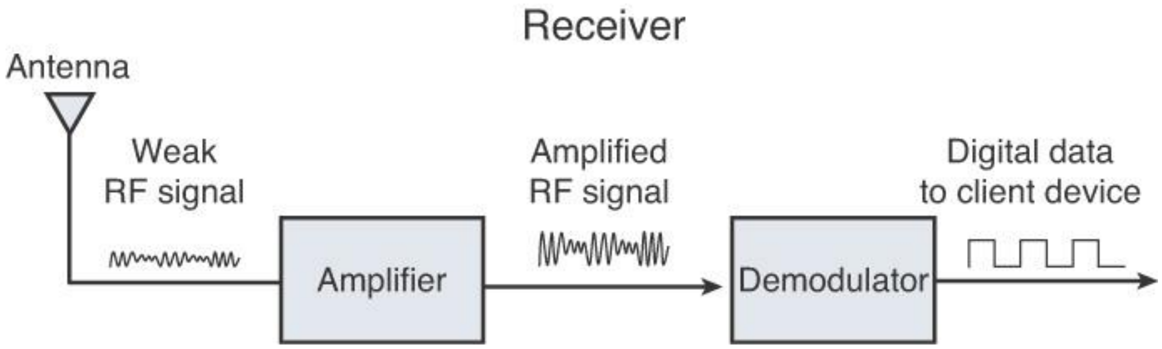


Figure 2-4 *A Receiver Consists of an Antenna, an Amplifier, and a Demodulator*

RF Modulation

RF modulation transforms digital data, such as binary 1s and 0s representing an e-mail message, from the network into an RF signal suitable for transmission through the air. This involves converting the digital signal representing the data into an analog signal. As part of this process, modulation superimposes the digital data signal onto a carrier signal, which is a radio wave having a specific frequency. In effect, the data rides on top of the carrier. To represent the data, the modulation signal varies the carrier signal in a manner that represents the data.

Modulation is necessary because it is not practical to transmit data in its native form. For example, say that Kimberlyn wants to transmit her voice wirelessly from Dayton to Cincinnati, which is about 65 miles. One approach is for Kimberlyn to use a really high-powered audio amplifier system to boost her voice enough to be heard over a 65-mile range. The problem with this, of course, is that the intense volume would probably deafen everyone in Dayton and all the communities between Dayton and Cincinnati. Instead, a better approach is to modulate Kimberlyn's voice with a radio wave or light carrier signal that's out of range of human hearing and suitable for propagation through the air. The data signal can vary the amplitude, frequency, or phase of the carrier signal, and amplification of the carrier will not bother humans because it is well beyond the hearing range.

The latter is precisely what modulation does. A modulator mixes the source data signal with a carrier signal. In addition, the transmitter couples the resulting modulated and amplified signals to an antenna, which is designed to interface the signal to the air. The modulated signal then departs the antenna and propagates through the air. The receiving station antenna couples the modulated signal into a demodulator, which derives the data signal from the signal carrier.

Amplitude-Shift Keying

One of the simplest forms of modulation is amplitude modulation (sometimes referred to as amplitude-shift keying), which varies the amplitude of a signal to represent data. Figure 2-5 illustrates this concept. Frequency-shift keying (FSK) is common for light-based systems whereby the presence of a 1 data bit turns the light on and the presence of a 0 bit turns the light off. Actual light signal codes are more complex, but the main idea is to turn the light on and off to send the data. This is similar to giving flashlights to two people in a dark room and having them communicate with each other by flicking the flashlights on and off to send coded information.

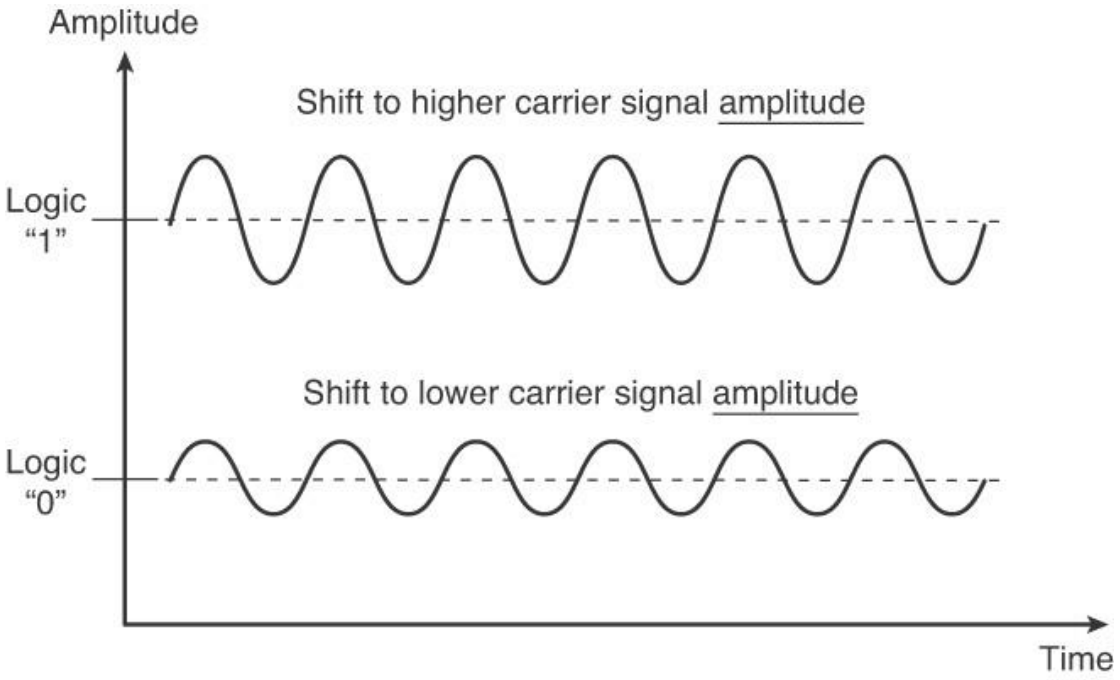

Amplitude
Shift to higher carrier signal amplitude
Logic "1"
Shift to lower carrier signal amplitude
Logic "0"
Time

Figure 2-5 *Amplitude-Shift Keying Varies the Amplitude of the Signal to Represent Digital Data*

Amplitude modulation alone does not work very well with RF systems because there are signals (noise) present inside buildings and outdoors that alter the amplitude of the radio wave, which causes the receiver to demodulate the signal incorrectly. These noise signals can cause the signal amplitude to be artificially high for a period of time; for example, the receiver would demodulate the signal into something that does not represent what was intended (for example, 10000001101101 would become 10111101101101). To combat impacts from noise, modulation for RF systems is more complex than using only amplitude modulation.

Frequency-Shift Keying

FSK makes slight changes to the frequency of the carrier signal to represent data in a manner that's suitable for propagation through the air at low to moderate data rates. For example, as shown inFigure 2-6, modulation can represent a 1 or 0 data bit with either a positive or negative shift in frequency of the carrier. If the shift in frequency is negative—that is, a shift of the carrier to a lower frequency—the result is a logic 0. The receiver can detect this shift in frequency and demodulate the results as a 0 data bit. As a result, FSK avoids the impacts of common noise that exhibits shifts in amplitude.

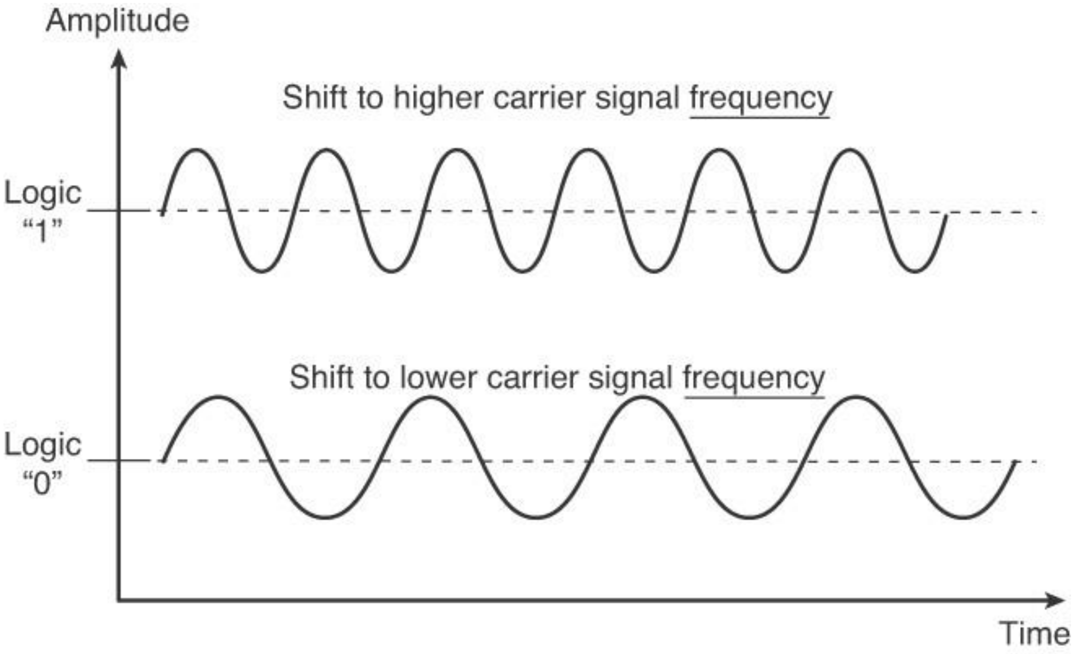

Amplitude
Shift to higher carrier signal frequency
Logic "1"
Shift to lower carrier signal frequency
Logic "0"
Time

Figure 2-6 *Frequency-Shift Keying Makes Use of Changes in Frequency to Represent Digital Data*

Phase-Shift Keying

Some systems use phase-shift keying (PSK), which is similar to FSK, for modulation purposes for low to moderate data rates. With PSK, data causes changes in the signal's phase, while the frequency remains constant. The phase shift, as Figure 2-7 depicts, can correspond to a specific positive or negative amount relative to a reference. A receiver can detect these phase shifts and realize the corresponding data bits. As with FSK, PSK is mostly immune to common noise that is based on shifts in amplitude.

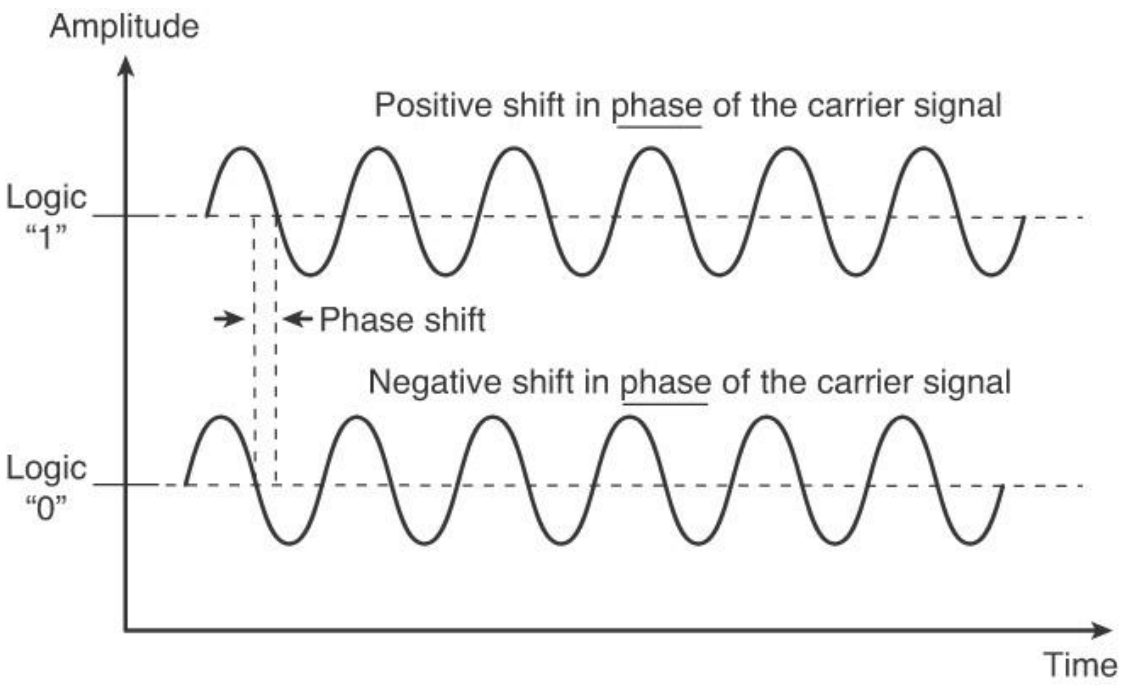

Amplitude
Positive shift in phase of the carrier signal
Logic "1"
Phase shift
Negative shift in phase of the carrier signal
Logic "0"
Time

Figure 2-7 *Phase-Shift Keying Makes Use of Changes in Phase to Represent Digital Data*

Quadrature Amplitude Modulation

Quadrature amplitude modulation (QAM) causes both the amplitude and phase of the carrier to change to represent patterns of data, often referred to as symbols. The advantage of QAM is the capability of representing large groups of bits as a single amplitude and phase combination. In fact, some QAM-based systems, for example, make use of 64 different phase and amplitude combinations, resulting in the representation of 6 data bits per symbol. Higher-order combinations of phase and amplitude in QAM make it possible for standards such as 802.11n and 802.11ac to support higher data rates.

Note

See Chapter 7, "IEEE 802.11 Physical (PHY) Layers," for details on the modulation and transmission frequencies that 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac use.

Spread Spectrum

After modulating the digital signal into an analog carrier signal using FSK, PSK, or QAM, some WLAN transceivers spread the modulated carrier over a wider spectrum to comply with regulatory rules. This process, called *spread spectrum*, significantly reduces the possibility of outward and inward interference. As a result, regulatory bodies generally do not require users of spread spectrum systems to obtain licenses. Spread spectrum, developed originally by the military, spreads a signal’s power over a wide band of frequencies (see Figure 2-8).

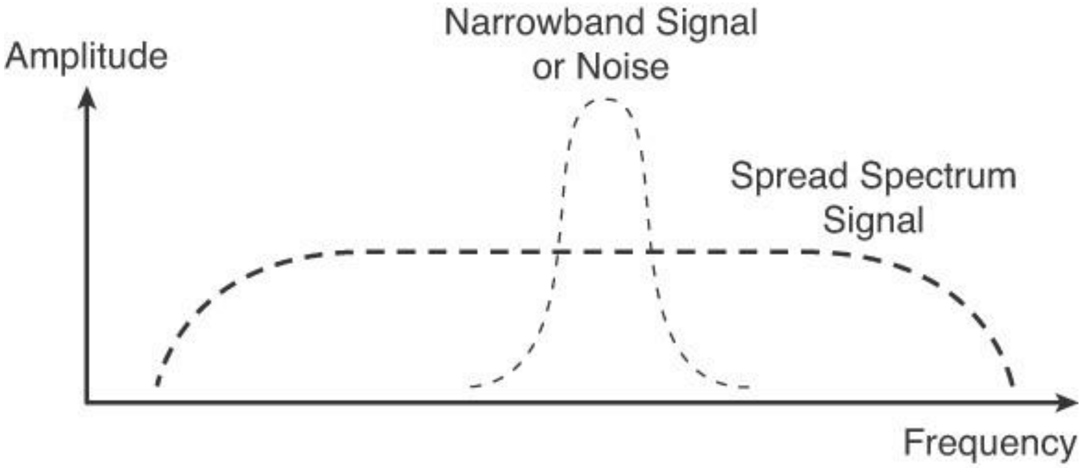


Figure 2-8 *Spread Spectrum Occupies a Wide Portion of the RF Spectrum*

Spread spectrum radio components use either direct sequence or frequency hopping for spreading the signal. Direct sequence modulates a radio carrier by a digital code with a bit rate much higher than the information signal bandwidth. Figure 2-9 is a hypothetical example of direct sequence that represents the transmission of three data bits (101) serially in time. The actual transmission is based on a different code word that represents each type of data bit (1 and 0). As shown in the figure, when sending a data bit 1, the radio sends the code word 00010011100 to represent the data bit. Similarly, when sending a data bit 0, the radio sends the code word 11101100011. The increase in the number of bits sent that represents the data effectively spreads the signal across a wider portion of the frequency spectrum.

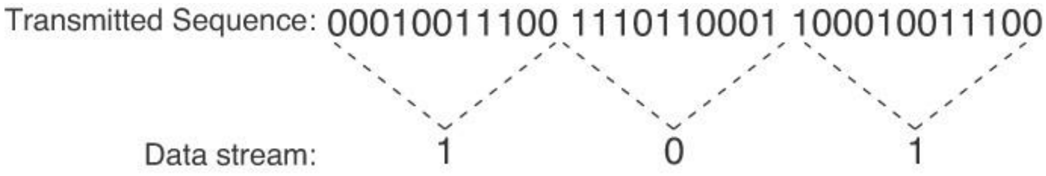


Figure 2-9 *Direct Sequence Is a Type of Spread Spectrum*

Frequency hopping uses a different technique to spread the signal by quickly hopping the radio carrier from one frequency to another within a specific range. Figure 2-10 illustrates this concept. The boxes labeled A, B, C, D, and E in the figure represent bursts of data that are sent at different times and frequencies. This also effectively spreads the signal across a wider part of the spectrum.

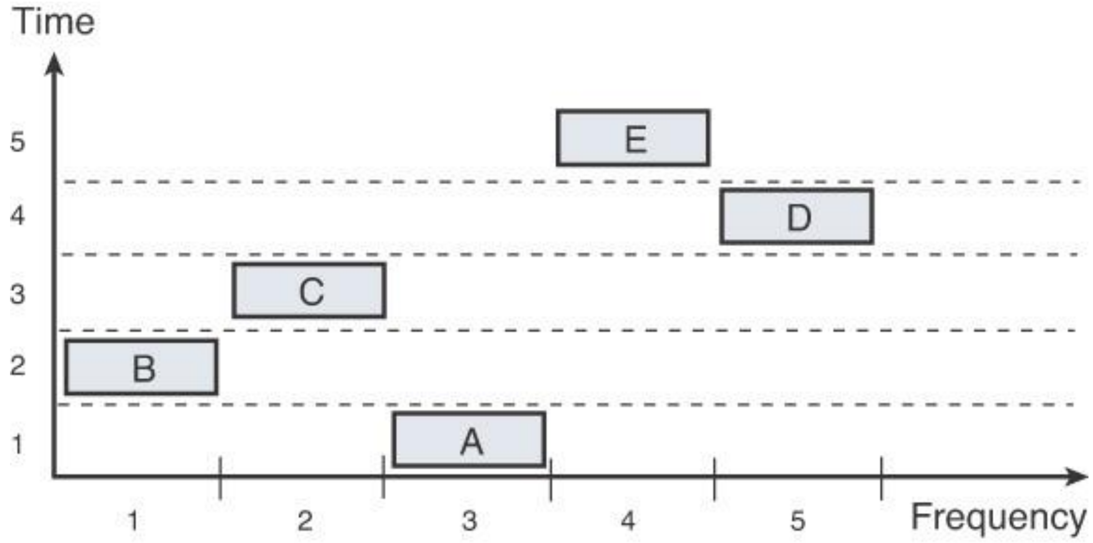


Figure 2-10 *Frequency Hopping Is a Type of Spread Spectrum*

The Advent of Frequency-Hopping Spread Spectrum

Hedy Lamarr, who was a well-known film actress during the 1940s, conceived the idea of frequency-hopping spread spectrum during the early part of World War II to keep the Germans from jamming the radios that guided U.S. torpedoes against German warships. (Lamarr was desperate to find a way she could help win the war against Germany. She was strongly opposed to the Nazis; in fact, she left her first husband for selling munitions to Hitler.)

Lamarr's idea was to transmit communications signals by randomly hopping from frequency to frequency to prevent the enemy from knowing what radio signal frequency to send for jamming purposes. It is amazing that she had no technical education but still thought of this very important communications concept.

Lamarr and film score composer George Antheil, who had extensive experience in synchronizing the sounds of music scores with motion pictures, set out to perfect the idea. One problem was how the torpedo's receiver was to know the frequency to listen to at specific times, because the idea was to send a random sequence of frequencies. Antheil was able to devise methods to keep a frequency-hopping receiver synchronized with the transmitter. His idea was to send signals to the torpedo using a long pattern of different frequencies that would appear to be random. The receiver, knowing the secret hopping pattern, would be able to tune to the correct frequency at the right time. This pseudo-random hopping sequence is what the frequency-hopping systems use today and what led to the development of other spread spectrum technologies.

Lamarr and Antheil sent details of their invention to the National Inventors Council. Charles Kettering, the director of the council, encouraged them to patent the idea. They filed the patent in 1941. Lamarr and Antheil then teamed with electrical engineers from MIT to provide the technical design. On August 11, 1942, Lamarr and Antheil received U.S. Patent Number 2,292,387 for their idea.

Because of the newness of the technology and clumsy mechanical nature of the initial design, spread spectrum was never used during World War II. The initial prototype used many moving parts to control the frequency of transmission and reception.

In the 1950s, Sylvania began experimenting with frequency hopping, using newly developed digital components in place of the initial mechanical system. By then, Lamarr and Antheil’s patent had expired. Sylvania, under contract with the U.S. Navy, used spread spectrum for the first time on ships sent to blockade Cuba in 1962. In the mid-1980s, the U.S. military declassified spread spectrum technology, and commercial companies began to exploit it for consumer electronics.

Lamarr and Antheil conceived an excellent modulation technique; however, they never received any compensation for their idea. Their main interest, expressed in a high degree of patriotism, was to help win the war against the Nazis. In March 1997, Lamarr and Antheil were honored with the Electronic Frontier Foundation’s Pioneer Award at its San Francisco convention, the Computers, Freedom, and Privacy Conference.

Orthogonal Frequency-Division Multiplexing

Instead of using spread spectrum, higher-speed WLANs make use of orthogonal frequency-division multiplexing (OFDM). OFDM divides a signal modulated with FSK, PSK, or QAM across multiple subcarriers occupying a specific channel (see Figure 2-11). OFDM is extremely efficient, which enables it to provide the higher data rates and minimize multipath propagation problems. OFDM has also been around for a while, supporting the global standard for asymmetric digital subscriber line (ADSL), a high-speed wired telephony standard.

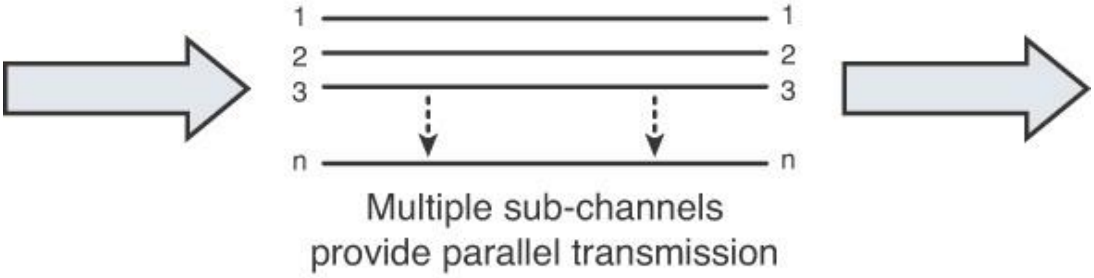


Figure 2-11 *OFDM Sends Multitudes of Data Simultaneously in Parallel*

Note

Some WLANs, such as 802.11ac, further increase data rate capability through spatial separation, which involves using the same modulation simultaneously within different portions of the frequency band.

RF Signal Propagation

A radio wave propagates fairly freely through the air and with some resistance through obstacles, such as walls and furniture. When deploying WLANs, you must be aware of several impairments, such as attenuation, noise, and multipath propagation, which impede the capability of a radio wave to successfully carry data to the destination.

Attenuation

As a radio signal propagates through the transmission medium, it experiences a decrease in amplitude (signal loss) referred to as *attenuation*. For example, a radio wave might have a signal amplitude of 20 dBm as it leaves the antenna at the source transceiver. After completing its journey of propagating through the transmission medium, the amplitude of the radio wave might be only –75 dBm.

Free Space Loss

A large part of the decrease in amplitude with attenuation results from what is known as free space loss (FSL), as depicted in Figure 2-12. The atmosphere causes the modulated signal to attenuate exponentially as the signal propagates farther away from the antenna. Therefore, the signal must have enough power to reach the desired distance at an acceptable signal level that the receiver needs for decoding purposes. The amplitude of a radio wave is proportional to the inverse of the square of the distance from the source. For example, if you double the distance between the transmitter and receiver, the amplitude of the radio wave at that location will be one-quarter of its initial value. Likewise, the amplitude of a radio wave is proportional to the inverse of the square of the radio wave’s frequency.

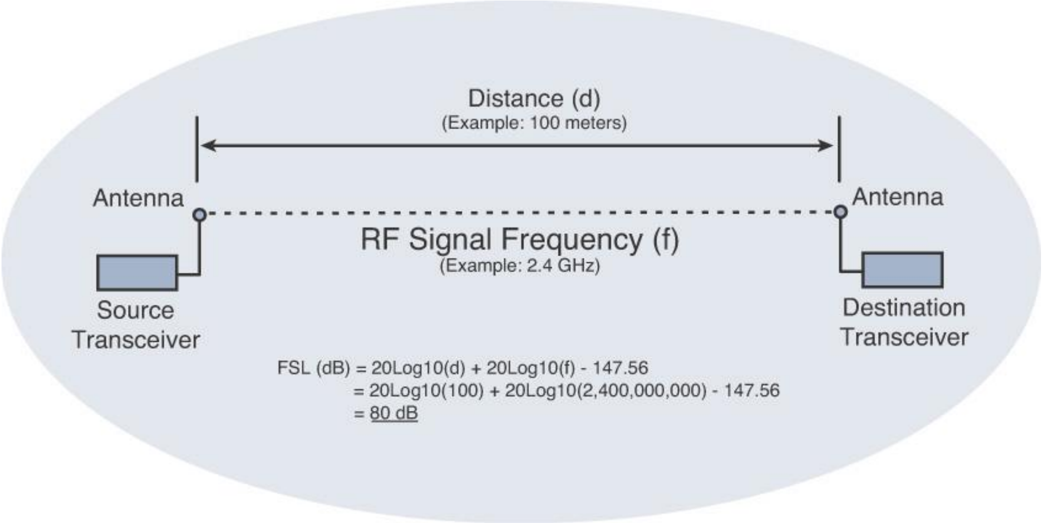


Figure 2-12 *Propagation of RF Signals Through the Air Medium Causes Significant Attenuation (FSL) to RF Signals*

You can calculate the attenuation (in dB) of a radio signal in free space (line of sight with no obstructions) by using the following formula:

FSL (dB) = 20Log10(d) + 20Log10(f) – 147.56

where d is the distance from the transmitter in meters, and the f is the frequency in Hertz.

For example, referring to Figure 2-12, you can calculate the FSL for an 802.11n (2.4 GHz signal) propagating over 100 meters as follows:

FSL (dB) = 20Log10(100) + 20Log10(2,400,000,000) – 147.56 = approximately 80 dB

If using 5-GHz frequencies for an 802.11n or 802.11ac implementation, the FSL at 100 meters would be as follows:

FSL (dB) = 20Log10(100) + 20Log10(5,000,000,000) – 147.56 = approximately 86 dB

Thus, the attenuation of radio waves based on FSL of a typical 802.11ac system is 80 to 86 dB over 100 meters. A 2.4-GHz signal with an amplitude at the source transceiver of 20 dBm, for instance, would only be –60 dBm (20 dBm – 80 dB) at 100 meters away from the source. Keep in mind that the preceding free space loss calculation is for completely open space, and other factors—such as the shape of the room and obstacles—might make the attenuation more or less. Also, note that the attenuation increases as the frequency increases; however, the actual effective range of the signal might be greater for the 5-GHz system because of less noise and interference in the 5-GHz band.

Physical Obstacles

As radio waves travel through physical obstacles, such as walls and ceilings, they decrease much more when compared to traveling through open air. The amount of attenuation varies significantly depending on the material, but a typical radio wave used in WLANs at signal amplitude of –60 dBm, for example, will decrease to approximately –63 dBm after going through an interior wall of a building (see Figure 2-13). In addition to walls, other obstacles, such as filing cabinets, shelves, fire doors, elevator shafts, and air conditioning ducts, offer varying amounts of attenuation. Also, be aware that some areas of the facility might have relatively high attenuation (50 dB or more), such as x-ray rooms in hospitals. In addition, some buildings have extensive steel and concrete support structures that can significantly attenuate radio waves.

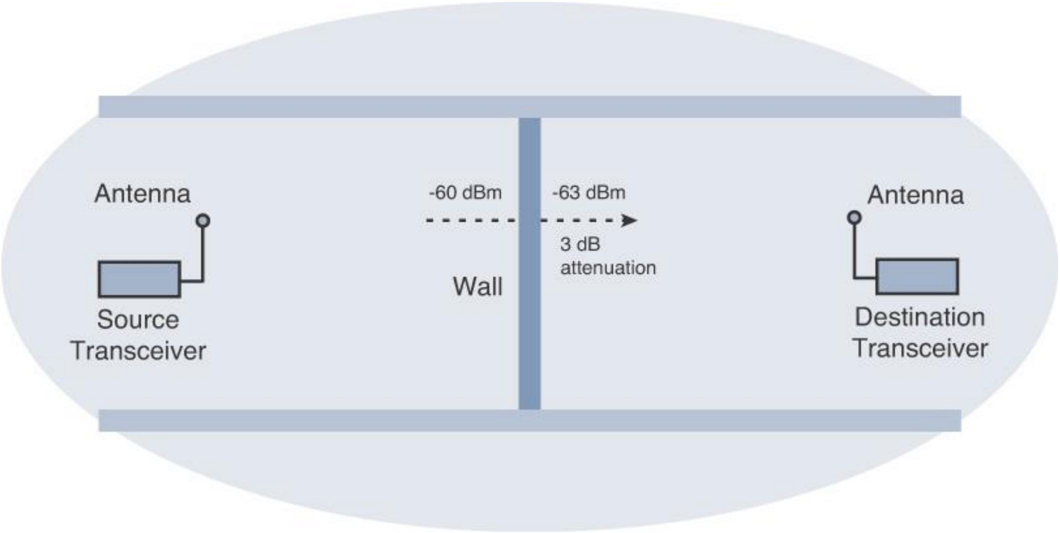


Figure 2-13 *Obstacles Contribute to the Attenuation of RF Signals*

If you are installing a wireless network outdoors, keep in mind that rain, fog, and snow increase the amount of water in the air and can cause significant attenuation to the propagation of modulated wireless signals. Smog clutters the air, adding attenuation to the communications channel, too. In addition, leaves on trees block transmissions in the spring and summer.

Note

See Chapter 15, "Performing a Wireless Site Survey," for details on how to ensure that a WLAN compensates for various transmission impairments.

Multipath Propagation

Multipath propagation occurs when portions of a radio wave take different paths when propagating from source to destination (see Figure 2-14). A portion of the signal might go directly to the destination, and another part might bounce from a desk to the ceiling and then to the destination. As a result, some of the signal will encounter delay and travel longer paths to the receiver.

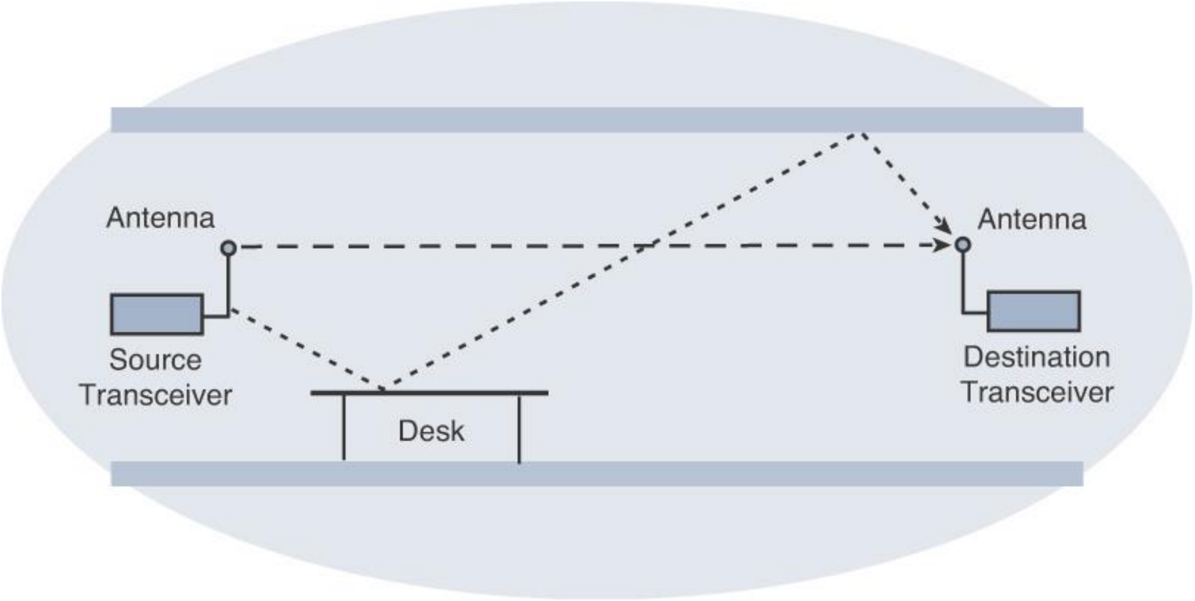


Figure 2-14 *Obstacles Get in the Way and Cause the Signal to Bounce in Different Directions*

Note

For more information about the impacts of multipath propagation, see Chapter 4, "Wireless LAN Implications."

Noise and Signal-to-Noise Ratio

The capability of a receiver to make sense of the radio waves it receives depends on the presence of other nearby radio waves, referred to as interfering signals, or noise. This noise can distort the communications, making it difficult for the receiver to correctly understand the data being sent. As an analogy, imagine two people, Evan and Shanna, trying to carry on a conversation while they are 20 feet apart. Shanna, acting as the transmitter, is speaking just loud enough for Evan, the receiver, to hear every word. If their baby, Kimberlyn, is crying loudly nearby, Evan might miss a few of Shanna's words. In this case, the interference of the baby has made it not possible to effectively support communications. Evan and Shanna need to move closer together, or Shanna needs to speak louder, or they need to find some way to make the baby stop crying. This is no different from the transmitters and receivers in wireless systems using radio waves for communications. It is possible to improve communications by either moving the transceivers closer together, increasing the transmit power, or reducing the surrounding noise.

In general, an average noise of –95 dBm (often referred to as *noise floor*) exists because of the electromagnetic impacts of the atmosphere. In addition to the noise floor, other electromagnet devices, such as microwave ovens, cordless phones, and other wireless networks, may operate sporadically and increase the average noise level to –90 dBm and even –80 dBm in some areas. As a result, it is very important to measure the noise and factor it in when designing a WLAN.

An important signal measurement is the signal-to-noise (SNR) ratio, which provides a figure of merit for a particular radio wave. The SNR (in dB) at a particular point (and point in time) in a network is simply the signal power (in dBm) of the radio wave minus the noise power (in dBm) at that point. Figure 2-15 illustrates the SNR.

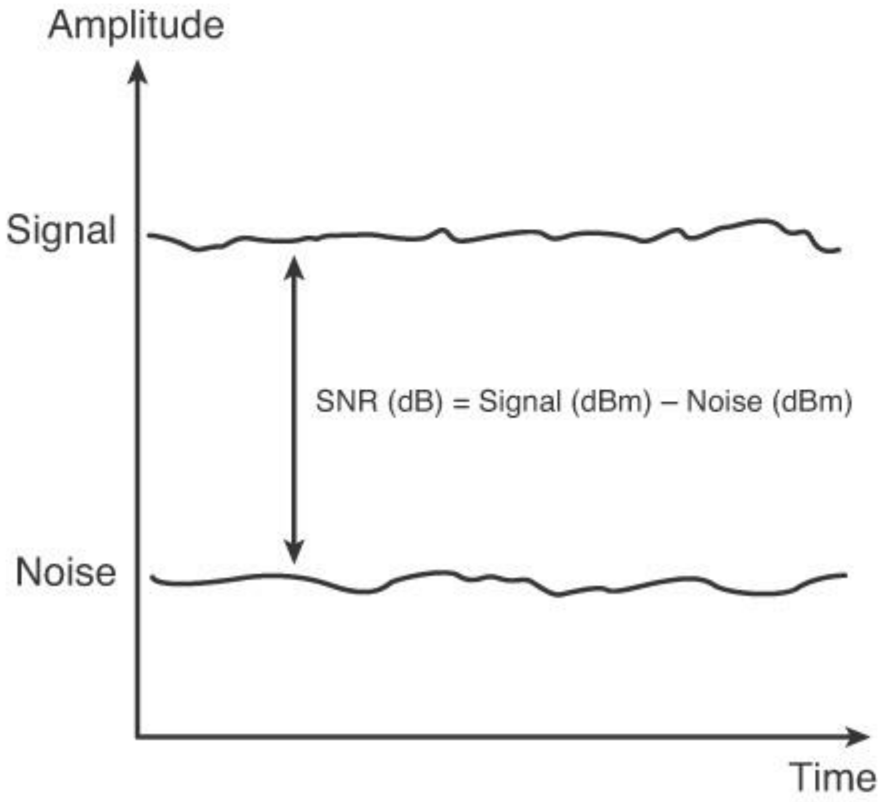


Figure 2-15 *SNR Is the Difference Between the Signal and Noise Power of a Signal at a Given Point in Time*

For example, a signal power of –65 dBm and noise power of –90 dBm yields an SNR of 25 dB. (The difference between values in dBm results in units of dB.) In other words, the signal in this example is 25 dB higher than the average noise, which generally provides excellent performance for 802.11 wireless networks. Even though the signal level is above the sensitivity of the receiver, the SNR must be positive to enable the receiver to distinguish the signal from the noise. For 802.11 wireless networks, it is important to ensure that the SNR at the receiver is at least 15 to 20 dB (maybe higher for some applications) to provide a safety margin to ensure that noise fluctuations do not cause too many retransmissions. Because of the varying operation of interfering sources, such as cordless phones, the noise levels (and corresponding SNR) can vary dramatically over time.

Note

For more details on radio frequency interference, see Chapter 4.

RF Mathematics

When working with WLANs, it is eventually necessary to perform RF mathematics, which involves converting units and dealing with gains and losses.

Converting Units

A problem is that technical literature for WLANs refers to both linear (watts) and logarithmic (dBm) units. The output power of an access point, for example, is generally given in mW. Most analyzers, though, display output power in dBm. Often, you must perform conversions so that all values are in the same units to determine path loss, calculate EIRP, and so on.

The following are relationships between mW and dBm:

dBm = (10Log10(mW))

and:

mW = 10(dBm/10)

As mentioned previously, dBm values do not fit into the linear world. For example, doubling the equivalent power in watts of 20 dBm is not 40 dBm. You can see this for yourself by using a calculator and finding the value in watts for 20 dBm. The answer is 100 mW. Now perform the calculation for 40 dBm, and you get 10,000 mW. That’s much more than doubling the power!

If you have a calculator with a logarithm (LOG) key, just punch in the numbers to get the results. For example, plug 100 mW into the equation for dBm, and you should find that the answer is 20 dBm. Try another one by converting 26 dBm to mW. You should get 400 mW. Instead of using a calculator, you can use a spreadsheet program, such as Microsoft Excel, to solve these types of problems.

To make life easier, you can memorize some simple relationships so that you can do RF mathematics easily without a calculator. A simple relationship is that if you multiply a value in mW by 10, the equivalent value in dBm increases by 10. (That is, dividing mW by 10 decreases dBm by 10.) The following are some typical equivalent values worth memorizing based on this rule:

0 dBm = 1 mW

10 dBm = 10 mW

20 dBm = 100 mW

30 dBm = 1000 mW (1 watt)

Also, if you multiply the value in mW by 2, the equivalent value in dBm increases by 3 dB (divide the value in mW by 2 and subtract 3 dB). For example, 10 dBm is equivalent to 10 mW. If you multiply 10 mW by 2, the resulting value in dBm is 13 dBm (10 dBm + 3 dB), which is equivalent to 20 mW. Similarly, if you divide 10 mW by 2, the resulting value in dBm is 7 dBm (10 dBm – 3 dB), which is equivalent to 5 mW. Thus, an antenna having 3 dB of gain doubles the transmit power of 100 mW (20 dBm), resulting in 200 mW (23 dBm). You could do this on a calculator, but it is much easier to calculate by remembering these simple rules.

Note

In communications systems, a dB (decibel) refers to the difference between one absolute value and another. For example, the difference between 12 dBm and 15 dBm is 3 dB.

As a practical example, say that you want to know the overall effective power in dBm of an access point that is set to 100 mW transmit power with an antenna having 6 dB gain. You might find yourself going through this exercise to know if the system is within regulatory limitations. You could use a calculator and convert 100 mW to dBm using the formula from above. Or, if you remember that 20 dBm equals 100 mW, all you have to do is add 6 dBm to 20 dBm, and you will end up with the correct answer of 26 dBm. The antenna gain of 6 dB adds 3 dBm to the value twice (that is, it doubles the power twice).

With a little practice, you will be quick with this type of mathematics. You might want to have a calculator nearby at first to check your work, but you will soon be running through these types of problems in your head.

Note

There are many online calculators for converting between dBm and milliwatts, such as the one at http://www.cpcstech.com/dbm-to-watt-conversion-information.htm.

Summary

Wireless LANs use radio waves to carry information between client devices and access points. A transceiver is a hardware component that transmits and receives radio waves. Modulation is a process that a transmitter implements to prepare the radio waves for propagation through the air medium. While en route between the source and destination, the radio waves encounter impairments, such as attenuation, noise, and multipath propagation, which can substantially reduce the amplitude and quality of the radio waves. SNR is a measurement that provides a figure of merit that characterizes the ability of a receiver for demodulating the radio wave successfully into information that the WLAN is conveying. To successfully decode a radio wave, the signal amplitude must be higher than the sensitivity of the reviver, and the SNR at the receiver must be high enough for the receiver to distinguish the signal from the noise.

Chapter 3. Wireless LAN Types and Components

This chapter will introduce you to:

- Types of Wireless LANs
- Wireless LAN Components
- Network Infrastructure Components

The 802.11 standard specifies details on how wireless LANs (WLANs) operate, with emphasis on stations (often referred to as client radios, or cards) and access points, which form ad hoc and infrastructure types of WLANs. This chapter defines each of these primary configuration types and components, as well as others.

Types of Wireless LANs

It is possible to configure WLANs into different architectures, depending on the requirements of the system. The physical architectures include the following:

- Ad hoc
- Infrastructure
- Mesh

Ad Hoc Wireless LANs

Ad hoc WLANs (sometimes referred to as "peer-to-peer" WLANs), as shown in Figure 3-1, only require 802.11 client radios in the client devices that connect to the network. Because there is no access point or WLAN controller and the stations are within range of each other, data transmitted by a particular source station travels directly to the applicable destination station. The rationale behind the ad hoc form of networking is to enable users to spontaneously set up WLANs. Access points are not necessary, which makes peer-to-peer networks easy to set up and take down. This can be beneficial, for example, if you want to establish a WLAN among several laptops in a conference room for a meeting in a building that has no WLAN that the laptops can connect to. These networks require no administration and very little preconfiguration. All that's needed to set up an ad hoc WLAN is to set the 802.11 radio in Microsoft Windows-based client devices to ad hoc mode.

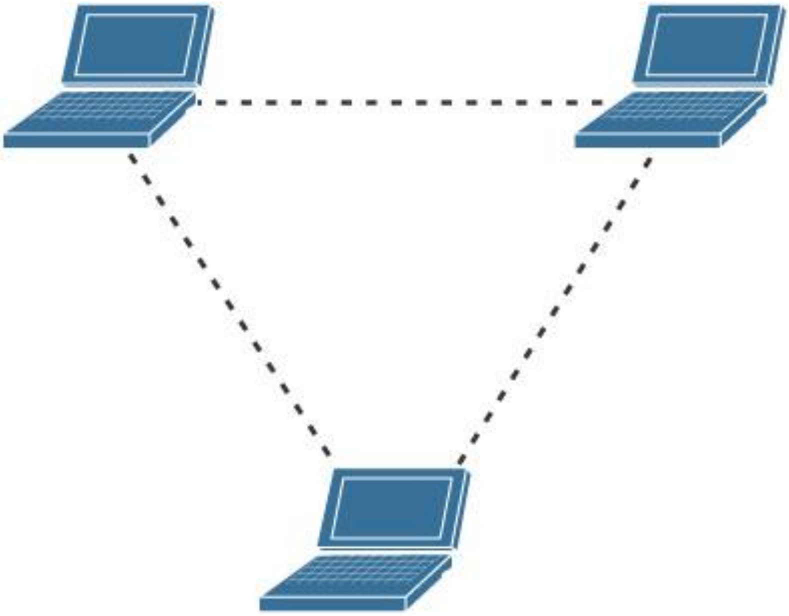


Figure 3-1 *An Ad Hoc Wireless LAN Provides Connectivity to Multiple Client Devices Within Radio Range of Each Other*

Note

The 802.11 standard refers to an ad hoc WLAN as an independent basic service set (IBSS).

The ad hoc form of communications is especially useful in public-safety and search-and-rescue applications. Medical teams require fast, effective communications when they rush to a disaster to treat victims.

They cannot afford the time to run cabling and install networking hardware. The medical team can use 802.11-equipped laptops and enable broadband wireless data communications as soon as they arrive on the scene.

The absence of an access point in an ad hoc network means that an ad hoc WLAN must take on more of the MAC-layer responsibilities. The first active ad hoc station (802.11-equipped client device set to ad hoc mode) establishes an IBSS and starts sending beacon frames, which are needed to announce the presence of the ad hoc network and maintain synchronization among the stations. Other ad hoc stations can join the network after receiving a beacon and accepting the IBSS parameters (for example, beacon interval) found in the beacon frame.

Each station that joins the ad hoc network must send a beacon periodically if it does not hear a beacon from another station within a short random delay period after the beacon is supposed to be sent. The random delay minimizes the transmission of beacons from multiple stations by effectively reducing the number of stations that will send a beacon. If a station does not hear a beacon within the random delay period, the station assumes that no other stations are active, and a beacon needs to be sent. After receiving a beacon, each station updates its local internal clock with the timestamp found in the beacon frame, assuming that the timestamp value is greater than the local clock. This ensures that all stations can perform operations, such as beacon transmissions and power management functions, at the same time.

Infrastructure Wireless LANs

Most companies, public hotspots, and homeowners implement infrastructure WLANs. An infrastructure WLAN, as shown in Figure 3-2, offers a means to extend a wired network. In this configuration, one or more access points interface wireless mobile devices to the distribution system. Each access point forms a radio cell, also called a basic service set (BSS), which enables wireless users located within the cell to connect to the access point. This allows users to communicate with other wireless users, as well as with servers and network applications connecting to the distribution system. A company, for example, can use this configuration to enable employees to access corporate applications and the Internet from anywhere within the facility.

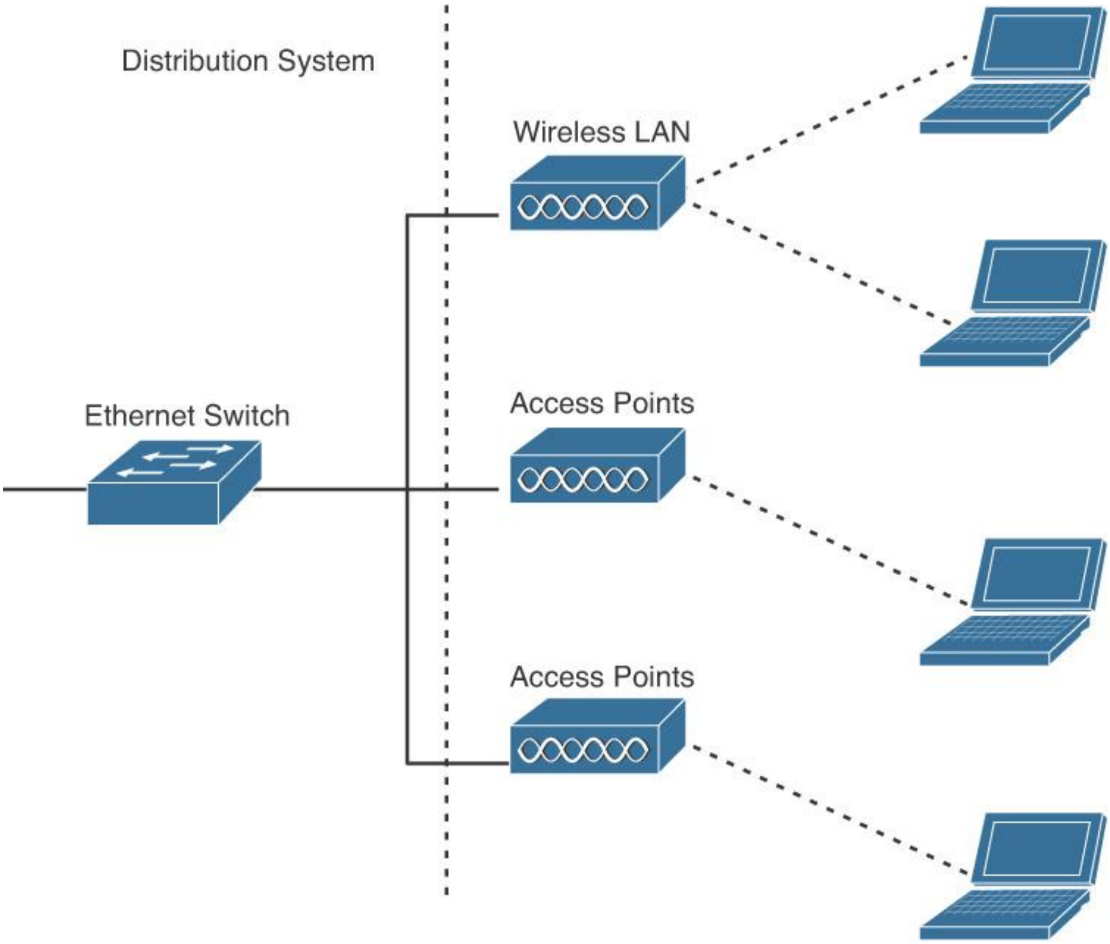


Figure 3-2 *An Infrastructure Wireless LAN Interfaces Client Devices to a Wired Distribution System and Extends Coverage Through Use of Access Points*

Each access point in the infrastructure WLAN broadcasts beacon frames, which identify the presence of the WLAN and synchronizes various events, such as 802.11 power management. Each access point creates a radio cell, with a coverage area that depends on the construction of the facility, chosen PHY layer, transmit power, and antenna type. This range is typically 100 feet in most enterprise facilities, depending on the data rate and environmental factors, such as building construction.

The desired level of performance, however, can impact the effective range of the access points. Lower data rates offer longer range than do higher data rates.

Note

The 802.11 standard refers to an infrastructure WLAN as an extended service set (ESS).

If a company installs access points with overlapping radio cells, as shown in Figure 3-3, then users can roam throughout the facility without any noticeable loss of connectivity. The radio card within the user’s mobile device will automatically re-associate with access points having stronger signals. For example, a user might begin downloading a file when associated with access point A. As the user walks out of range of access point A and within range of access point B, the client radio automatically re-associates the user to access point B and continues the downloading of the file through access point B. The user generally does not experience any noticeable delays, but voice over WLAN phones might drop connections if the roaming delay exceeds 150 milliseconds.

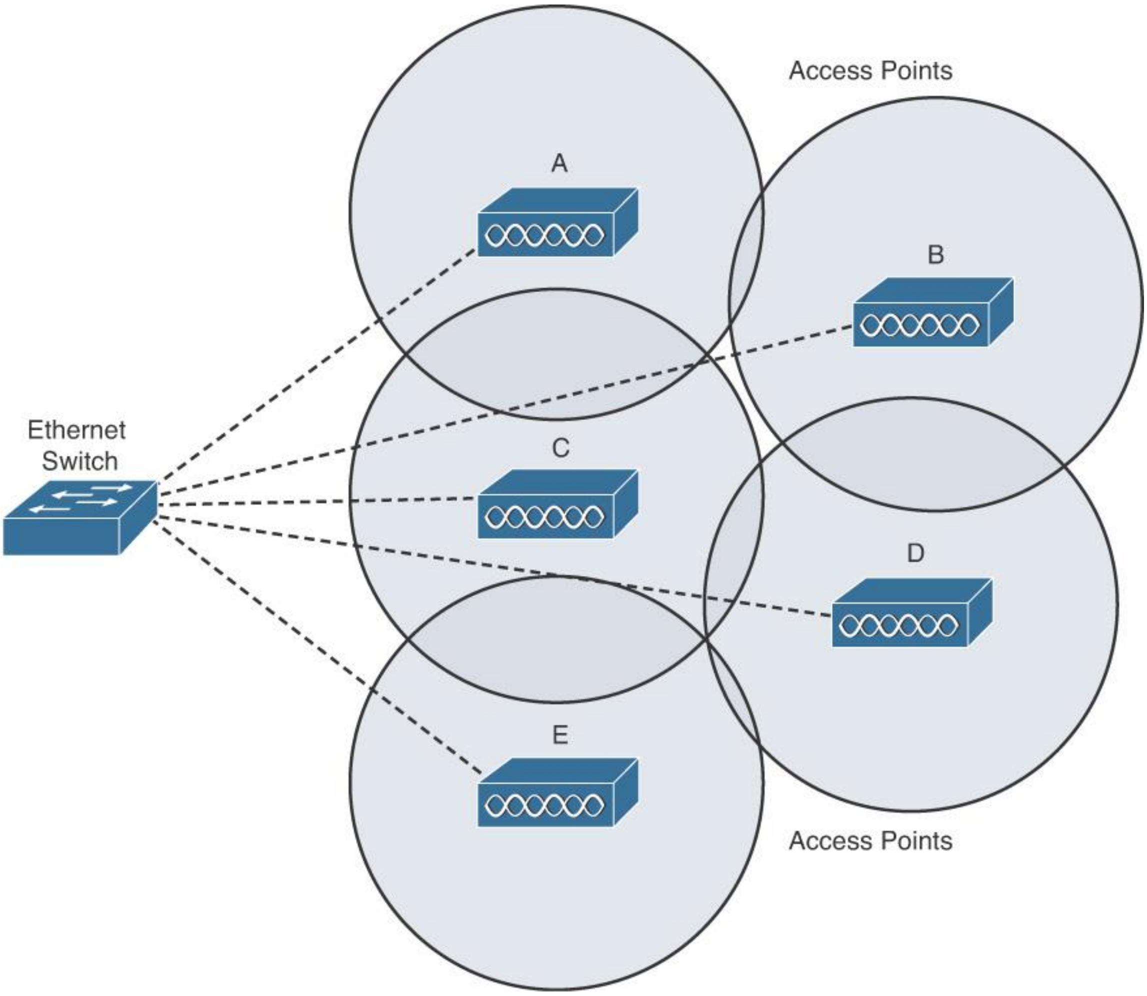


Figure 3-3 *Multicell Wireless LAN with Overlapping Cells Supports Roaming*

In infrastructure WLANs, data transmissions do not occur directly between the wireless clients. Data traffic going from one wireless user to another user must travel through an access point (see Figure 3-4). The access point receives the data traffic going from client A to client B, for example, and retransmits the data to client B. As a result, significant data traffic between wireless users decreases throughput because of the access point needing to relay the data to the destination user. If the source wireless user is sending data to a node on the distribution system, then the access point does not need to retransmit the data to other wireless users. The access point (if it is an autonomous type) delivers the data directly to the distribution system for routing to the applicable node. In the case of a controller-based WLAN, the access point hands over the data to an applicable controller, and the controller delivers the data to the distribution system.

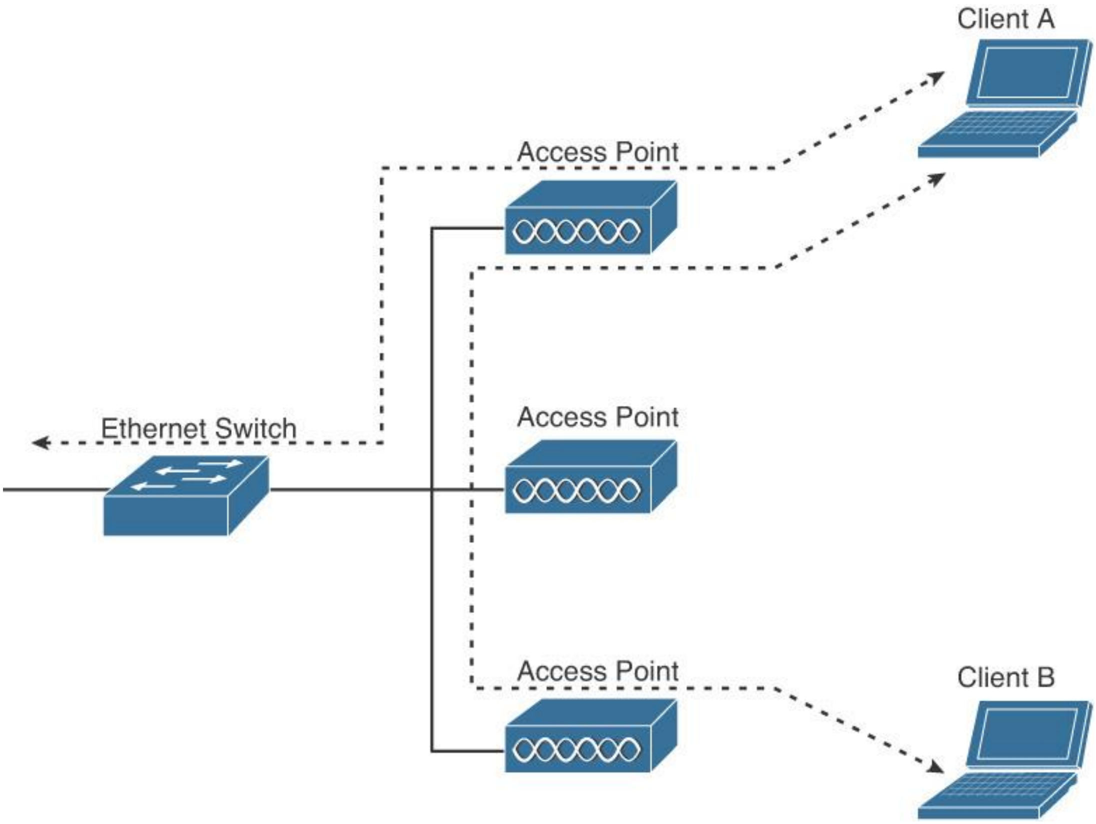


Figure 3-4 *Typical Flow of Data Through an Infrastructure Wireless LAN*

In addition to overlapping cells, the 802.11 standard also supports collocated and disjointed radio cells, as shown in Figure 3-5.

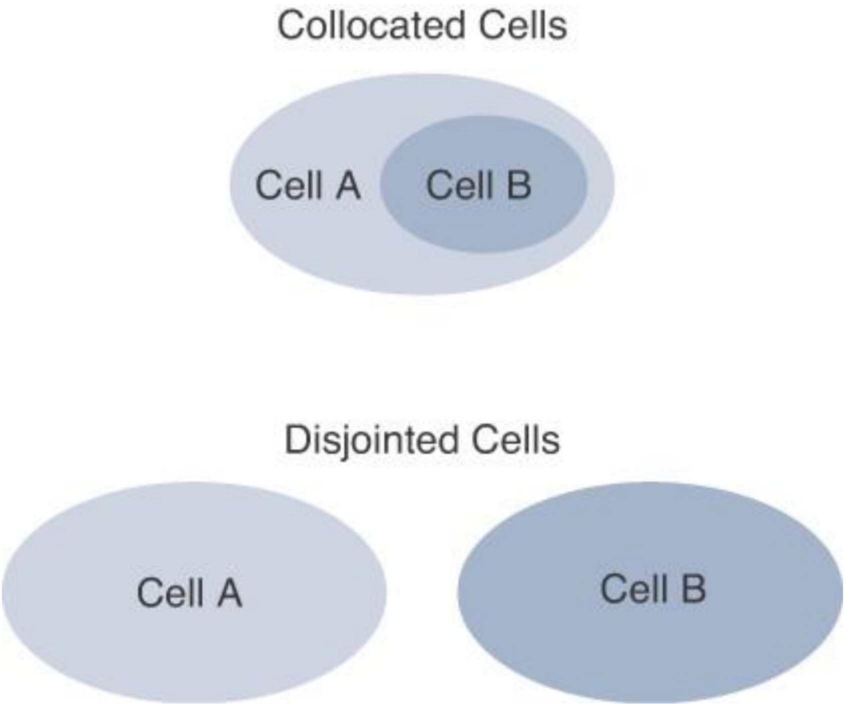


Figure 3-5 *Collocated and Disjointed Wireless LANs*

The collocated radio cell configuration is useful if a company needs greater capacity than a single access point can deliver. In this scenario, two or more access points are set up so that their radio cells overlap significantly. This works well if the access points are set to non-conflicting radio channels. A portion of the users in the area, for example, associate with access point A, and the other users associate with access point B. This boosts the capacity of that particular area.

A company can install disjointed access points when complete coverage throughout the facility is not necessary. For example, the company might install an access point in each conference room and not the rest of the building. If the radio cells are disjointed, then users will temporarily lose connection to the network and then re-associate when they come within range of another access point. An 802.11 network, though, supports this form of network, similarly to roaming with the overlapping radio cells. The re-association delay is a function of the time it takes the user to move into range of the next access point. The wireless application in use, however, might or might not be able to tolerate this longer roaming delay.

Wireless Mesh Networks

Wireless mesh networks make use of mesh nodes, which are similar to access points, except that mesh nodes connect to each other wirelessly rather than via Ethernet, as do most infrastructure wireless networks (see Figure 3-6). Thus, mesh networks avoid the need for Ethernet connections. You can install them just about anywhere, as long as electrical power is available (or you can use solar power for most outdoor installations).

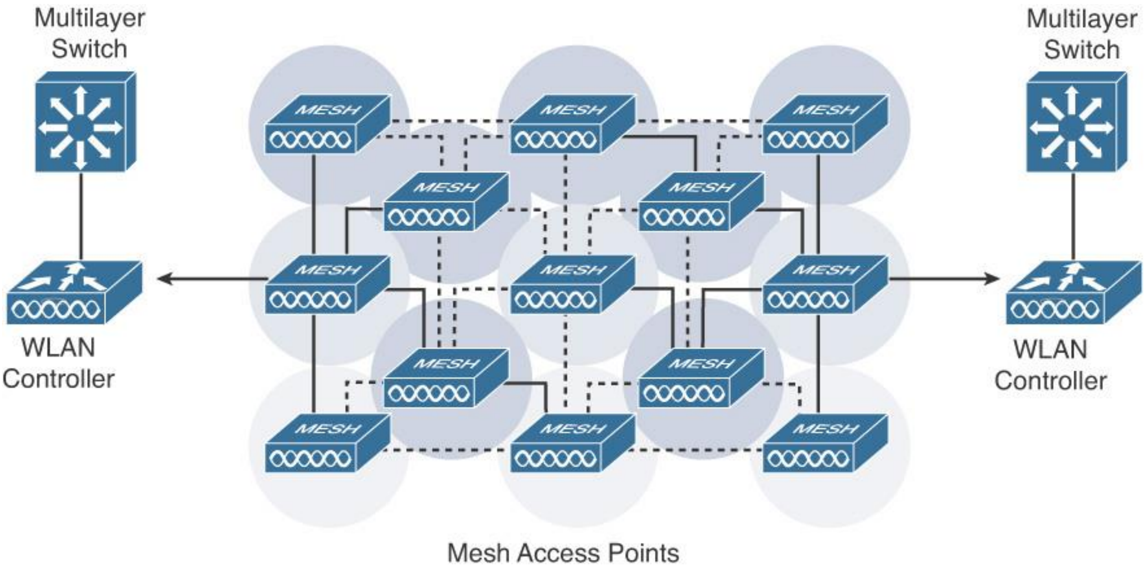


Figure 3-6 *A Mesh Network Includes Mesh Access Points That Connect with Each Other Wirelessly*

A mesh network is beneficial in areas where it is not feasible to install a traditional WLAN consisting of access points. For example, a mesh network approach makes sense in residential and city-wide Wi-Fi networks. The deployment of cabled access points over larger, open areas is a daunting task because of the massive amount of data cabling that must be installed and the countless permissions. Other places where installations of cabled access points are difficult include convention centers, college campuses, stadiums, marinas, parks, and construction sites.

Client devices connect to a mesh node similar to the method used for connection to an access point in an infrastructure network. Each mesh node implements a routing protocol that routes packets between client devices and wired connections to the Internet and servers. A mesh network offers multiple paths from source to destination, and intelligent routing algorithms allow each node to make a decision on which path to forward packets through the network to improve performance. If the link between a pair of nodes along one of the paths is congested, for example, then the algorithms establish another path that avoids the congested link.

Also, if a node goes down, an alternate route is chosen based on the routing algorithms.

Note

To extend the capability of 802.11 serving large-scale outdoor wireless networks, the 802.11 Working Group published an amendment to the 802.11 standard (802.11s) in 2011 to address special functions related to mesh networking. For example, 802.11s includes the Hybrid Wireless Mesh Protocol (HWMP), which provides a common multi-hopping routing protocol across mesh nodes.

Latency can vary significantly on mesh networks, depending on the number of users and hops that are necessary for moving packets through the backhaul network. Roaming and routing delays can affect performance, especially for VoIP applications. Even if the data rate between the user and the local backhaul node is kept high, which many of the mesh network vendors claim, the delays across the network might be substantial.

Often the lack of electrical power for mesh nodes in some areas leads to installation delays and unforeseen costs. In outdoor installations, some light poles do not supply adequate electrical power, or occasionally mounting assets, such as rooftops, do not have any readily available power. In these cases, the use of solar panels can be an option for generating power for mesh nodes and backhaul equipment. In this case, the network equipment actually runs off a battery, and the solar panel generates electricity to recharge the battery and power the mesh node if the battery is charged. Without a battery, there would be no power available at night or when something, such as clouds, obstructs the sunlight.

The use of solar energy is free, which can save electricity costs when running a mesh network. A problem, however, is that the cost of solar panels and batteries can be several hundred dollars for each mesh node. This makes the use of solar power generally feasible only where the cost of installing electrical lines is relatively expensive or where electricity is very unreliable. For example, Chittagong in Bangladesh decided to power some mesh nodes with solar energy because electrical power there is not stable enough.

If using solar panels for generating electricity for mesh nodes is appealing, then be certain to investigate average sunlight on a daily basis and ensure that the solar panels and batteries specified will supply an adequate amount of power for the equipment. This can be a bit tricky because predicting the amount of sunlight might not be accurate enough to satisfy network availability requirements.

Wi-Fi Mesh Hot Zones

Many large municipalities have installed or are planning to install Wi-Fi networks for creating city-wide wireless coverage. These deployments have had ups and downs in terms of signal coverage and performance, and they are very costly. As an alternative to covering large expansive areas, some municipalities and private entities, such as home and apartment owners, are building smaller-scale Wi-Fi networks (hot zones) that offer wireless Internet connectivity to smaller groups of people. This appears to be a more feasible approach.

For example, a municipality might install a Wi-Fi network to cover a 1- or 2-mile stretch of the town's main street, where it is likely that businesses and the public can strongly benefit from free Internet connectivity or mobile access to the Internet. Furthermore, an apartment owner might provide coverage to tenants, or a homeowner or an entrepreneur might offer Internet connectivity to a specific neighborhood. In many cases, the benefits of enabling web browsing, e-mail, and possibly voice telephony are enough to warrant the installation of a Wi-Fi hot zone.

Wireless LAN Components

Several different types of components comprise a WLAN.

Client Devices

As with a wired LAN system, a WLAN needs a way for users to gain access to applications and services. Whether the network is wireless or wired, a client device is an interface between the user and the network. Figure 3-7 illustrates examples of the client devices that can interface with a WLAN. In addition to client devices that people use, a wireless network can interface to machines, such as robots, and control systems. In this case, the client device is an end system, not a user device.

Figure 3-7 *Wireless LANs Support a Multitude of Client Devices*

The selection of the right client devices significantly impacts the usability of an application and the corresponding return on investment of the network. Think about application requirements and choose devices with the optimum weight, keypad, screen, battery longevity, and ruggedness. Client devices in warehouses, for example, will probably undergo more physical abuse than those in use in a typical office setting. Thus, in this scenario, choose rugged user devices that will withstand an industrial environment. Before rolling out hundreds of client devices to users, carry out testing at pilot sites with a representative group of users. That way, you will be sure that the chosen devices will best fit requirements. Also, involve upper management in the trials to receive adequate levels of buy-in, which of course is sometimes necessary to continue funding for a wireless project.

Implementing Client Device Wipe Functions

More and more companies are beginning to deploy device wipe functions (which erase a device's memory) to ensure that wireless client devices are secure in case they are lost or stolen. For example, an employee who's lost his/her device can inform a system administrator that the device is gone, and the administrator can issue a command to the device to wipe the memory and applications from the device. In case the device is out of range of the wireless network, functions of the device itself can be preconfigured to automatically perform the wiping if someone mistakenly enters the wrong username and password too many times. Just be sure to do a good job of replicating the device data on a server!

Client Radio

A client radio implements the 802.11 MAC-layer functions and a specific PHY layer, such as 802.11a, 802.11b, 802.11g, 802.11n, or 802.11ac. Figure 3-8 illustrates the primary internal components of an 802.11 client radio. Firmware on the radio implements 802.11 MAC-layer functionality, and a transceiver provides the actual transmitting and receiving tasks corresponding to the specific 802.11 PHY layer implemented. The bus interface binds the client radio to the client device (for example, laptop computer) via a bus interface standard. The software driver interfaces the client radio to the client device operating system, such as Microsoft Windows or Linux.

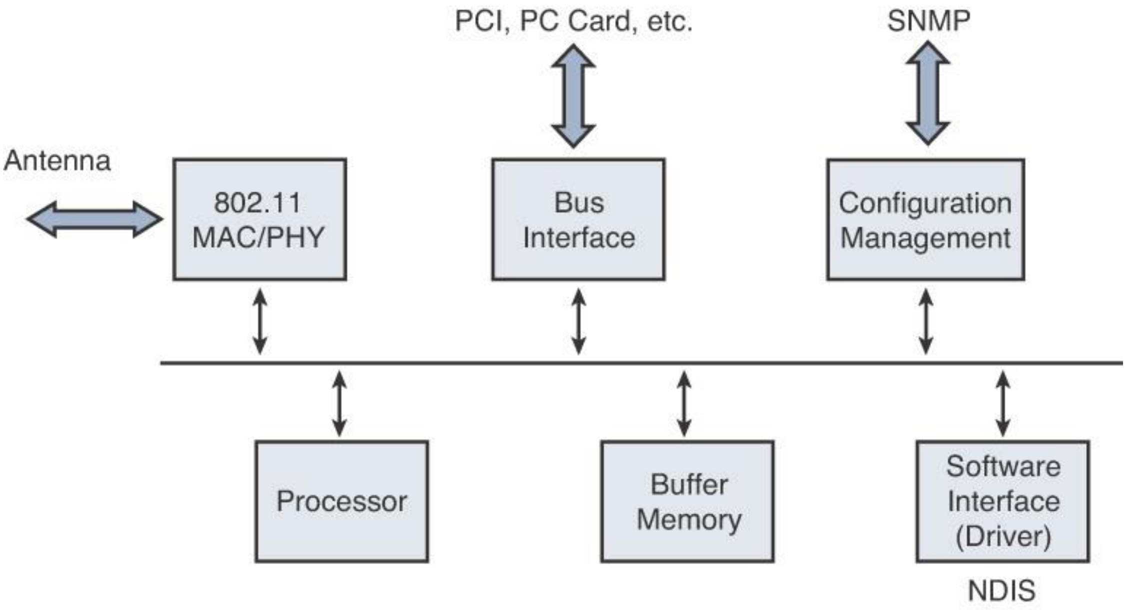


Figure 3-8 *An 802.11 Client Radio Includes Components Necessary to Interface Client Devices to an 802.11 Network*

Note

The 802.11 standard refers to client radio functionality as an 802.11 station (sometimes abbreviated as STA).

Multimode radios make it possible for client devices to associate with networks implementing different PHY layers. For example, an 802.11n client radio is backward compatible with 802.11g. With this dual-mode capability, for example, a user is equipped with WLAN interfaces that maximize interoperability and capability to migrate from 802.11g to 802.11n networks.

Computers process information in digital form, with low direct current (DC) voltages representing data 1s and 0s. These signals are optimum for transmission within the computer, not for transporting data through wired or wireless media. A client radio device couples the digital signal from the end-user appliance to the wireless medium, which is air, to enable an efficient transfer of data between sender and receiver. This process includes the modulation and amplification of the digital signal to a form acceptable for propagation to the receiving location.

The interface between the client device and the radio device includes a software driver that couples the client's operating system software to the card. This driver must be compatible with the operating system that the client device implements. Most client radios have drivers for Microsoft Windows, for instance. Drivers for Linux might be available, but they are sometimes difficult to find.

The client radio generally takes the shape of a wireless network interface card (NIC) that facilitates the modulator and communications protocols. The radio card conforms to one of several form factors that defines a physical and electrical bus interface that enables the radio card to communicate with a computing device. The following are types of standard form factors for interfacing client radios to client devices:

- Industry Standard Architecture (ISA)
- Peripheral Component Interconnect (PCI)
- Mini-PCI
- PC card
- ExpressCard
- CompactFlash (CF)
- Universal Serial Bus (USB)

Figure 3-9 includes photos of some of the various form factors.

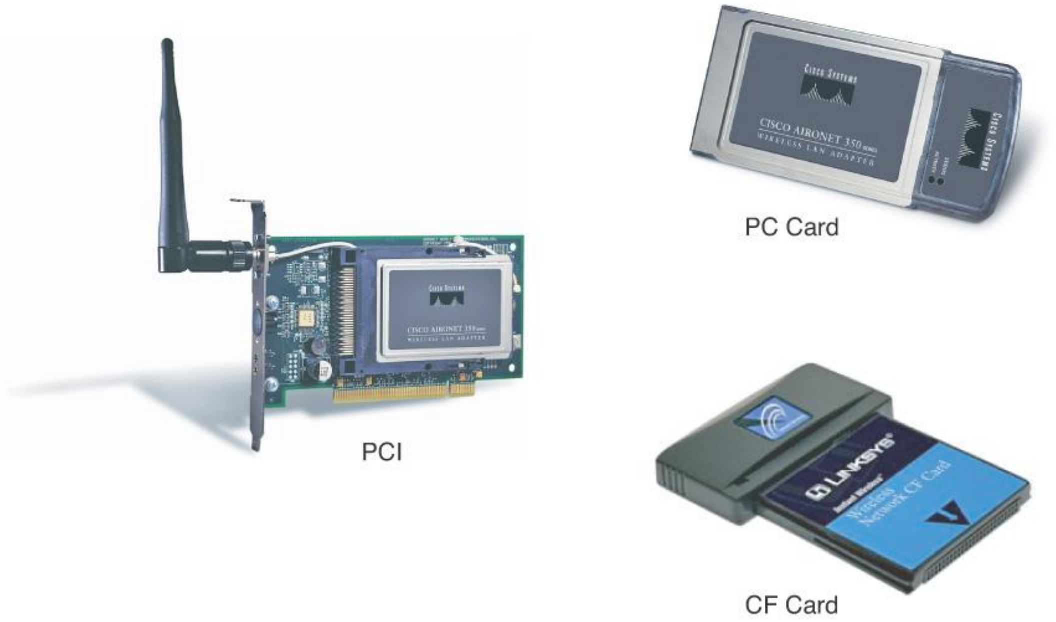


Figure 3-9 *Client Radio Cards Have Various Form Factors and Electrical Interfaces*

The sections that follow cover the form factors in greater detail.

Industry Standard Architecture

The Industry Standard Architecture (ISA) bus is a common bus interface in the desktop PC world. ISA has been around since the early 1980s for use in the IBM PC/XT and PC/AT. Because of this, the proliferation of ISA has been significant in desktops. Despite its lack of speed (2 Mbps), nearly all PCs manufactured up until a short time ago had at least one ISA bus. The ISA bus has failed, however, to advance at the pace of the rest of the computer world, and higher-speed alternatives are now available. It is not advisable to deploy ISA radio cards because of the likelihood that they will become obsolete.

Peripheral Component Interconnect

The Peripheral Component Interconnect (PCI) bus, which is the most popular bus interface for PCs today, has a throughput rate of 264 Mbps. Intel originally developed and released PCI in 1993, and it satisfies the needs of most recent generations of PCs for multimedia, graphics, and networking cards. PCI cards were the first to popularize Plug and Play (PnP) technology. PCI circuitry can recognize compatible PCI cards and then work with the computer’s operating system to set the resource allocations for each card. This helps save time and prevents installation headaches.

An example of a PCI radio card is the Linksys Wireless-N PCI Adapter.

Note

To ensure good connectivity with an access point, think about purchasing PCI cards that have external antenna connectors to allow the placement of an antenna on top of or next to the desk to avoid having the desk block the radio waves.

Mini-PCI

A Mini-PCI card is a small version of a standard desktop PCI card. It has all the same features and functionality of a normal PCI card but is about one-quarter the size. Mini-PCI cards are integrated in laptops as an option to buyers, with antennas that are often integrated out of view within the monitor's case or even up next to the LCD screen. A strong advantage of this form of radio card is that it frees up the PC card slot for other devices. In addition, manufacturers can provide Mini-PCI-based wireless connectivity at lower costs.

The Mini-PCI card is not without disadvantages, however. If you want to replace a Mini-PCI card yourself, you may have to disassemble most of the laptop—and doing so could void the manufacturer's warranty. Mini-PCI cards might also lead to lower performance because they require the computer to do some, if not all, of the processing. Despite these drawbacks, the Mini-PCI card has revolutionized the wireless laptop world.

PC Card

Developed in the early 1990s by the Personal Computer Memory Card International Association (PCMCIA), a PC card is a 16-bit credit card–sized peripheral device that can provide extended memory, modems, connectivity to external devices, and, of course, WLAN capabilities to laptops. Some PC card NICs are referred to as CardBus, which is a 32-bit implementation of a PC card. CardBus is faster and more likely to be the basis for 802.11n radio cards.

Antennas are generally integrated into a wireless PC card, with a stub that extends outside the PC card slot and provides omnidirectional RF propagation patterns. In most cases, these integrated antennas provide good performance. Some PC cards, however, come with optional removable antennas in case you have a need to use alternative, possibly higher-gain, antennas.

Some access points incorporate PC card radio NICs and are easily replaceable, accommodating newer technologies (for example, 802.11ac) as they become available. In most cases, end users can swap the radio NICs and do relatively simple firmware upgrades. This extends the life of the access point hardware, which of course saves money in the long run.

ExpressCard

ExpressCard provides high performance in a smaller form factor—about half the size of a PC card. PCMCIA developed the ExpressCard standard with assistance from the USB Implementers Forum (USB-IF) and the Peripheral Component Interconnect-Special Interest Group (PCI-SIG). Many feel that ExpressCard is the next generation of client card technology and will eventually replace PC card and CardBus. Because of its small design, ExpressCard radios are ideal for "closed box" wireless devices, such as data collectors.

CompactFlash

SanDisk Corporation first introduced CompactFlash (CF) in 1994, and WLAN radio cards based on CF form factors became available roughly a decade later. A CF card is very small, weighing half an ounce and less than half the thickness and one-quarter the volume of a PC card radio card. A CF card also draws very little power, which enables batteries to last longer than for devices using PC cards. Some PDAs come with direct CF interfaces, which results in a very lightweight and compact wireless PDA.

Universal Serial Bus

The majority of external 802.11 radio devices, such 802.11 modems and print servers, connect to client devices via Universal Serial Bus (USB), which provides electrical power and data interface to connected peripherals, such as 802.11 radios. The USB-IF has developed a series of USB specifications. USB 1.0, introduced in 1994, has a speed of 12 Mbps. In 2000, the USB-IF released USB 2.0, with a higher data rate of 480 Mbps. USB 3.0 (referred to as SuperSpeed USB), released in late 2008, has a speed that's 10 times faster than USB 2.0.

Note

In practice, you should limit the length of a USB cable to 16 feet.

Access Points

Similar to a client radio, an access point implements the common MAC functions and specific physical layers and provides a connection to a common distribution system (generally Ethernet). The access point is the primary component of an infrastructure WLAN. Figure 3-10 illustrates the primary internal components of an 802.11 access point.

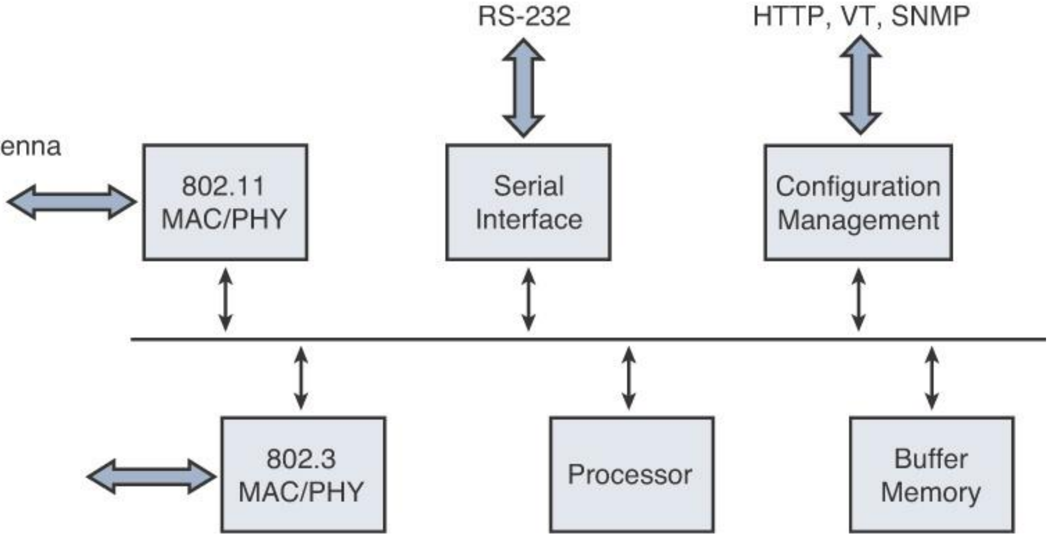


Figure 3-10 *An 802.11 Access Point Includes Components Necessary to Form an Infrastructure Wireless LAN*

Client radios associate with a single access point and can roam to different access points as the need arises, such as when roaming through a facility. In many cases, access points have multiple radios. For example, an access point might have a 2.4-GHz radio and a 5-GHz radio. This makes it possible to maintain some clients operating on 2.4-GHz channels and some clients operating on 5-GHz channels. For example, a lower-performance data application could operate at 2.4 GHz, and higher-performance applications, such as Wi-Fi phones, could operate at 5 GHz. That way, the phones won’t be bogged down by data applications.

Autonomous Access Points

Most WLANs implemented in the past made use of autonomous access points (see Figure 3-11), and many of those networks still exist today. An example of an autonomous access point is any Cisco access point that implements Cisco IOS software. An autonomous access point is relatively intelligent and implements enough functions to be able to interconnect with other access points via conventional Ethernet switches. The configuration of the access points is either done through specialized management software or by logging in to each access point individually.

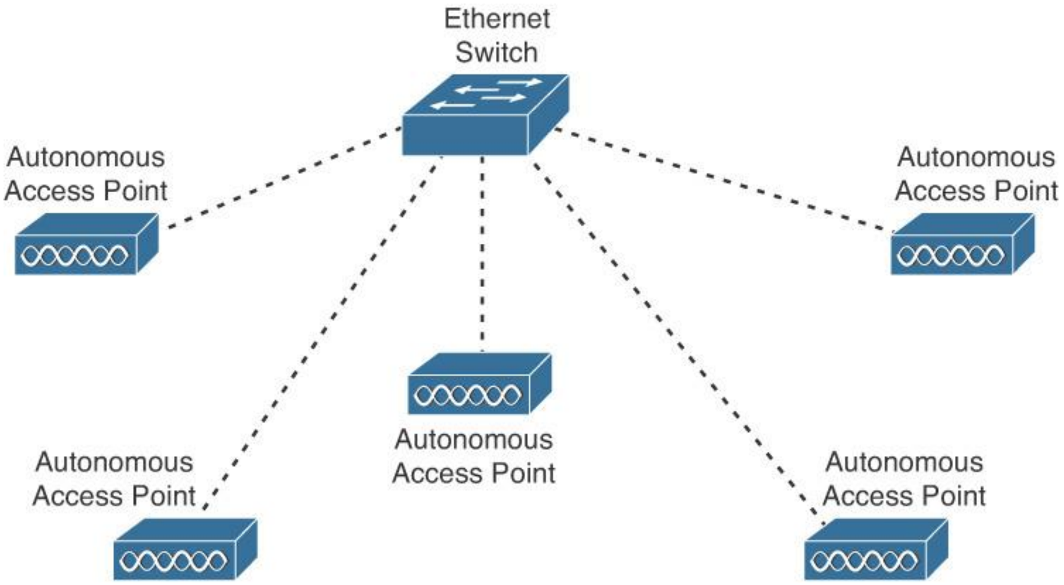


Figure 3-11 *Autonomous Access Points Offer Distributed Management and Control*

Controller-Based Access Points

As an alternative to traditional intelligent access points, some companies offer "lightweight" access points that implement the basic 802.11 functions (see Figure 3-12). An example of a lightweight access point is any Cisco access point that implements Cisco Lightweight Access Point Protocol (LWAPP) or the IETF standard Control and Provisioning of Wireless Access Points (CAPWAP). These lightweight access points connect to a WLAN controller, which provides centralized enhancements for management, security, and performance.

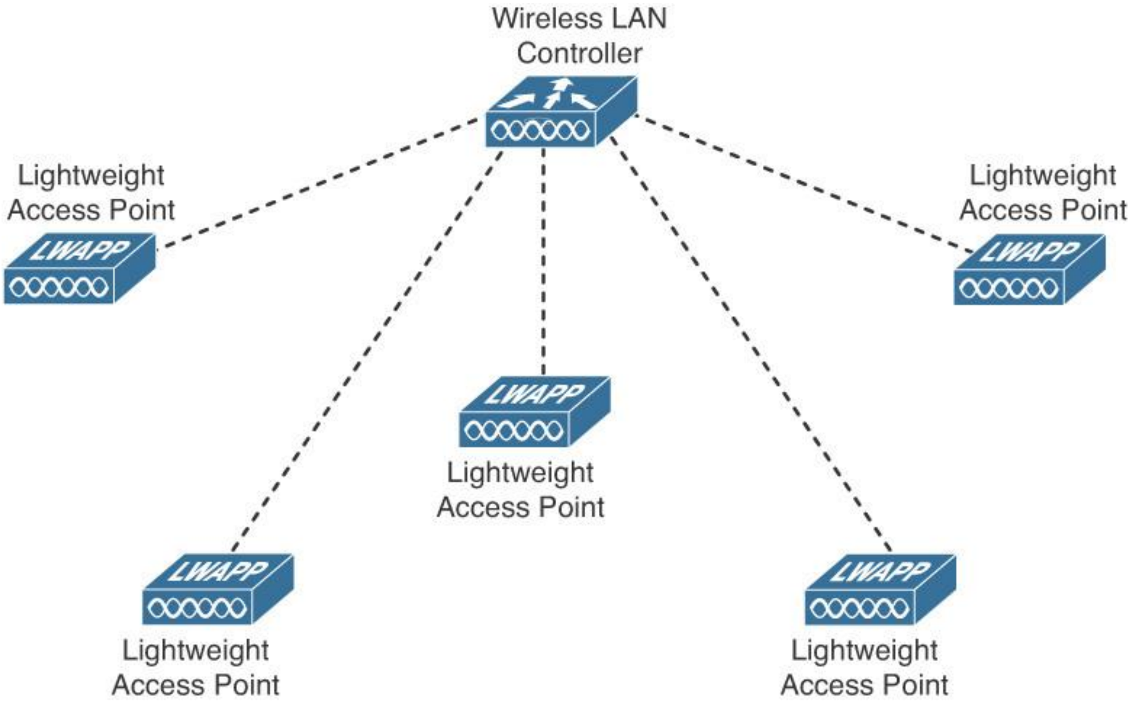


Figure 3-12 *Controller-Based Access Points Provide Centralized Management and Control*

Note

You can find an up-to-date list of 802.11-certified access points and client radio devices at the Wi-Fi Alliance website: www.wi-fi.org.

Wi-Fi Routers

By definition, a router transfers packets between networks. The router chooses the next best link to send packets on to reach the destination. Routers use IP packet headers and routing tables, and they use internal protocols to determine the best path for each packet. Most routers connect a LAN (like the one in your home or office) to a WAN (like the cable system running your cable modem) by interfacing a broadband modem to the network within the enterprise, small office, or home.

A WLAN router, such as the Linksys WRT300N, adds the function of an access point to a multiport Ethernet router. This combines multiple Ethernet networks with wireless connections, too. A typical WLAN router includes four Ethernet ports, an 802.11 access point, and sometimes a parallel or USB port so it can be a print server. This gives wireless users the same ability as wired users to send and receive packets over multiple networks.

There might be some confusion over the difference between WLAN routers and access points. The main thing to remember is that access points allow wireless clients access to a single network, while WLAN routers allow clients to browse several different networks. A router always takes the IP address into account to make decisions on how to forward (route) the packet; on the other hand, access points ignore the IP address and forward all packets.

In addition, WLAN routers implement the Network Address Translation (NAT) protocol, which enables multiple network devices to share a single IP address, generally provided by the Internet service provider (ISP). Wireless LAN routers also have the capability to provide port-based control, firewall management, and Dynamic Host Configuration Protocol (DHCP) services for client devices. These functions make the WLAN router much more versatile than an access point.

Consider using a WLAN router for the following reasons:

- **Sharing IP addresses:** Wireless LAN routers offer strong benefits in home and small office settings. For example, you can subscribe to a cable modem service that provides a single IP address through DHCP to the router, and the router then provides IP addresses via DHCP to clients on your local network. Figure 3-13 illustrates this concept. In such a setup, NAT maps a particular client on the local network to the ISP-assigned IP address whenever that client needs to access the Internet. As a result, you should use a WLAN router if you plan to have more than one networked device on a local network sharing a single ISP-assigned address. Instead of having one box for the router and another box for the access point, you can use a WLAN router that provides both in the same box.

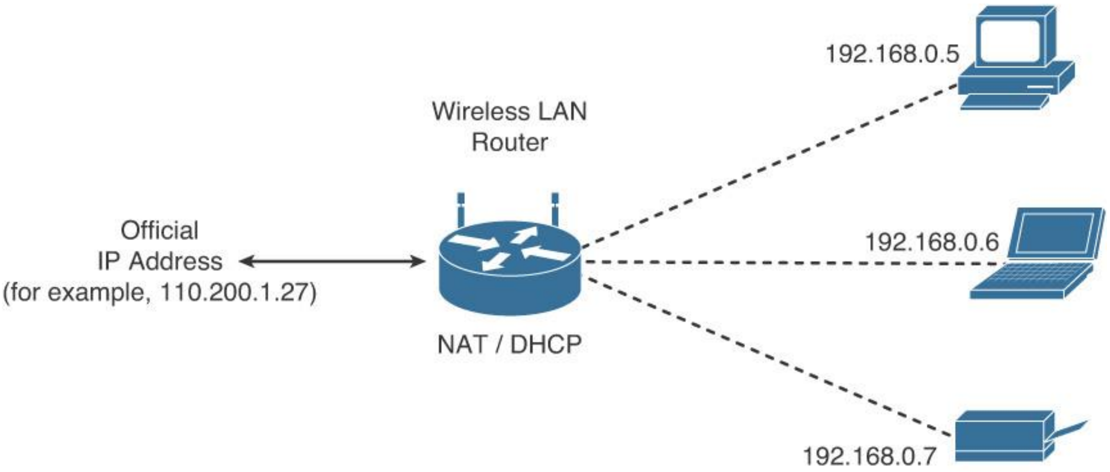


Figure 3-13 *Wireless LAN Routers Are Beneficial for Sharing a Single Official IP Address and Distributing Unique IP Addresses to Each Client Radio*

Note

For larger WLANs, such as for a hospital, it is generally best to make use of a dedicated DHCP server. In that case, the installation of access points rather than WLAN routers will be the most cost-effective and easiest to manage.

- **Connecting multiple networks:** Wireless LAN routers are ideal for wireless networks in public areas, especially if multiple networks are accessible. For instance, a university might have a separate network in each of its buildings. Students sitting outside might want to gain access to one or more of these networks and also surf the Internet. A WLAN router enables them to access everything through the wireless connection.
- **Improving network performance:** Because routers send packets only to specific, directed addresses, they do not forward the often numerous broadcast packets that are sent out by other devices. This results in an increase in throughput because of lower utilization on the network and less work needed by the router. This enables WLANs to operate much more effectively. The router, however, will offer more delay than an access point, but the impacts are generally unnoticeable.
- **Increasing security:** A strong advantage of WLAN routers is that they provide an added layer of security, on both the wired and

wireless sides. The wired side is usually protected by a firewall and has extensive access control filters. These filters can be set based on MAC address, IP address, URL, domain name, and even a set schedule that allows access only at certain times. If an unauthorized user tries to access the network, an e-mail alert is immediately sent to the network administrator. For supporting sensitive information, many WLAN routers support multiple and concurrent IPsec sessions, so users can more securely access networks through a range of virtual private network (VPN) clients.

Mesh Nodes

A mesh node is the primary component of a mesh network. Each mesh node includes an access point, which implements 802.11 and inter-node wireless connectivity to enable communications between mesh nodes. Client devices equipped with an 802.11 radio device connect to the access point functionality of the mesh node. A single radio can implement both the access point and the inter-node wireless connectivity. In multi-radio implementations, the access point can operate independently on a dedicated RF channel, while the internode communications takes place on a different RF channel. In this case, communications between the client devices and the mesh node can occur simultaneously with the internode communications. As a result, multi-radio mesh nodes provide better performance than single-radio solutions.

Antennas

An antenna couples RF energy between the radio transceiver and the air medium. The transmitter within a radio device sends an RF signal to the antenna, which acts as a radiator and propagates the signal through the air. The antenna also operates in reverse, capturing RF signals from the air and making them available to the receiver.

Some radio devices have integrated antennas that you cannot change. For example, laptops that have integrated wireless capability generally integrate the antenna within the cover or body of the laptop, which is not visible or changeable by the user. Some client devices, such as bar code scanners, use permanently mounted antennas. With these types of products, you have no choice but to use the antenna the vendor supplies. Other WLAN devices, however, have antennas that are interchangeable. In fact, it is a good idea to purchase access points with removable antennas. These allow more flexibility by enabling the selection of an antenna having characteristics best suited for the specific application.

The following are common antenna characteristics:

- **Antenna bandwidth and power:** For 802.11 WLANs, you need to use an antenna tuned for either 2.4 GHz or 5 GHz, depending on the spectrum on which the system is designed to operate. An antenna will work efficiently only if the frequency range of the antenna matches that of the radio. Antennas can handle a specific amount of power put out by the transmitter. In the case of 802.11, the antenna will generally be rated greater than 1 watt to handle the maximum peak transmit power of the radio device. For most applications, the antenna power specification will not be of too much concern to you because of the relatively low power that WLANs transmit.
- **Radiation pattern:** Antenna manufacturers provide illustrations indicating the radiation pattern of the antenna. The radiation pattern defines how radio waves propagate in relation to the antenna. This radiation pattern applies to both transmit and receive functions of the antenna. The antenna allows the transceiver to have a particular range in different directions for both sending radio waves and receiving them. The actual propagation of radio waves conforms to the radiation pattern. If you increase the transmit power of the transceiver, the range of the radio waves will increase with the same shape as the radiation pattern.
- **Antenna gain:** The gain of an antenna represents how well it increases effective signal power, with decibels (dB) as the unit of measure. Most antenna manufacturers specify antenna gains with

dBi unit, which is the true gain of the antenna relative to an isotropic antenna. An isotropic antenna has a radiation pattern that resembles a beach ball with an antenna at its center. An antenna with isotropic radiation pattern is theoretical and not physically used in practice.

- **Antenna diversity:** Antenna diversity, which makes use of multiple antennas for a single radio, can aid in combating multipath propagation. An access point may implement a spatial diversity antenna system, which consists of two antennas that interchangeably receive and transmit radio signals. An access point will receive a signal on both antennas, but many times, because of multipath propagation and interference, the same signal will not reach both antennas at the same time and strength. The access point will then perform internal calculations to optimize the received signal. The main benefits of spatial diversity antenna systems are improved coverage and signal reception.

The most common antenna types for WLANs have omnidirectional radiation patterns (see Figure 3-14). Omnidirectional antennas propagate RF signals in all directions equally on a horizontal plane but limit the range on the vertical plane. This radiation pattern resembles a very large doughnut with the antenna at the center of the hole. Omnidirectional antennas, having gains ranging up to 6 dBi, apply to most applications inside buildings. Omnis provide the widest coverage and make it possible to form somewhat circular overlapping cells from multiple access points located throughout the building. Most access points ship with standard omnis having relatively low gain. Consider using higher-gain ones to increase range, which enables wider spacing of access points. This can reduce the number of access points and reduce costs. To take advantage of the range benefits, though, the client devices must have equivalent gain antennas and transmit power of the access points.

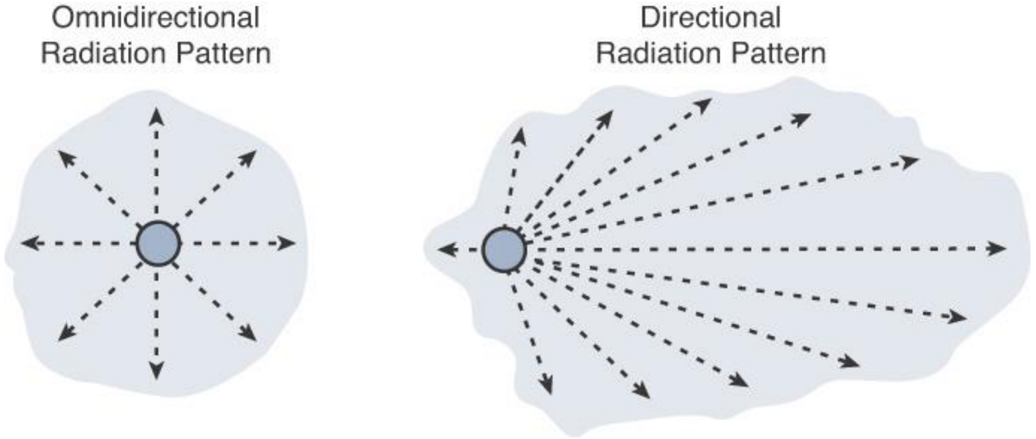


Figure 3-14 *Omnidirectional and Directional Radiation Patterns of Antennas*

Note

It is important to note that the actual propagation of radio waves in relation to an antenna might be somewhat different than the radiation pattern (which is based on an open area). Obstructions such as walls and office furniture attenuate the signals, which might cause them to travel differently than the radiation pattern.

A directional antenna (often called a yagi) transmits and receives RF signals more in one direction than others (refer to Figure 3-14). This radiation pattern is similar to the light that a flashlight or spotlight produces. Directional antennas have higher gain, such as 9 or 12 dBi, and have a narrower beam width, which limits coverage on the sides of the antennas.

Directional antennas work best for covering large, narrow areas or supporting point-to-point links between buildings. In some cases, a directional antenna will reduce the number of access points needed within a facility. For example, a long loading dock of a distribution center might require three access points having omnis, but the use of a high-gain directional antenna would likely require only a single access point.

RF Amplifiers

Similar to the gain associated with an antenna, an external RF amplifier increases the effective power of the RF signal. An amplifier is installed between the antenna and the access point, as shown inFigure 3-15, and it must be designed to amplify the frequency range in which the WLAN operates (for example, 2.4 or 5 GHz). RF amplifiers for WLANs specify a range of power inputs and deliver a constant power output. For example, a 4-watt RF amplifier will deliver 4 watts to the antenna when the input to the amplifier is between 1 and 100 mW. An amplifier also has a receive gain specification (for example, 12 dB), which defines how well the amplifier can increase the power of the signals that it receives. If the antenna is mounted outdoors, it is important to use a lightning protector and properly ground the system. To avoid excessive cable attenuation, use low-loss coaxial cable and keep cable runs as short as possible.

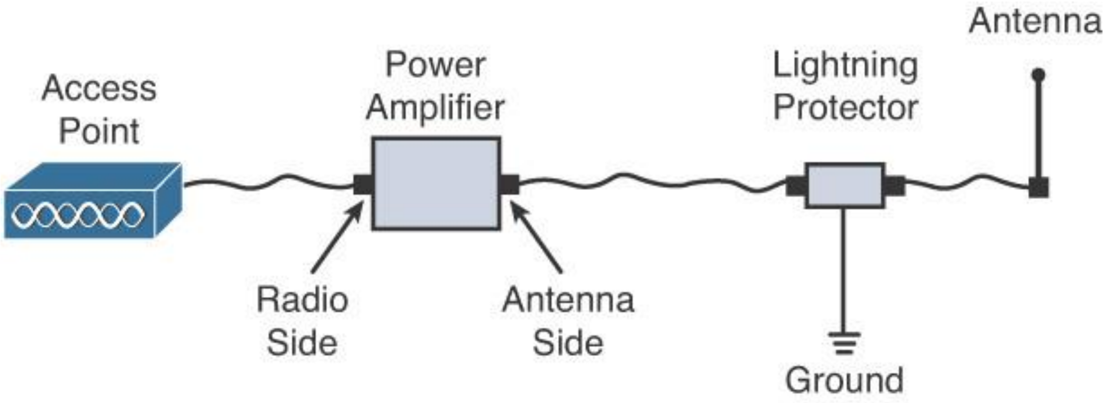


Figure 3-15 *Power Amplifiers Boost RF Signals to Increase Range*

Note

When purchasing RF amplifiers, you must comply with special licensing requirements.

Consider using an RF amplifier to extend the range of an access point, especially for outdoor areas. For example, you might have an area needing signal coverage where it is not practical to install an access point or a mesh node. In this case, the amplifier might be able to increase transmit and receive gains enough to cover the area.

Repeaters

A repeater regenerates radio signals to extend the range of a WLAN. As shown in Figure 3-16, a repeater does not physically connect by wire to any part of the network. Instead, a repeater receives radio signals (802.11 frames) from an access point, a wireless client device, or another repeater on a particular RF channel and retransmits the frames without changing the frame contents on the same RF channel. This makes it possible for a repeater located between an access point and a distant user to act as a relay point for frames traveling back and forth between the user and the access point. As a result, wireless repeaters are an effective solution to overcome signal impairments such as RF attenuation. The wireless repeater fills in the coverage holes.

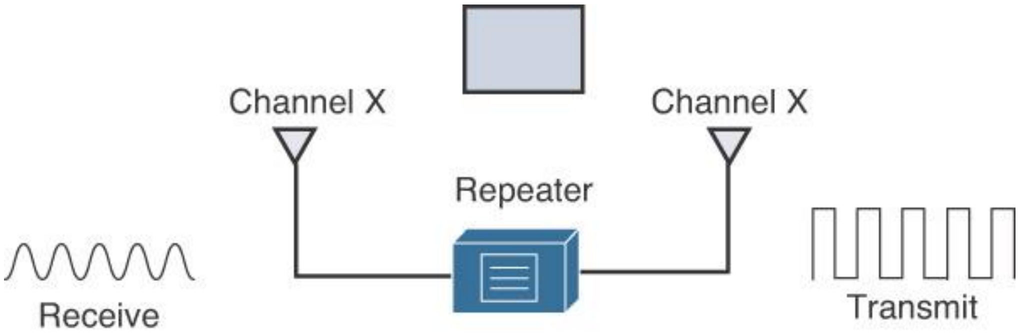


Figure 3-16 *A Repeater Reshapes RF Signals and Extends the Range of a Wireless LAN*

A downside of using a wireless repeater, however, is that it will reduce throughput capacity of the WLAN by roughly 50 percent in the area covered by the repeater. A repeater must receive and retransmit each frame on the same RF channel, which effectively doubles the number of frames that are sent over the WLAN. This problem compounds when using multiple repeaters because each repeater duplicates the number of frames sent. Thus, be sure to plan the use of repeaters sparingly and keep the total count within a particular area below three.

Bridges

A bridge provides a method for connecting dissimilar networks. A remote bridge connects networks that are not next to each other, such as networks in different buildings. With remote bridges, directional antennas are most often used to form a point-to-point or point-to-multipoint network. Workgroup bridges are advantageous for connecting one or more client devices (which do not have wireless client radios) to a WLAN. These types of connections offer a substitute for a client radio device, making it useful when the device, such as a printer, PC, or video game console, has an Ethernet port and no 802.11 radio card. In some cases, you might have no way of adding a radio device to a particular client device, which makes using a bridge the only way to go wireless. Figure 3-17illustrates various bridge configurations.

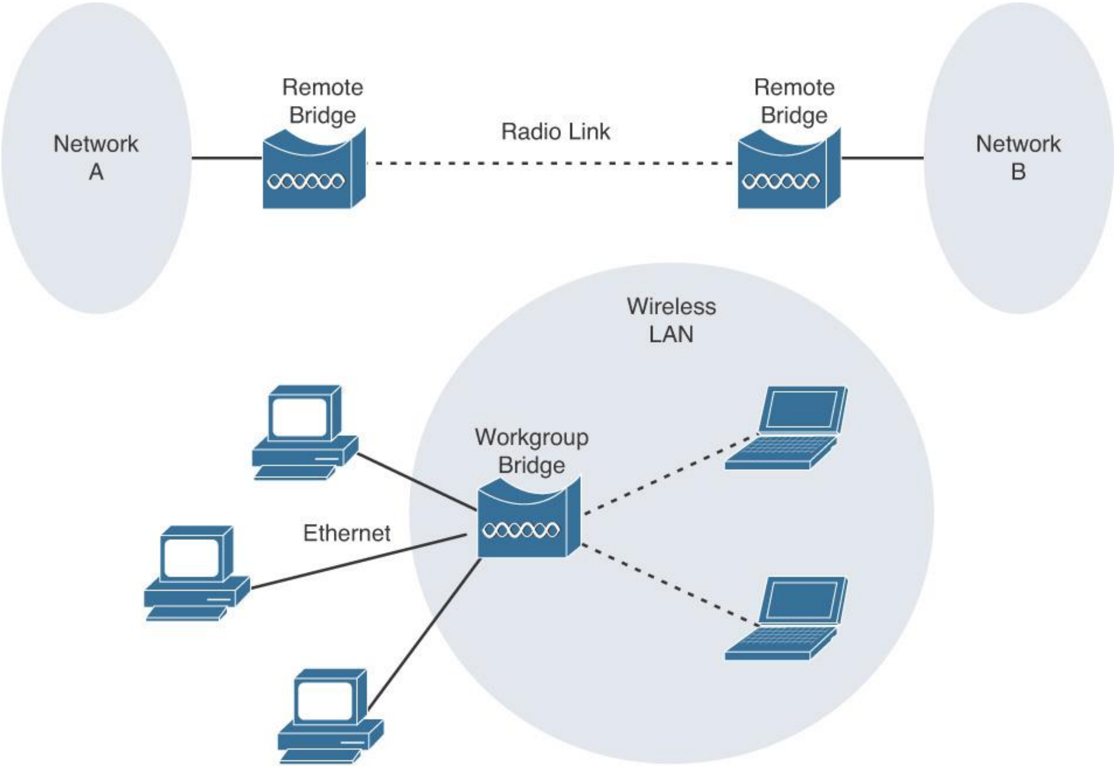


Figure 3-17 *Bridges Offer Multiple Methods for Connecting Client Devices and Networks*

A bridge receives packets on one port and retransmits them on another port. A bridge will not start retransmission until it receives a complete packet. Some bridges retransmit every packet on the opposite port, whether or not the packet is heading to a station located on the opposite network. A learning bridge, which is more common, examines the destination address of every packet to determine whether it should forward the packet based on a decision table that the bridge builds over time. This increases efficiency because the bridge will not retransmit a packet if it knows that the destination address is on the same side of the bridge as the sending address. Learning bridges also age address table entries by deleting addresses that have not been heard from for a specified amount of time.

Create Bookmark

Network Infrastructure Components

A complete wireless system consists of more than what the 802.11 standard specifies. Other components are necessary to fully depict an architecture that satisfies application requirements. You need to specify these components when designing a system. Some of these components, such as a distribution system, might already be present in the facility where you are installing a WLAN. Companies generally have existing distribution systems, such as Ethernet LANs and WAN connectivity.

The following types of components compose a network infrastructure:

- Network distribution system
- Power over Ethernet
- Application connectivity software

The sections that follow cover the infrastructure components in greater detail.

Network Distribution Systems

Designers of the 802.11 standard purposely avoided defining a particular distribution system (refer to Figure 3-2) for connecting access points; rather, they left system architects the freedom to implement 802.11-compliant networks as effectively as possible, given the situation. As a result, you need to decide what technologies and products will constitute a distribution system if multiple access points are necessary to extend the range of a complete wireless system.

In most cases, you can specify an Ethernet network infrastructure to act as the distribution system. All enterprise 802.11 access points are capable of connecting to Ethernet networks. Even mesh nodes generally have Ethernet ports for enabling a mesh node to communicate with a central tower for backhaul purposes.

Switches

An 802.3-based distribution system (also referred to as the wired backbone) consists of switches or hubs that tie together users (PCs and access points) equipped with 802.3 client cards. The switch or hub is somewhat analogous to an 802.11 access point. The main difference, obviously, is that the hub or switch provides the connections over a physical medium, and an access point uses radio waves.

A hub offers a single collision domain among multiple wired users. When one user’s Ethernet NIC sends data, all other stations connected to the LAN hold off sending data until the medium is idle. A traditional access point most closely resembles a hub. A switch is more sophisticated than a hub and connects one user to another without blocking access of other users. The switch improves throughput because of the smaller resulting collision domains. Users do not have to wait until others are finished before sending data. This is why you should use switches rather than hubs for interconnecting wireless access points and controllers, especially for 802.11ac networks. Hubs are considered “old” technology and are used only in very small networks; they are nearly nonexistent in enterprise networks.

Figure 3-18 compares the flow of packets through a hub and through a switch.

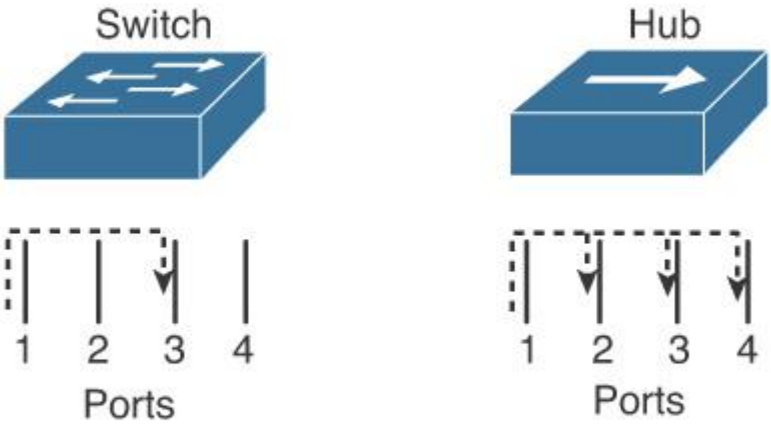


Figure 3-18 *Hubs and Switches Treat Frames Differently*

In a WLAN, the switch or hub connects access points. This creates a wired backbone and enables WLAN roaming protocols to work. Most access points accommodate connection to a switch or hub via an RJ-45 connector and twisted-pair wiring. The Ethernet cable can be up to roughly 300 feet long. As a result, you need to plan the installation of hubs or switches to avoid exceeding this distance. If distances exceed 300 feet, you can interconnect switches via optical fiber and place switches close to access points in various parts of the facility.

Consider the following when deploying a distribution system for a WLAN:

- **Use a hub only for very small deployments:** If the WLAN consists of only a few access points, then you can probably get by with a hub. There is no need to pay extra money for a switch for smaller deployments in this situation if you have an older hub lying around. In addition, digital subscriber line (DSL) and cable modem interfaces generally come equipped with a built-in, four-port Ethernet hub.
- **Use switches for enterprise-wide deployments:** A larger WLAN with many access points will benefit from the use of Ethernet switches. For very large networks, consider implementing a master switch that interconnects a series of smaller switches. Connect the switches together using optical fiber to improve security and increase the range of the distribution system.
- **Select the appropriate data rate:** In most cases, 10-Mbps Ethernet was sufficient to support interconnections among 802.11b access points, but you need 100 Mbps/1 Gbps (preferred) data rates for 802.11n and possibly higher data rates for 802.11ac.
- **Create a separate IP domain for the WLAN or SSID:** Some network devices continuously send broadcast packets that propagate freely throughout Ethernet networks. Access points also forward these broadcast packets to all users on the WLAN. In many

enterprise scenarios, the broadcast packets will flood the WLAN and severely limit performance for wireless users. So separate the WLAN (or possibly each SSID) from the rest of the corporate network through a router or separate virtual LAN (VLAN). Keep in mind that a controller-based network may block broadcast packets by default, making it unnecessary to use separate domains for blocking broadcasts.

Optical Fiber

If you need a very high degree of noise immunity or information security, consider using optical fiber rather than UTP. Optical fiber is a medium that uses changes in light intensity to carry information from one point to another. An optical-fiber distribution system consists of a light source, optical fiber, and a light detector. A light source changes digital electrical signals into light (that is, on for a logic 1 and off for a logic 0), the optical fiber transports the light to the destination, and a light detector transforms the light into an electrical signal.

The main advantages of optical fiber are very high bandwidth (megabits per second and gigabits per second), information security, immunity to electromagnetic interference, lightweight construction, and long-distance operation without signal regeneration. As a result, optical fiber is superior for bandwidth-demanding applications and protocols, operation in classified areas and between buildings, and installation in airplanes and ships. Most municipalities have optical fiber installed along most streets, and it is possible (especially for city governments) and advantageous to use this optical fiber for connecting WLANs in different buildings.

Tip

Use optical fiber to connect hubs and switches and provide connections between buildings. This will be more expensive than using twisted-pair wiring, but benefits such as higher data rates and less possibility of interference on inter-building links generally outweigh the higher cost.

Power over Ethernet

Power over Ethernet (PoE) avoids the need for an electrical outlet (or electrical extension cord) for powering access points and other system components. Figure 3-19 depicts several PoE configuration options. A PoE solution only requires technicians to deploy a single Ethernet cable to the access point for supplying both power and data. The most common PoE in use today is based on the IEEE 802.3af standard (ratified in 2003), which specifies up to 15.4 watts of power. This is generally enough to support the operation of a wireless access point, but additional power equipment may be necessary to support access points operating both 2.4-GHz and 5-GHz radios simultaneously. The newer 802.3at version of PoE (ratified in 2009) provides up to 25 watts of power and can easily support dual radios, but 802.3at is less commonly available in existing switches installed in organizations. With PoE, power sourcing protocols automatically detect the presence of an appropriate "powered device" (for example, an access point) and inject current into the cable. An access point using PoE can operate solely from the power it receives through the data cable.

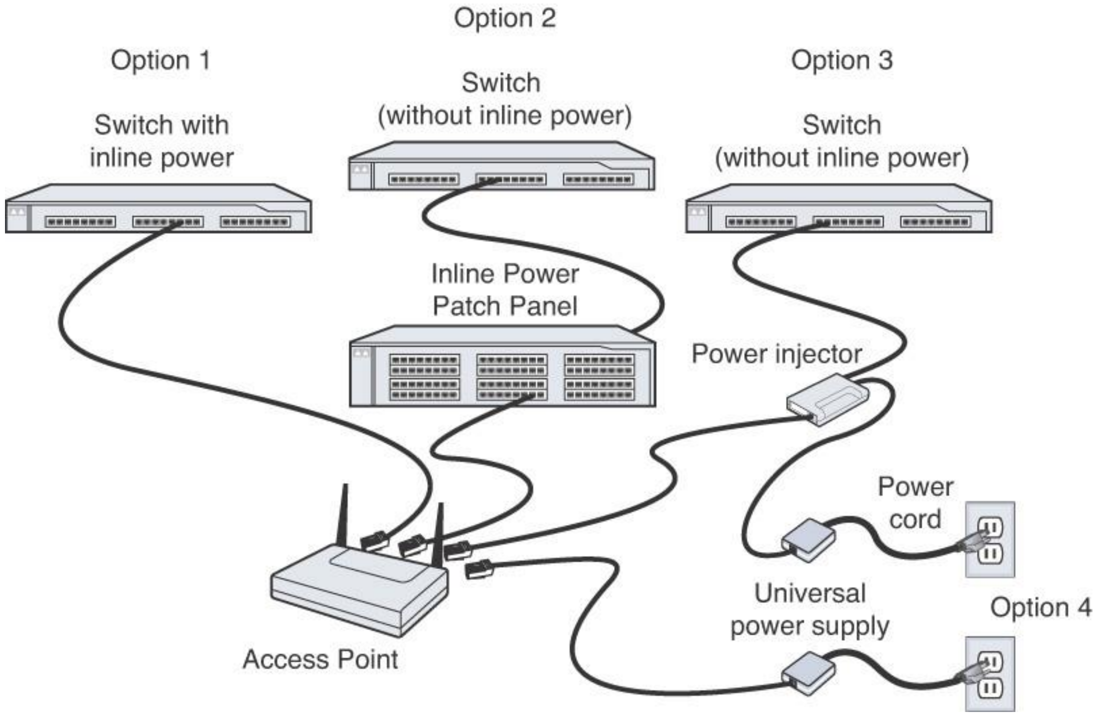


Figure 3-19 *Several Options Exist for Supporting Electrical Power to Access Points over Cabling*

PoE solutions have the following benefits as a result of not needing AC power cords:

- **Cost savings:** PoE significantly reduces the need for electricians to install conduit, electrical wiring, and outlets throughout a facility.

In larger installations, these items can be relatively expensive. Consider an installation of 50 or more access points. This requires lots of conduits, outlet boxes, and electrical wiring, as well as the time of a qualified electrician. The low costs of deploying PoE compared to traditional electrical circuits lead to worthwhile returns on investment.

- **Flexible access point locations:** With PoE, a WLAN designer has greater freedom to locate access points. You do not need to depend on only locations within short distances from AC outlets. The independence from electrical outlets also makes it easier to relocate access points in the future, if needed, to fine-tune RF coverage or increase capacity. Thus, PoE enables companies to more easily maximize the performance of a WLAN.
- **Higher reliability:** Systems with fewer wires tend to be more reliable. With WLANs not using PoE, cleaning people may unplug an access point to use its AC outlet to power vacuum and buffing equipment. Electricians rewiring electrical circuits could inadvertently cut power to an access point. PoE eliminates the possibility of such situations disrupting the operation of the network.
- **Enhanced operational support:** Many PoE devices implement Simple Network Management Protocol (SNMP), which enables support staff to remotely manage the electrical power supplied to the access points. For example, support staff can disable a PoE-enabled access point by shutting off its power after detecting a security breach. The temporary disabling of the access point can protect against an intruder continuing to access corporate systems. Other SNMP-based features enable the monitoring of the condition and consumption of power, which enhances the ability to ensure smooth and efficient network operations.
- **Simpler international development:** For manufacturers, PoE offers the benefit of the vendor not needing to provide different power cords for various countries. This not only helps keep the cost of access points down, it means installers need to worry about one less piece of equipment. Standards for PoE are still under development within the Institute of Electrical and Electronics Engineers (IEEE).

Many vendors incorporate inline PoE into their enterprise-class access point solutions; you seldom find PoE in inexpensive home networking products. This is the most basic type of PoE system, connecting only one access point at a time to a power source. This is done through a PoE injector, which fits between the source signal (modem, switch, and so on) and the access point via Category 5 or higher cable. The injector connects to a power outlet through a regular electrical cord. For optimum benefits, you can plan the placement of the injector near a power outlet, such as within the communications room near the switch.

The injector receives current from the power outlet and sends it through the Cat5 cable to the access point. Think of this configuration as a T, with the injector at the intersection, the source signal and access point at either side of the top line, and the power outlet at the bottom point.

Inline PoE devices are best for small office applications. Because there are very few access points (or even just one) in these applications, the costs for the injectors are less than the cost of purchasing a more elaborate PoE hub. In some cases, smaller installations will not even benefit from PoE because you can generally locate the access point close enough to an electrical outlet to use a traditional (old-fashioned) power cord.

Another way to implement PoE is to install a “power hub” between the source signal and the access points. This implementation follows the same concept as the inline PoE system, except that the hub feasibly supports multiple access points rather than just one. Multiple Ethernet cables run from the switch into the power hub, which connects directly to a power outlet. Multiple power-infused Ethernet cables run from the other side of the hub to various access points.

Using PoE hubs is a good approach when dealing with a large-scale installation that has existing switches, such as adding a WLAN to an existing wired Ethernet network. PoE hubs give an installer the ability to run power to multiple access points while using only one power outlet, saving time and preventing the huge headache caused by dealing with too many wires (and electricians). PoE hubs can each usually support up to 12 access points.

The most convenient way to implement PoE is to integrate it into a switch. This eliminates the need to buy extra equipment, making it most cost-effective to deploy a WLAN. The switch itself connects to a power outlet, and each port includes PoE capability integrated within the switch. The access points connect directly to the PoE-based switch ports to receive both electrical power and data over the Cat5 cable.

Integrated PoE is an optimum solution for providing electrical power to access points. It is definitely the approach to use when installing a new, large-scale network. Unfortunately, most large companies already have an existing wired Ethernet network, and replacing the existing switches is impractical and expensive. If a company is just starting up or replacing its existing wired backbone, however, integrated PoE is the ideal approach.

Application Connectivity Software

The traditional components of a wireless network (for example, radio cards and access points) provide a path for data to flow between the end-user device and a wired network that has connectivity to the host or server. To communicate effectively, wireless systems must also include connectivity between the end user and the application software and system databases. The following sections describe the primary methods for providing wireless application connectivity.

Terminal Emulation

Terminal emulation software makes an end-user device appear as a terminal to application software running on a host-based operating system, such as UNIX and AS/400. For example, Virtual Terminal (VT) emulation software interfaces with an application running on a UNIX host. Likewise, 5250 emulation software interfaces with an application running on an IBM AS/400. Terminal emulation software on wireless appliances generally communicates with the host using Telnet over TCP/IP protocols. After a connection is made with the host, the application software residing on the host can send display information (such as login prompts, menus, and data) to the appliance, and keyboard strokes will be sent to the application. Thus, the software on the host provides all application functionality.

A Case for Terminal Emulation

A police station in Florida was losing track of evidence that it acquired through the investigation of crimes. This had become a big problem because when the court needed the evidence, police officials could not find the evidence in a timely manner. This often delayed trial proceedings. As a result, the police chief decided to implement an asset-tracking system to manage the items and their specific locations. This system, based on the use of bar codes and handheld scanning equipment, needed a wireless network to support mobility when performing asset-management functions (such as picking and inventory) in the relatively large room that contained the evidence.

Because no IS staff members were available to do the project, the police chief outsourced the complete system implementation to a reliable system integrator. After careful analysis of functionality requirements and the existing system, the integrator developed a design that specified the use of off-the-shelf asset-management software, two 802.11-compliant handheld scanners, an 802.11

access point, and connectivity software. The asset-management software was hosted on the existing UNIX server that supported the police station’s jail management software. The access point interfaced the wireless handheld scanners to an existing Ethernet network, providing a network connection to the UNIX server.

When dealing with the connectivity software, the integrator narrowed the choices to either terminal emulation or middleware. Direct database connectivity was not an option because there was no way to interface directly with the database. All interaction with the database was done through the application software only.

The integrator decided to use terminal emulation (VT220) for several reasons. First, there would have been no significant gain in performance by using middleware with only two wireless appliances sending data over the wireless network. The relatively small amount of data sent between appliances and the UNIX application offered very little impact to the 2-Mbps wireless network. In addition, the price for two terminal-emulation licenses for the appliances was much lower than the cost of purchasing middleware software. Also, the police station had no plans to move to a client/server system. Overall, terminal emulation was the lowest-cost form of connectivity software, based on the police station’s requirements.

Some companies implement terminal controllers that provide an efficient interface between an end-user device and the host. The terminal controller provides effective management of the wireless end-user devices while maintaining constant connections with the host. The problem with these controllers is that they generally do not support forms of connectivity other than terminal emulation. For example, they do not support interfaces to databases via open database connectivity (ODBC), as many of the newer end systems require.

Note

If a wireless appliance running terminal-emulation software does not connect to the host, be sure that the host is running TCP/IP. It is common to not implement TCP/IP software for host computers (especially mainframes) if the original implementation did not interface with a network. In these cases, you will have to install the TCP/IP software to establish communications between the appliance and the host.

Browser-Based Approaches

The explosive use of smart phones, tablets, and the Internet is prompting the rapid development of browser-based application connectivity technologies and standards for interfacing with information and applications at websites on the Internet and company intranets. A major problem with accessing the web wirelessly today, however, is that most web pages are written to display information on large desktop screens over relatively high-bandwidth physical connectivity. These pages do not work well over lower-data-rate wireless connections and small handheld device screens. In addition to solving these performance issues, the wireless Internet revolution is fueling the need for interoperability in the way mobile devices access web-based information.

Direct Database Interfaces

Some companies develop customized versions of application software that run on an end-user device and interface directly with a database on a server via ODBC or proprietary protocols. With this configuration, the software on the end-user device generally provides all application functionality. The application software with direct database connectivity generally uses TCP/IP software as a basis for communicating with the server. Some programmers refer to this form of development as *socket programming*.

Note

The advantage of writing the appliance software to interface with ODBC is that it provides an open interface to the many databases that are ODBC compliant. This enables you to write one application that can interface with databases from different vendors.

Wireless Middleware

Wireless network middleware is an intermediate software component generally located on the wired network between the wireless end-user devices and the application or data residing on the wired network (see Figure 3-20). Middleware client software runs on the end-user device and communicates using efficient (often proprietary) wireless protocols with middleware software (controller) residing on a platform such as UNIX or Microsoft Windows 2000. The middleware controller software communicates with host applications and databases over a wired connection.

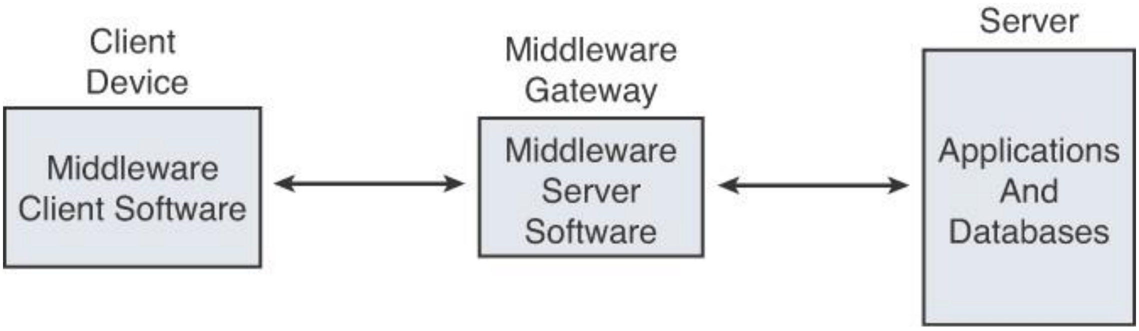

Client Device
Middleware Client Software
Middleware Gateway
Middleware Server Software
Server
Applications And Databases

Figure 3-20 *Wireless Middleware Resides Between a Client Device and an Application Server*

With the continuing need to support bandwidth-intensive applications, companies will implement wireless middleware as part of their wireless network solutions, with the goal of increasing performance. To accomplish this, middleware attempts to counter wireless network impairments, such as limited bandwidth and disruptions in network connections. Middleware enables highly efficient and reliable communications over a WLAN, while maintaining appropriate connections to application software and databases on the server/host via the more reliable wired LAN.

Traditionally, middleware suppliers could only enable a limited set of end-user devices and only interface with a specific end system. Presently, suppliers are striving to make middleware as open as possible by incorporating many different end-user devices, hosts, and servers. End-user companies generally select middleware software based on the ability to interface with their specific end systems, which tend to be IBM AS/400s, Microsoft 2000 Server machines, or UNIX hosts. In addition, end users generally want wireless middleware software capable of supporting a variety of end-user devices provided by different vendors. This minimizes limitations when adding additional end-user devices in the future.

The following vendors provide wireless middleware solutions:

- **Connect:** www.connectrf.com
- **Iona:** www.iona.com
- **NetMotion:** www.netmotionwireless.com
- **Wavelink:** www.wavelink.com

A Case for Wireless Middleware

A boat-building company in Maine decided to implement a quality-assurance system to improve the efficiency of the inspections is performs periodically. Several times throughout the process of manufacturing each boat, inspectors need to walk throughout the plant and record flaws as the boats are being assembled. The new system includes a handheld PC with an 802.11-compliant radio card that communicates to the corporate information system. For each boat, the inspector enters the boat's serial number, and then the system prompts the inspector through a series of questions that pertain to the quality of specific items of that particular boat. As the inspector answers the questions, the wireless network transports the data back to the corporate information system for viewing by construction managers.

The company's corporate information system consists of an IBM mainframe that supports most of the company's application software, servers that host databases, 3,270 terminals that interface with the mainframe applications, PCs that run client application software and interface with the databases, and an Ethernet network that ties everything together. The information that the new quality-assurance system uses is located on both the mainframe and the database servers. As a result, the corporate IS group had to pay close attention to the type of connectivity software to use to satisfy the requirements of both operating environments.

The IS group evaluated several alternatives for connectivity software: the use of terminal emulation, direct database connectivity, and middleware. Terminal emulation for the handheld PCs would interface easily with the mainframe system, but it would not provide an interface to the database servers. Likewise, direct database connectivity would interface with the database servers but not the mainframes. For this project, middleware was clearly the best alternative. The need to seamlessly interface with both the mainframe and the database server systems was imperative.

Summary

As you can see from this chapter, the implementation of a WLAN involves more than just installing radio cards and access points. The implementation might also include the use of WLAN routers, bridges, repeaters, and amplifiers. The limited connectivity you might have with a WLAN will negatively impact performance of other aspects of the system that might not be optimized for wireless applications. As a result, you need to consider the wired backbone that will interconnect the access points, software that interfaces with the servers, and IP address assignments. Attention to these elements in addition to the core WLAN components will maximize the performance and success of your WLAN implementation.