CISCO

CCNA Wireless Exam Preparation

CCNA Wireless

Official Exam Certification Guide

- ✔ Master **IUWNE 640-721** exam topics with the official study guide
- ✔ Assess your knowledge with **chapter-opening quizzes**
- ✔ Review key concepts with **Exam Preparation Tasks**
- ✔ Practice with **realistic exam** questions on the CD-ROM

ciscopress.com

Brandon James Carroll

CCNA Wireless Official Exam Certification Guide

Brandon James Carroll

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

Printed in the United States of America

First Printing October 2008

Library of Congress Cataloging-in-Publication Data:

Carroll, Brandon.
CCNA wireless official exam certification guide / Brandon James Carroll.
p. cm.
ISBN 978-1-58720-211-7 (hbk. : CD-ROM)
1. Wireless LANs--Examinations--Study guides. 2. Electronic data processing personnel--Certification--Study guides. I. Title.
TK5105.78C37 2009
004.6'8076--dc22
2008038512

ISBN-13: 978-1-58720-211-7

ISBN-10: 1-58720-211-5

Warning and Disclaimer

This book is designed to provide information about the 640-721 Implementing Cisco Unified Wireless Networking Essentials (IUWNE) certification exam. 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

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

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
1-800-382-3419
corpsales@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 email 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

Executive Editor: Brett Bartow

Cisco Representative: Anthony Wolfenden

Managing Editor: Patrick Kanouse

Cisco Press Program Manager: Jeff Brady

Senior Development Editor: Christopher Cleveland

Copy Editors: Karen A. Gill, Gayle Johnson

Project Editor: Mandie Frank

Technical Editors: Bobby Corcoran, Robert Marg

Editorial Assistant: Vanessa Evans

Proofreader: Sheri Cain, Water Crest Publishing, Inc.

Book and Cover Designer: Louisa Adair

Indexer: Tim Wright

Composition: Mark Shirar

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.**

Foreword

CCNA Wireless Official Exam Certification Guide is an excellent self-study resource for the Cisco IUWNE (640-721) exam. Passing the IUWNE exam validates the knowledge and skills required to successfully secure Cisco network devices.

Gaining certification in Cisco technology is key to the continuing educational development of today's networking professional. Through certification programs, Cisco validates the skills and expertise required to effectively manage the modern enterprise network.

Cisco Press exam certification guides and preparation materials offer exceptional—and flexible—access to the knowledge and information required to stay current in your field of expertise or to gain new skills. Whether used as a supplement to more traditional training or as a primary source of learning, these materials offer users the information and knowledge validation required to gain new understanding and proficiencies.

Developed in conjunction with the Cisco certifications and training team, Cisco Press books are the only self-study books authorized by Cisco, and they offer students a series of exam practice tools and resource materials to help ensure that learners fully grasp the concepts and information presented.

Additional authorized Cisco instructor-led courses, e-learning, labs, and simulations are available exclusively from Cisco Learning Solutions Partners worldwide. To learn more, visit http://www.cisco.com/go/training.

I hope that you find these materials to be an enriching and useful part of your exam preparation.

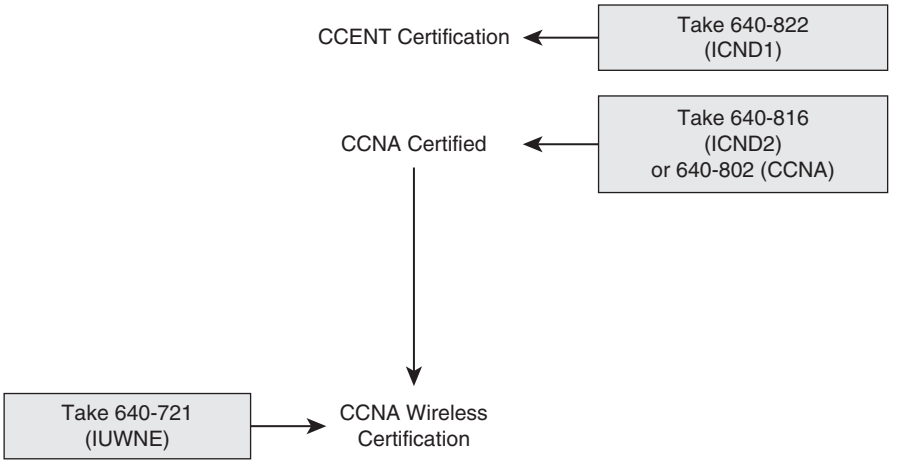
Erik Ullanderson
Manager, Global Certifications
Learning@Cisco
May 2008

Introduction

Welcome to the world of Cisco Certified Network Associate (CCNA) Wireless! As technology continues to evolve, wireless technologies are finding their way to the forefront. This clearly indicates the progression from a fixed wired type of connectivity to a more fluid, mobile workforce that can work when, where, and how they want. Regardless of your background, one of the primary goals of the new CCNA Wireless certification is to introduce you to the Cisco Unified Wireless Network (CUWN).

In June 2008, Cisco announced new CCNA specialties, including CCNA Security, CCNA Wireless, and CCNA Voice. These certifications, released 10 years after the initial CCNA, represent the growth of Cisco into new and emerging industries. Certification candidates can now specialize into specific areas of study. Figure I-1 shows the basic organization of the certifications and exams used to achieve your CCNA Wireless certification.

Figure I-1 *Cisco Certifications and CCNA Wireless Certification Path*



As you can see from the figure, a traditional CCNA certification is a prerequisite before you venture into the CCNA Wireless certification.

Goals and Methods

The most important and somewhat obvious goal of this book is to help you pass the Implementing Cisco Unified Wireless Networking Essentials (IUWNE) exam (640-721). In fact, if the primary objective of this book were different, the book title would be misleading; however, the methods used in this book to help you pass the IUWNE exam are designed to also make you much more knowledgeable about how to do your job.

This book uses several key methodologies to help you discover the exam topics that you need to review in more depth so that you can fully understand and remember those

details and prove to yourself that you have retained your knowledge of those topics. This book does not try to help you pass by memorization but helps you truly learn and understand the topics. The CCNA Wireless exam is the foundation for Cisco professional certifications to come, and it would be a disservice to you if this book did not help you truly learn the material. Therefore, this book will help you pass the CCNA Wireless exam by using the following methods:

- Helping you discover which test topics you have not mastered
- Providing explanations and information to fill in your knowledge gaps
- Supplying exercises and scenarios that enhance your ability to recall and deduce the answers to test questions
- Providing practice exercises on the topics and the testing process via test questions on the CD

In addition, this book uses quite a different style from typical certification-preparation books. The newer Cisco certification exams have adopted a style of testing that essentially says, "If you do not know how to do it, you will not pass this exam." This means that most of the questions on the certification exam require you to deduce the answer through reasoning or configuration rather than just memorization of facts, figures, or syntax from a book. To accommodate this newer testing style, I have written this book as a "real-world" explanation of Cisco wireless topics. Whenever possible, key concepts are explained using real-world examples rather than showing tables full of syntax options and explanations, which are freely available at Cisco.com. As you read through this book, you will definitely get a feeling of, "This is how I can *do* this" rather than, "There is the general syntax I need to memorize," which is exactly what you need for the newer Cisco exams.

Who Should Read This Book?

This book is designed to provide a twofold purpose. The primary purpose is to tremendously increase your chances of passing the CCNA Wireless certification exam. The secondary purpose is to provide the information necessary to deploy a CUWN and a Cisco Mobility Express (CME) network as part of the Smart Business Communications System (SBCS). The new Cisco exam approach provides an avenue to write the book with both a real-world and certification-study approach at the same time. As you read through this book and study the configuration examples and exam tips, you will truly understand how you can deploy a wireless network, while at the same time feel equipped to pass the CCNA Wireless certification exam.

Strategies for Exam Preparation

Strategies for exam preparation will vary depending on your existing skills, knowledge, and equipment available. Of course, the ideal exam preparation would consist of building a small wireless lab with a 2106 wireless LAN controller and an 1131AP, as well as a Cisco Mobility Express (CME) 526 controller and 521 AP. You would also need a switch

and a few wireless clients so that you could work through configurations as you read through this book. However, not everyone has access to this equipment, so the next best step you can take is to read through the chapters in this book, jotting notes down with key concepts or configurations on a separate notepad. Each chapter begins with a "Do I Know This Already?" quiz designed to give you a good idea of the chapter content. In some cases, you might already know most of or all the information covered in a given chapter.

After you have read this book, look at the current exam objectives for the CCNA Wireless exam listed on the Cisco website (http://www.cisco.com/certification). If you see areas shown in the certification exam outline that you would still like to study, find those sections in the book and review them. When you feel confident in your skills, attempt the practice exam included on the book CD. As you work through the practice exam, note the areas where you lack confidence, and review those concepts or configurations in the book. After you have reviewed the areas, work through the practice exam a second time and rate your skills. Keep in mind that the more you work through the practice exam, the more familiar the questions will become and the less accurate the practice exam will measure your skills. After you have worked through the practice exam a second time and feel confident with your skills, schedule the real IUWNE (640-721) exam through VUE (www.vue.com). You should typically take the exam within a week from when you consider yourself ready to take it so the information is fresh in your mind.

Cisco exams are difficult. Even if you have a solid grasp of the information, many other factors play into the testing environment (stress, time constraints, and so on). If you pass the exam on the first attempt, fantastic! If not, know that this is happens to many people. The next time you attempt the exam, you have a major advantage: You have experienced the exam firsthand. Although future exams might have different questions, the topics and general "feel" of the exam will remain the same. Take some time to study areas from the book where you felt weak on the exam. You must wait a certain period between attempts, so use that time to make yourself more prepared in the areas in which you scored low.

640-721 IUWNE Exam Topics

Table I-1 lists the exam topics for the 640-721 IUWNE exam. This table also lists the book parts where each exam topic is covered.

Table I-1 *Exam Topics for 640-721 IUWNE Exam*

Book Part(s) Where Topic Is Covered	Exam Topic
Describe WLAN fundamentals	
Part I	Describe basics of spread spectrum technology (modulation, DSSS, OFDM, MIMO, Channels reuse and overlap, Rate-shifting, CSMA/CA)

Table I-1 *Exam Topics for 640-721 IUWNE Exam (continued)*

Book Part(s) Where Topic Is Covered	Exam Topic
Part I	Describe the impact of various wireless technologies (Bluetooth, WiMAX, ZigBee, cordless phone)
Part I	Describe wireless regulatory bodies, standards and certifications (FCC, ETSI, 802.11a/b/g/n, Wi-Fi Alliance)
Part I	Describe WLAN RF principles (antenna types, RF gain/loss, EIRP, refraction, reflection, etc.)
Part I	Describe networking technologies used in wireless (SSID —> WLAN_ID —> Interface — >VLAN, 802.1Q trunking)
Part I	Describe wireless topologies (IBSS, BSS, ESS, Point-to-Point, Point-to-Multipoint, basic Mesh, bridging)
Part III	Describe 802.11 authentication and encryption methods (Open, Shared, 802.1X, EAP, TKIP, AES)
Part I	Describe frame types (management, control, data)
Install a basic Cisco wireless LAN	
Part II	Describe the basics of the Cisco Unified Wireless Network architecture (Split MAC, LWAPP, stand-alone AP versus controller-based AP, specific hardware examples)
Part II	Describe the Cisco Mobility Express Wireless architecture (Smart Business Communication System — SBCS, Cisco Config Agent — CCA, 526WLC, 521AP - stand-alone and controller-based)
Part II	Describe the modes of controller-based AP deployment (local, monitor, H-REAP, sniffer, rogue detector, bridge)
Part II	Describe controller-based AP discovery and association (OTAP, DHCP, DNS, Master Controller, Primary, Secondary, Tertiary, n+1 redundancy)
Part II	Describe roaming (Layer 2 and Layer 3, intra-controller and inter-controller, mobility groups)
Part II	Configure a WLAN controller and access points, WLC: ports, interfaces, WLANs, NTP, CLI and Web UI, CLI wizard, LAG, AP: Channel, Power
Part II	Configure the basics of a stand-alone access point (no lab) (Express setup, basic security)
Part II	Describe RRM

Table I-1 *Exam Topics for 640-721 IUWNE Exam (continued)*

Book Part(s) Where Topic Is Covered	Exam Topic
Install Wireless Clients	
Part II	Describe client OS WLAN configuration (Windows, Apple, and Linux.)
Part II	Install Cisco ADU
Part II	Describe basic CSSC
Part II	Describe CCX versions 1 through 5
Implement basic WLAN Security	
Part III	Describe the general framework of wireless security and security components (authentication, encryption, MFP, IPS)
Part III	Describe and configure authentication methods (Guest, PSK, 802.1X, WPA/WPA2 with EAP- TLS, EAP-FAST, PEAP, LEAP)
Part III	Describe and configure encryption methods (WPA/WPA2 with TKIP, AES)
Part III	Describe and configure the different sources of authentication (PSK, EAP-local or -external, RADIUS)
Operate basic WCS	
Part III	Describe key features of WCS and Navigator (versions and licensing)
Part III	Install/upgrade WCS and configure basic administration parameters (ports, O/S version, strong passwords, service vs. application)
Part III	Configure controllers and APs (using the Configuration tab, not templates)
Part III	Configure and use maps in the WCS (add campus, building, floor, maps, position AP)
Part III	Use the WCS monitor tab and alarm summary to verify the WLAN operations
Conduct basic WLAN Maintenance and Troubleshooting	
Part III	Identify basic WLAN troubleshooting methods for controllers, access points, and clients
Part III	Describe basic RF deployment considerations related to site survey design of data or VoWLAN applications, Common RF interference sources such as devices, building material, AP location, basic RF site survey design related to channel reuse, signal strength, cell overlap

Table I-1 *Exam Topics for 640-721 IUWNE Exam (continued)*

Book Part(s) Where Topic Is Covered	Exam Topic
Part III	Describe the use of WLC show, debug and logging
Part III	Describe the use of the WCS client troubleshooting tool
Part III	Transfer WLC config and O/S using maintenance tools and commands
Part III	Describe and differentiate WLC WLAN management access methods (console port, CLI, telnet, ssh, http, https, wired versus wireless management)

How This Book Is Organized

Although you can read this book cover to cover, it is designed to be flexible and allow you to easily move between chapters and sections of chapters to cover just the material that you need more work with. If you do intend to read all the chapters, the order in the book is an excellent sequence to use.

Part I, "Wireless LAN Fundamentals," consists of Chapters 1 through 9, which cover the following topics:

- **Chapter 1, "Introduction to Wireless Networking Concepts":** This chapter discusses the basics of wireless networking along with some of the challenges you may face. It is intended to be an introductory chapter to what you will be covering in chapters to come.
- **Chapter 2, "Standards Bodies":** This chapter focuses primarily on the standards bodies involved in wireless technology.
- **Chapter 3, "WLAN RF Principles":** This chapter discusses WLAN transmissions along with some of the influences on WLAN transmissions. You will also learn how to determine your signal strength and determine what may be influencing your wireless deployment.
- **Chapter 4, "WLAN Technologies and Topologies":** This chapter covers the various wireless topologies that you may come across, from Wireless Personal Area Networks (WPAN) to wireless LANs (WLANs). It also offers a further look at 802.11 topologies, including Ad-hoc mode and Infrastructure mode. In addition, you get a look at roaming and some vendor-specific topologies.
- **Chapter 5, "Antennae Communications":** This chapter focuses on antennas. It covers everything from how antennas work to how they are regulated. It even discusses the different types of antennas that Cisco offers.
- **Chapter 6, "Overview of the 802.11 WLAN Protocols":** This chapter examines each of the 802.11 protocols, including 802.11a, 802.11b, 802.11g, and even 802.11n.

- **Chapter 7, "Wireless Traffic Flow and AP Discovery":** This chapter discusses how traffic flows in a wireless network and shows you the various headers and communications. You will also learn how a client discovers an AP.
- **Chapter 8, "Additional Wireless Technologies":** This chapter takes into account the other wireless technologies that are seen in the market today, including Bluetooth, ZigBee, and WiMax.
- **Chapter 9, "Delivering Packets from the Wireless to Wired Network":** This chapter dives into the flow of a packet. You will actually experience the journey of a packet as it travels from the wireless to the wired network.

Part II, "Cisco Wireless LANs," which focuses primarily on configuration and consists of Chapters 10 through 16, covers the following topics:

- **Chapter 10, "Cisco Wireless Networks Architecture":** This chapter discusses the CUWN architecture and the devices involved.
- **Chapter 11, "Controller Discovery and Association":** In this chapter, you will learn how an AP discovers a controller and associates with it. You will also learn what steps to take to provide controller redundancy.
- **Chapter 12, "Adding Mobility with Roaming":** This chapter discusses how clients roam, how the controllers are configured to support roaming, and all that is involved in asymmetric roaming, symmetric roaming, and mobility anchors.
- **Chapter 13, "Simple Network Configuration and Monitoring with the Cisco Controller":** This chapter is your first configuration chapter that gets into allowing client access. In this chapter, you will learn how to build a WLAN with open authentication.
- **Chapter 14, "Migrating Standalone APs to LWAPP":** This chapter discusses the process of migrating a standalone AP to LWAPP using various tools.
- **Chapter 15, "Cisco Mobility Express":** This chapter discusses the Mobility Express solution for small environments. In this chapter, you will learn how to configure the Cisco 526 controller and 521 AP.
- **Chapter 16, "Wireless Clients":** This chapter discusses the Windows wireless clients with the Wireless Zero Configuration utility, the Apple Airport utility, and the Linux Network Configuration utility. You will also learn how to set up the Aironet Desktop Utility (ADU) and the Cisco Secure Services Client (CSSC). Finally, you will learn about the Cisco Compatible Extensions Program (CCX).

Part III, "WLAN Maintenance and Administration," which consists of Chapters 17 through 20, covers the following topics:

- **Chapter 17, "Securing the Wireless Network":** This chapter discusses the various methods of securing wireless networks. This chapter covers the many EAP methods, 802,.1X, Wired Equivalent Privacy (WEP), and Wi-Fi Protected Access (WPA)/WPA2.

- **Chapter 18, "Enterprise Wireless Management with the WCS and the Location Appliance":** This chapter introduces the Wireless Control System (WCS) that can be used to manage large deployments with many controllers.
- **Chapter 19, "Maintaining Wireless Networks":** This chapter discusses the management side of things. Here you learn how to perform maintenance tasks, including upgrades.
- **Chapter 20, "Troubleshooting Wireless Networks":** This chapter discusses troubleshooting techniques for wireless networks using the various tools that are available. You will learn to use the command-line interface (CLI) of the controller as well as the WCS.

In addition to the 20 main chapters, this book includes tools to help you verify that you are prepared to take the exam. Chapter 21, "Final Preparation," includes guidelines that you can follow in the final days before the exam. Appendix A, "Answers to the 'Do I Know This Already?' Quizzes," will help you verify your knowledge based on the self-assessment quizzes at the beginning of each chapter. The Glossary helps to navigate you through the many terms associated with wireless networking. Also, the CD-ROM includes quiz questions and memory tables (refer to Appendix B and C on the CD-ROM) that you can work through to verify your knowledge of the subject matter.

This chapter covers the following subjects:

Wireless Frame Transmission: A discussion of how frames are transmitted on a wireless LAN.

Wireless Frame Headers: A look at the headers used in wireless transmissions.

Frame Types: Putting together how the frame types are used in managing and connecting to a network.

A Wireless Connection: A look at a wireless connection.

CHAPTER 7

Wireless Traffic Flow and AP Discovery

It is not likely that in your everyday activity you will be following the flow of traffic. At least the hope is that you will not have to. On occasion, however, you will need to analyze the flow of traffic in troubleshooting network issues. For this reason and just so that you have a complete understanding of what is involved in wireless transmissions, you need to understand wireless traffic flow and the process of discovering an AP. In this chapter, you will learn how a client finds an AP, associates, and sends traffic.

You should do the "Do I Know This Already?" quiz first. If you score 80 percent or higher, you may want to skip to the section "Exam Preparation Tasks." If you score below 80 percent, you should spend the time reviewing the entire chapter. Refer to Appendix A, "Answers to the 'Do I Know This Already?' Quizzes" to confirm your answers.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz helps you determine your level of knowledge of this chapter's topics before you begin. Table 7-1 details the major topics discussed in this chapter and their corresponding quiz questions.

Table 7-1 *"Do I Know This Already?" Section-to-Question Mapping*

Foundation Topics Section	Questions
Wireless Frame Transmission	1–5
Wireless Frame Headers	6–7
Frame Types	8–12

1. What are the three frame types seen in a wireless LAN? (Choose three.)

- **a.** Management
- **b.** Control
- **c.** Data
- **d.** Contention

2. What type of frame is used for acknowledging receipt of data?

   a. Control
   b. Reply
   c. Null
   d. Management

3. What frame type is used to send beacons?

   a. Control
   b. Management
   c. Informational
   d. Data

4. To determine if the medium is in use, which of the following are used? (Choose all that apply.)

   a. Clear channel assessment
   b. Carrier assessment sense
   c. Virtual channel assessment
   d. Virtual carrier sense

5. Which interframe space is used for quickly sending a frame?

   a. UIFS
   b. DIFS
   c. SIFS
   d. PIFS

6. How many MAC addresses can be present in a wireless header?

   a. 1
   b. 2
   c. 3
   d. 4

7. Which of the following is a management frame type?

   a. Probe response
   b. ACK
   c. RTS
   d. Null function

8. Beacons contain information to assist clients in accessing the network. Which of the following is *not* in a beacon?

   a. Beacon interval
   b. Capability information
   c. A reference time for the cell
   d. The WEP passphrase

9. A client that connects by hearing a beacon is said to use what type of scanning?

   a. Passive
   b. Classic
   c. Active
   d. Fast

10. A client that sends a probe request is said to use what type of scanning?

    a. Preemptive
    b. Dynamic
    c. Passive
    d. Active

11. A client that sends a deauthentication message must reauthenticate when it returns to the cell. True or false?

    a. True
    b. False

12. A client that sends a disassociation message must reauthenticate when it returns to the cell. True or false?

    a. True
    b. False

Foundation Topics

Wireless Frame Transmission

When people talk about wireless networks, they often say that they are just like wired 802.3 LANs. This is actually incorrect, aside from the fact that they use MAC addresses. Wireless LANs use the 802.11 frame structure, and you can encounter multiple types of frames. To get a better understanding, you can begin by learning the three types of wireless frames. Once you are familiar with the three types of wireless frames, you can further your knowledge by taking a deeper look at interframe spacing (IFS) and why it is necessary.

Wireless Frame Types

Wireless LANs come in three frame types:

- **Management frames:** Used for managing a user's ability to connect to another station. Management frame types include association request, association response, and reassociation request, just to name a few. (See Table 7-2 for a complete list.)
- **Control frames:** Used to help communication between stations. Examples of control frames include RTS, CTS, acknowledgments (ACKs), and power save poll (PSP).
- **Data frames:** Frames that contain data and also null-function frames.

Now that you have an idea of what frames are used, it is helpful to see how these frames are sent. For this, you need to understand a few more terms that might be new to you. Because all the terms meld together to some degree, they are explained in context throughout the next section.

Sending a Frame

Recall that wireless networks are half-duplex networks. If more than one device were to send at the same time, a collision would result. If a collision occurs, the data from both senders would be unreadable and would need to be resent. This is a waste of time and resources. To overcome this issue, wireless networks use multiple steps to access the network. Wireless LANs use carrier sense multiple access collision avoidance (CSMA/CA), which is similar to the way 802.3 LANs work. The *carrier sense* part means that a station has to determine if anyone else is sending. This is done with clear channel assessment (CCA), and what it means is that you listen. You can, however, run into an issue where two devices cannot hear each other. This is called the hidden node problem. This issue is overcome using virtual carrier sense (VCS). The medium is not considered available until both the physical and virtual carrier report that it is clear.

Each station must also observe IFS. IFS is a period that a station has to wait before it can send. Not only does IFS ensure that the medium is clear, but it ensures that frames are not sent so close together that they are misinterpreted. The types of IFS periods are as follows:

- **Short interframe space (SIFS):** For high priority traffic used for ACKs, among other things

- **Point interframe space (PIFS):** Used for medium priority traffic or when an AP is going to control the network using the point coordination function (PCF)
- **Distributed interframe space (DIFS):** Used for data frames and is the normal spacing between frames

Each of these has a specific purpose as defined by the IEEE.

SIFS is used when you must send a frame quickly. For example, when a data frame is sent and must be acknowledged (ACK), the ACK should be sent before another station sends other data. Data frames use DIFS. The time value of DIFS is longer than SIFS, so the SIFS would preempt DIFS because it has a higher priority.

Figure 7-1 illustrates the transmission of a frame. In the figure, Station A wants to send a frame. As the process goes, both the physical and virtual carrier need to be free. This means the client has to listen. To listen, the client chooses a random number and begins a countdown process, called a *backoff timer*. The speed at which the countdown occurs is called *slot time. 802.11b uses long slot time, with slots 20 microseconds long, while 802.11a and g use short slot time, with slots that are 9 microseconds long*.

Key Topic

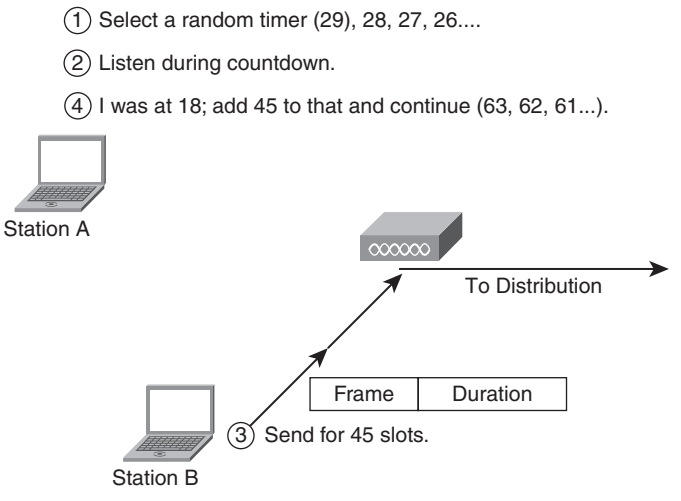


Figure 7-1 *Sending a Frame: Part 1*

It works like this:

1. Station A selects the random timer value of 29.
2. Station A starts counting at 29, 28, 27, 26, and so on. While Station A is counting down, it is also listening for whether anyone else is sending a frame.
3. When the timer is at 18, Station B sends a frame, having a duration value in the header of 45.

4. The duration of 45 that is in the header of the frame sent by Station B is called a *network allocation vector (NAV)* and is a reservation of the medium that includes the amount of time to send its frame, wait for the SIFS, and then receive an ACK from the AP.
5. Station A adds 45 to the 18 that is left and continues counting down, 63, 62, 61, and so on. The total time that Station A waits before sending is called the *contention window*.
6. When the timer on Station A reaches 0 it listens to the medium. If the medium is still clear, it can send its frame as illustrated in Figure 7-2.

If Station A sends but fails, it resets the backoff timer to a new random number and counts down again. The backoff timer gets larger as the frames fail in transmission. For example, the initial timer can be any number between 0 and 31. After the first failure, it jumps to any number between 0 and 127. It doubles for the next failure, then again, then again.

This entire process is known as the *distributed coordination function* (DCF). This simply means that each station is responsible for coordinating the sending of its data. The alternative to DCF is *point coordination function (PCF)*, which means the AP is responsible for coordination of data transmission.

Key Topic

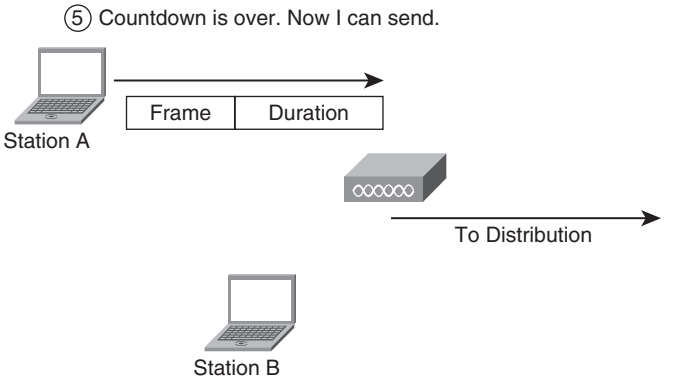


Figure 7-2 *Sending a Frame: Part 2*

If the frame is successful, an ACK must be sent. The ACK uses the SIFS timer value to make sure it is sent quickly. Some amount of silence between frames is natural. The SIFS is the shortest period of silence. The NAV reserves this time. A normal silence time is the DIFS. Again, the ACK uses SIFS because you want it to be sent immediately. The station that sends the ACK waits for the SIFS and then ACKs with the duration of 0. This is how the end of the transmission is indicated.

Wireless Frame Headers

Figure 7-3 shows a wireless frame. Each of the fields has been expanded so you can see it more clearly. It is beneficial to understand these fields and how they play a part in the sending and receiving of wireless frames.

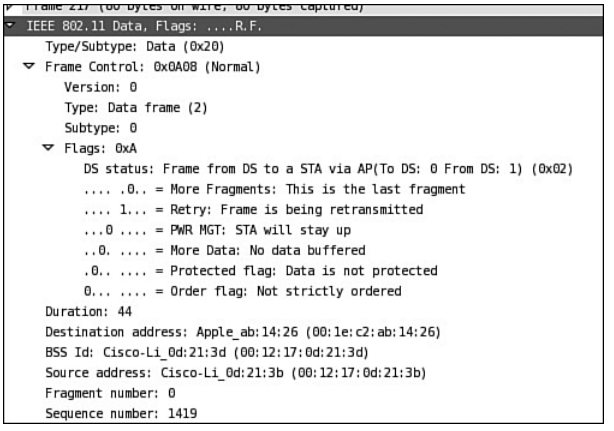


Figure 7-3 *Wireless Frame Capture 1*

As you can see from the capture, a preamble is present, denoted with the Type/Subtype label, followed by a Frame Control field. The preamble can be anywhere from 76 to 156 bytes. The Frame Control field is 2 bytes. It tells what type of frame it is. In this case, it is a data frame.

The Flags field indicates that the frame is traveling *from* the DS (the distribution system, or the wired network), not toward the DS. This is represented with a single byte. In the figure, this is a frame that is coming back to the client.

Following the Flags field is a Duration field. The Duration field indicates how long the medium is reserved while this frame is being sent and includes time for an ACK to be sent in reply. The idea behind this process is to prevent collisions.

A wireless frame can have up to three MAC addresses following the Duration field. This is a total of 18 bytes. In the figure, you can see the following:

- Destination MAC address
- BSS ID, which is also a MAC address
- Source MAC address

The source address (SA) is the station that sent the frame. The transmitter address (TA) is the address of the station that is emitting the frame; in Figure 7-3, a TA is not shown. In some scenarios, a TA might vary from an SA. For example, if a wireless frame is relayed through a repeater, the TA would be the radio of the repeater, and the SA would be the sending device. The destination address (DA) is the final destination of the frame; in this case, it is the wireless client.

The Sequence Control field (2 bytes) indicates whether the frame is a fragment. Again, in Figure 7-3, the Sequence Control field is indicated with *Fragment Number* and shows that this is number 0, or the last fragment. This leads to an interesting topic—fragmentation. When and why would you fragment on a wireless network? The answer is that a wireless frame is, by default, 2346 bytes long. Considering that the frame is going to move to or from an Ethernet distribution that has a maximum transmission unit (MTU) of 1500 bytes and can see frames as big as 1518 bytes or slightly larger (depending on the trunking used), the frames on the wireless side are too big and need to be chopped up.

Optionally, you can see a fourth MAC address, a receiving address (RA), which is the address of the *direct* station that this frame is sent to; however, this is not seen in the figure (in the figure the DA address has already fulfilled this function, so the RA address was not needed). The frame could be relayed through a wireless bridge or repeater. This additional address adds six more bytes.

Finally, the frame body follows (not seen in the figure). It can be up to 2306 bytes and references only two MAC addresses, just like any other L2 frame. The frame body is encapsulated inside the last header shown in the figure.

In addition, you might see a 4-byte frame check sequence (FCS) following the L2 frame. This is common but not required.

Frame Types

For the most part, all frames are going to have the same type of header. The difference is in the body of the frame. The body is more specific and indicates what the frame is all about. Table 7-2 shows some frame types.

Table 7-2 *Frame Types Table*

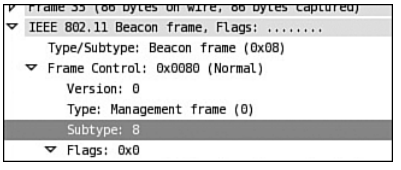
Management	Control	Data
Beacon	Request to Send (RTS)	Simple data
Probe Request	Clear to Send (CTS)	Null function
Probe Response	Acknowledgment	Data+CF-ACK
Association Request	Power-Save-Poll (PS-Poll)	Data+CF-Poll
Association Response	Contention Free End (CF-End)	Data+CF-Ack
Authentication Request	Contention Free End + Acknowledgment (CF-End +ACK)	ACK+CF-Poll
Authentication Response	CF-ACK	
Deauthentication	CF-ACK+CF-Poll	
Reassociation request		
Reassociation response		
Announcement traffic indication message (ATIM)		
Each frame type merits its own discussion to follow.		

Management Frames

Management frames, as their name indicates, are used to manage the connection. In looking at a frame capture, the Type field indicates Management, and the subtype tells what kind of management frame it is. As Table 7-2 listed, there are 11 Management frame types. There are some more-often seen frames that you should be familiar with. These frame types are discussed in the following sections.

Beacons and Probes

Figure 7-4 shows a management frame with a subtype of 8. This indicates that it is a beacon frame, which is used to help clients find the network.



Key Topic

Figure 7-4 *Management Frame Capture*

Figure 7-5 shows a sample network where the AP is sending a beacon frame.

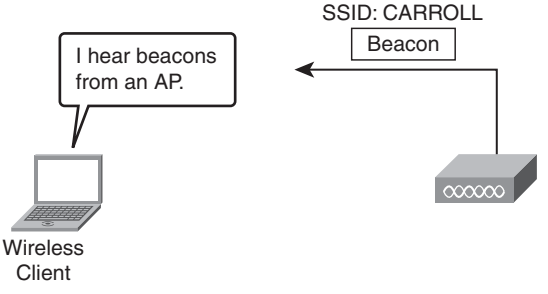


Figure 7-5 *Sample Network Using Beacon Frames*

When the client hears the beacon frame, it can learn a great deal of information about the cell. In Figure 7-6, you can see that the beacon frame includes a timestamp that gives a reference time for the cell, the beacon interval, and a field called Capability Information, which provides specifics for this cell. The Capability Information field includes information regarding power save mode, authentication, and preamble information.

A beacon frame also includes the SSIDs that the AP supports, the rates that are supported, and six fields called Parameter Set that indicate modulation methods and such.

Another field you will find is Traffic Indication Map (TIM), which indicates whether the AP is buffering traffic for clients in power-save mode.

When a client sees a beacon frame, it should be able to use that information to determine if it is able to connect to the wireless Cell. Chapter 16, "Wireless Clients," covers the

Key Topic

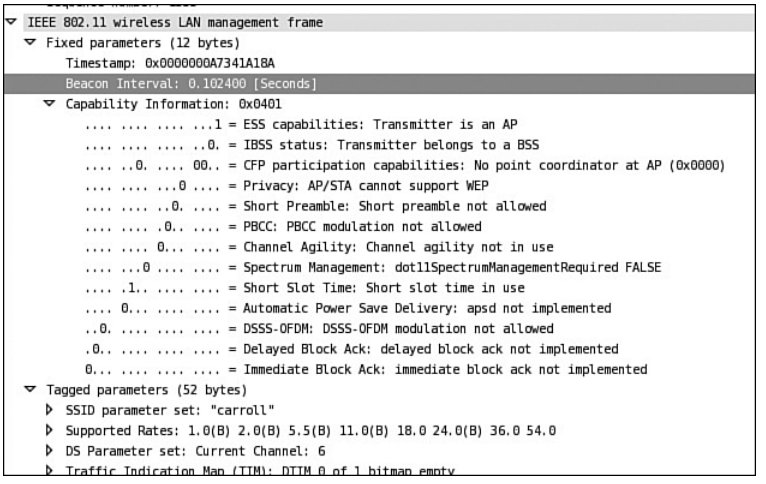


Figure 7-6 *Beacon Frame Details*

process of how a client searches channels and displays connection capability information. For now, just understand that the beacon frame allows a client to passively scan a network.

Sometimes, however, you do not want to passively scan a network. Perhaps you know exactly what SSID you want to connect to. In this situation, you can actively scan a network to determine if the SSID you are looking for is accessible. When a client actively scans a network, it uses probe request and probe response messages. Figure 7-7 shows a client actively scanning.

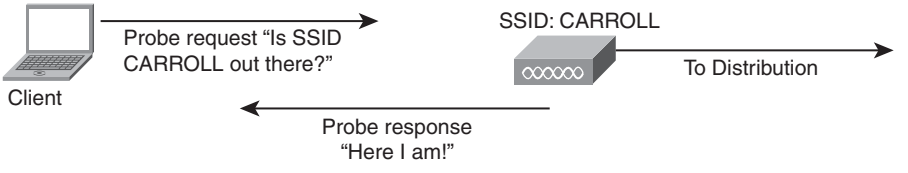


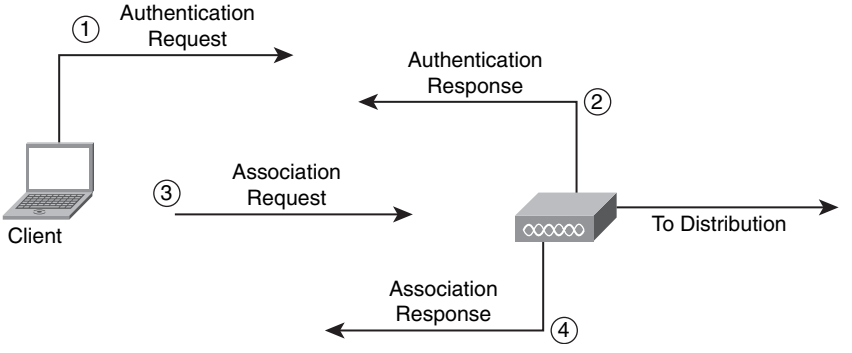
Figure 7-7 *Active Scanning*

As you can tell in the figure, the client is looking for a wireless cell with the SSID of "Carroll." This client sends a probe request and the AP, upon receiving the probe request, issues a probe response. The probe response is similar to the beacon frame, including capability information, authentication information, and so on. The difference is that a beacon frame is sent on an automated basis (every 100 ms by default) and a probe response is sent only in response to a probe request.

Connecting After a Probe or Beacon

After a client has located an AP and understands the capabilities, it tries to connect using an authentication frame. This frame has information about the algorithm used to authenticate, a number for the authentication transaction, and information on whether authentication has succeeded or failed.

One thing to note is that authentication can be *Open*, meaning that no authentication algorithm such as WEP is being used. The only reason an authentication message is used is to indicate that the client has the capability to connect. In Figure 7-8, the client is sending an authentication request, and the AP is sending an authentication response. Upon authentication, the client sends an association request, and the AP responds with an association response.



Key Topic

Figure 7-8 *Authentications and Association*

Leaving and Returning

When a client is connected to a wireless cell, either the client or the AP can leave the connection by sending a deauthentication message. The deauthentication message has information in the body as to why it is leaving. As an alternative, a client can send a disassociation message, which disassociates the client from the cell but keeps the client authenticated. The next time a client comes back to the wireless cell, it can simply send a reassociation message, and the AP would send a reassociation response—eliminating the need for authentication to reconnect to the cell.

Note: Cisco Unified Wireless networks use deauthentication messages to contain rogue APs. This concept is a little outside of this discussion but will be covered in Chapter 10, "Cisco Wireless Networks Architecture."

Control Frames

One of the most common control frames is the ACK, which helps the connection by acknowledging receipt of frames. Other control frames include the request to send (RTS) and clear to send (CTS), which were discussed in Chapter 6, "Overview of the 802.11 WLAN Protocols." The ACK, RTS, and CTS frames are used in DCF mode.

The control frames that are used in PCF mode are as follows:

- Contention Free End (CF+End)
- Contention Free End Ack (CF +end_ack_)

- CF-Ack
- CF Ack+CF Poll
- CF-Poll

These frames are also discussed in the paragraphs to follow.

When an AP takes control of a network and shifts from DCF mode (every station for itself) to PCF mode (the AP is responsible for everyone sending), the AP lets all stations know that they should stop sending by issuing a beacon frame with a duration of 32768. When this happens and everyone stops sending, there is no longer a contention for the medium, because the AP is managing it. This is called a *contention free window (CFW)*. The AP then sends poll messages to each client asking if they have anything to send. This is called a CF-Poll, as illustrated in Figure 7-9.

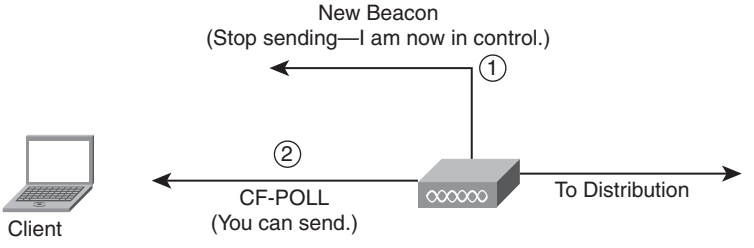


Figure 7-9 *CF-Poll in PCF Mode*

Figure 7-10 illustrates how the AP might control communication. Here, the AP has data to deliver to the client (DATA). It allows the client to send data (CF-Poll) and acknowledges receipt of the client data (CF-ACK).

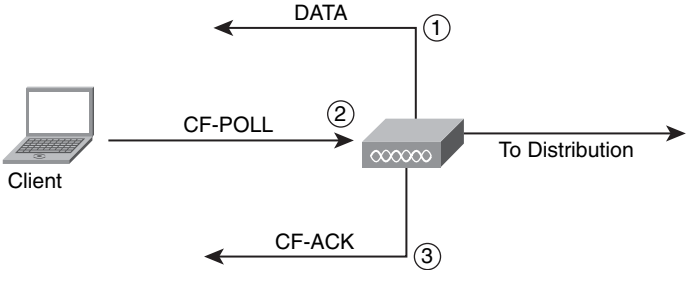


Figure 7-10 *Data + CF-Poll + CF-ACK*

Other variations exist, but from these examples you should have a decent understanding of PCF operation.

Power Save Mode and Frame Types

Another mode of operation mostly seen on laptops is called power save mode. Looking back at Table 7-2, you can see that a control frame is related to a power save (PS-Poll). In a

power save, a client notifies an AP that it is falling asleep by using a null function frame. The client wakes up after a certain period of time, during which the AP buffers any traffic for it. When the client wakes up and sees a beacon frame with the TIM listing that it has frames buffered, the client sends a PS-Poll requesting the data.

Frame Speeds

One final item to discuss before putting it together is frame speed. The AP advertises mandatory speeds at which a client must be able to operate. You can use other speeds, but they are not mandatory. For example, 24 Mbps might be mandatory, but an AP might also be capable of 54 Mbps. A client *must* support 24 Mbps but is allowed to use the best rate possible, in this example 54 Mbps. When data is sent at one rate, the ACK is always sent at 1 data rate lower.

A Wireless Connection

Using Figures 7-11 through 7-18, you can step through a simple discovery and association process.

1. The AP sends beacons every 100 milliseconds, as shown in Figure 7-11.

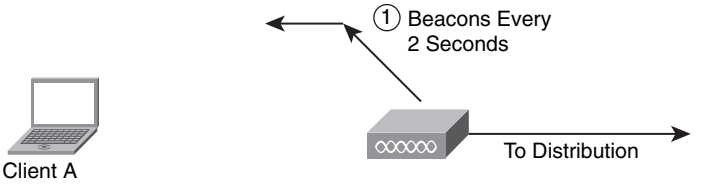


Figure 7-11 *AP Beacons*

2. Client A is passively scanning and hears the beacon. This enables the client to determine whether it can connect. You can see this in Figure 7-12.

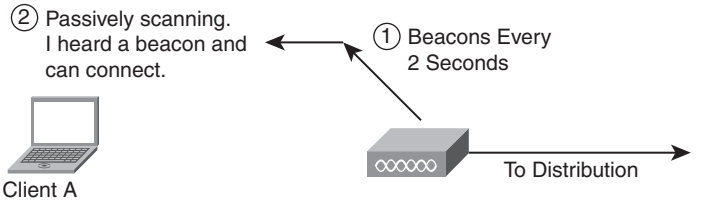


Figure 7-12 *Passive Scanning*

3. A new client (Client B) arrives. Client B is already configured to look for the AP, so instead of passive scanning, it sends a probe request for the specific SSID (see Figure 7-13).

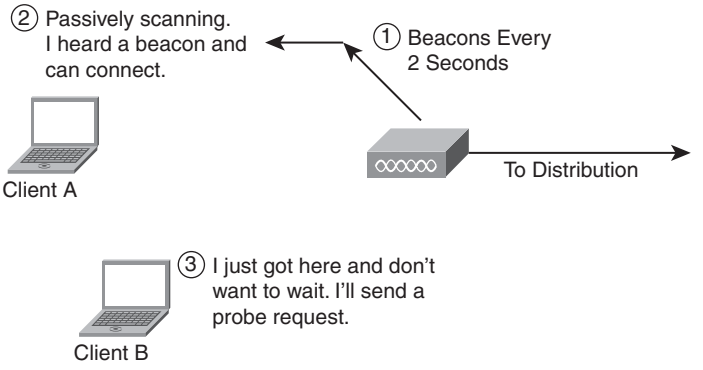


Figure 7-13 *Active Scanning Probe Request*

4. The AP sends a probe response, seen in Figure 7-14, which is similar to a beacon. This lets Client B determine if it can connect.

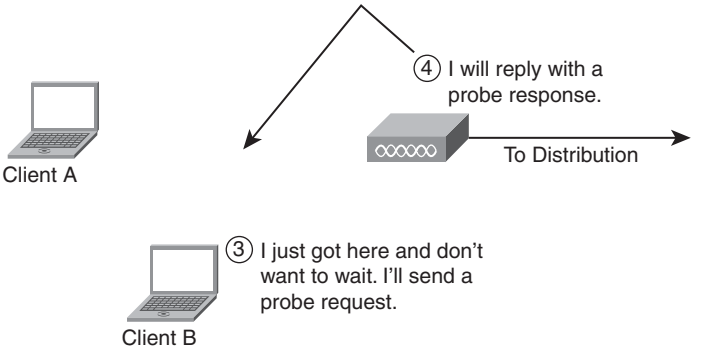


Figure 7-14 *Probe Response*

5. From this point on, the process would be the same for Client A and Client B. In Figure 7-15, Client B sends an authentication request.

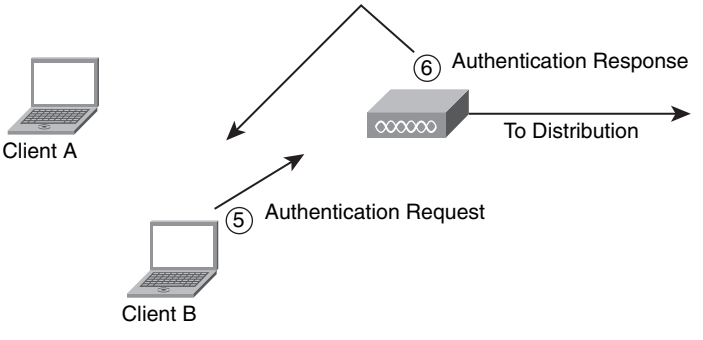


Figure 7-15 *Association Request and Response*

6. Also seen in Figure 7-15, the AP returns an authentication response to the client.
7. The client then sends an association request, as seen in Figure 7-16.

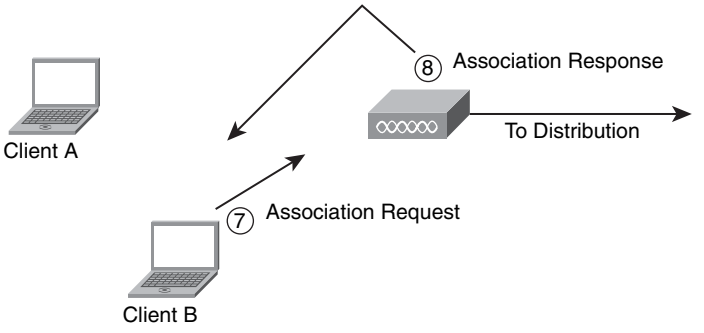


Figure 7-16 *Association Request and Response*

8. Now the AP sends an association response, also seen in Figure 7-16.
9. When the client wants to send, it uses an RTS, assuming this is a mixed b/g cell. The RTS includes the duration, as you can see in Figure 7-17.

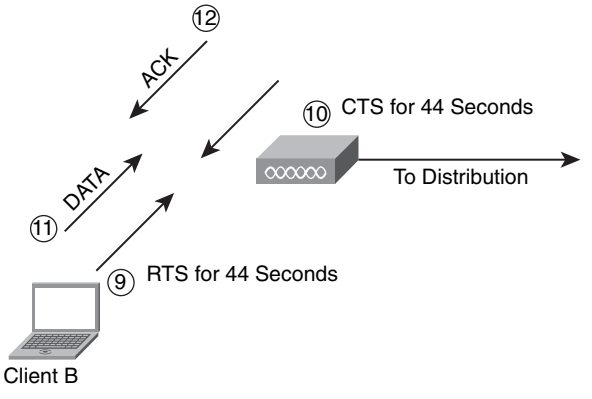


Figure 7-17 *RTS/CTS*

10. Also seen in Figure 7-17, the AP returns a CTS.
11. The client sends the data (see Figure 7-17).
12. The AP sends an ACK after each frame is received (Figure 7-17).
13. In Figure 7-18, the client sends a disassociation message.
14. The AP replies with a disassociation response (Figure 7-18).
15. The client returns and sends a reassociation message (Figure 7-18).
16. The AP responds with a reassociation response (Figure 7-18).

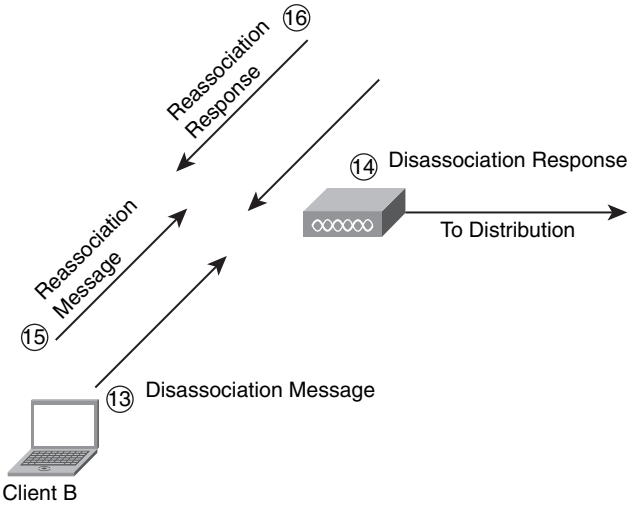


Figure 7-18 *Reassociation*

Again, this process has other variations, but this should give you a pretty good understanding of how to manage a connection.

Exam Preparation Tasks

Review All the Key Concepts

Review the most important topics from this chapter, noted with the Key Topics icon in the outer margin of the page. Table 7-3 lists a reference of these key topics and the page number where you can find each one.

Table 7-3 *Key Topics for Chapter 7*

Key Topic Item	Description	Page Number
Figure 7-1	Sending a frame: part 1	117
Figure 7-2	Sending a frame: part 2	118
Figure 7-3	Wireless frame capture	119
Table 7-2	Frame types table	120
Figure 7-4	Management frame capture	121
Figure 7-6	Beacon frame details	122
Figure 7-8	Authentication and association	123

Complete the Tables and Lists from Memory

Print a copy of Appendix B, "Memory Tables," (found on the CD) or at least the section for this chapter, and complete the tables and lists from memory. Appendix C, "Memory Tables Answer Key," also on the CD, includes completed tables and lists to check your work.

Definition of Key Terms

Define the following key terms from this chapter, and check your answers in the Glossary:

management frames, control frames, data frames, CSMA/CA, CCA, hidden node problem, virtual carrier sense, IFS, SIFS, DIFS, ACK, backoff timer, NAV, slottime, contention window, DCF, PCF, SA, RA, TA, DA, MTU, beacon, probe request, probe response, authentication request, authentication response, association request, association response, TIM, ATIM, passive scan, active scan, deauthentication message, deauthentication response, disassociation message, disassociation response, null function frame, PS-Poll

Index

NUMBERS

A

B

C

D

E

F

G - H

I

J - K - L

M

N - O

P

Q - R

S

T

U - V

W

X - Y - Z