EDITION
CWAP-402

CWAP®
Certified Wireless Analysis Professional

Official Study Guide

Certified Wireless Network Professional
cwnp®
Vendor-Neutral Enterprise
Wi-Fi Certification

Certitrek PUBLISHING

Certified Wireless Analysis Professional (CWAP®) Official Study Guide (CWAP-402)

Copyright © 2016 by CertiTrek Publishing. All rights reserved. Printed in the United States of America. Except as permitted under the United States Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a data base or retrieval system, without the prior written permission of the publisher.

All trademarks or copyrights mentioned herein are the possession of their respective owners and CertiTrek Publishing makes no claim of ownership by the mention of products that contain these marks. Trademarks include CWNP®, CWTS®, CWNA®, CWSP®, CWDP®, CWAP®, CWNE®, and CWNT®.

First printing June 2016

ISBN: 978-0-9967213-8-7

Technical Reviewer

Lee Badman

Copy Editors

CWNP Staff

Authors

Tom Carpenter

CWNP Staff

Production Supervisor

Josie Miller

Project Manager

Brad Crump

Introduction

WLANs are pervasive and problems in WLANs are nearly as common. The WLAN engineer must have troubleshooting skills and understand the operations of WLANs in order to troubleshoot them effectively. The Certified Wireless Analysis Professional (CWAP®) certification proves that you have this skillset.

Wireless troubleshooting involves knowledge of RF operations, 802.11 protocols, analysis tools (such as protocol and spectrum analyzers), and troubleshooting methodologies. All of these knowledge areas are addressed in the CWAP-402 exam, making a CWAP-certified professional an individual you can trust to analyze networks and quickly resolve any problems discovered. From performance tuning to connectivity issues, the CWAP-certified professional is prepared to tackle the job.

In order to obtain your CWAP certification, you must also possess the CWNA® certification. It is a prerequisite to be qualified for CWAP certification status. The exam objectives are listed below; however, you can learn more about the CWAP certification and its requirements by visiting the CWNP.com website and selecting Certifications > CWAP.

CWAP-402 Exam Objectives

The CWAP-402 exam is organized into four knowledge domains as follows:

- Troubleshooting Processes—5%
- 802.11 Communications—25%
- WLAN Hardware—15%
- Protocol and Spectrum Analysis—35%
- Troubleshooting Common Problems—20 %

This breakdown simply means that 5% of the questions on the exam will be in the first knowledge domain, 25% in the second, and so on. As you can see, this means that the largest pool of questions will come from the Protocol and Spectrum Analysis knowledge domain.

The following detailed objectives list should be used as your guide during exam preparation. All exam questions are written to the objectives.

CWAP-402 Objectives

1.0 Troubleshooting Processes—5%

1.1 Understand industry and vendor-recommended troubleshooting processes and implement the same to resolve common 802.11 wireless networking problems.

1.2 Apply the OSI Model to the troubleshooting processes and problem resolution methods used in 802.11 wireless networks.

1.3 Use the appropriate tools (network analysis and operating system tools) to troubleshoot specific problems including no network connectivity, slow network performance, unavailable resources, and unavailable services.

2.0 802.11 Communications—20%

2.1 Explain the 802.11 communications processes including authentication, association, security negotiation, frame transmission, and factors impacting data rates.

2.2 Understand the different WLAN architectures in use and their impact on performance and operations.

2.3 Understand and explain the 802.11 frames including general frame format, management frames, control frames, and data frames, and how they apply to WLAN analysis.

2.4 Understand and explain the 802.11 PHY header and preamble and the indications for WLAN performance and operations.

3.0 WLAN Hardware—15%

3.1 Understand client devices and operations including radios, drivers, supplicants, and implementations.

3.2 Describe and discover access point (AP) options, configurations and behaviors, including internal and external antennas, Ethernet connections, power options, and management options.

3.3 Explain the functionality of WLAN controllers and managers including protocols used, installation locations, and supported data communication options.

3.4 Describe and implement WLAN analysis hardware for protocol analysis and spectrum analysis.

3.5 Describe and analyze wired infrastructure hardware including routers and switches as well as servers and services.

4.0 Protocol and Spectrum Analysis—35%

4.1 Describe the common functionality and features of protocol analyzers.

4.2 Demonstrate the ability to install, configure, and use a protocol analyzer to capture and analyze WLAN traffic.

4.3 Demonstrate the ability to use a protocol analyzer to capture the appropriate wired traffic related to WLAN operations.

4.4 Define terminology related to spectrum analysis including SNR, duty cycle, sweep

cycles, signal strength, resolution bandwidth, and utilization.

4.5 Understand the common functions and features of a protocol analyzer as it relates to WLAN analysis.

4.6 Demonstrate the ability to install, configure, and use a PC-based spectrum analyzer to analyze RF activity in an area.

4.7 Recognize RF patterns of common devices including 802.11 devices, Bluetooth devices, microwave ovens, wireless video devices, and cordless phones.

5.0 Troubleshooting Common Problems—20%

5.1 Understand and explain common wired problems that impact the WLAN including DNS, DHCP, switch configuration, WLAN controller access, and PoE.

5.2 Demonstrate the ability to troubleshoot wired issues using protocol analyzers, operating system commands, and hardware troubleshooting.

5.3 Select the appropriate location for placement of a protocol analyzer on the wired network and use it to troubleshoot common issues including DHCP, DNS, and data communications issues.

5.3 Analyze and repair Quality of Service (QoS) issues on the wired side of the network.

5.4 Recognize and repair common WLAN issues including insufficient capacity, lack of connectivity, interference, and QoS problems.

5.5 Diagnose and repair roaming problems including dropped VoIP calls, broken connections, and lack of reconnect.

5.6 Understand and repair issues related to WLAN security including authentication, encryption, and mobile device management (MDM).

5.7 Recognize and repair common client-side problems including unstable drivers, configuration errors, incompatible supplicants, and operating system bugs and vulnerabilities.

Target Audience

As an important note, this book is written for those preparing for the CWAP certification and not as a general guide to wireless networking that also happens to include analysis. You will find, in the very first pages that this book is written to an individual who already understands wireless networking from a functional perspective. No review of basic 802.11 fundamentals is to be found here. Therefore, if you are CWNA certified, you are ready to begin exploring this book with full understanding. However, if you are not CWNA certified, you should have extensive knowledge of wireless networks before venturing further.

Acknowledgements for Content

Finally, we at CWNP would like to thank the following individuals for assisting us in the production of this resource. They provided valuable content that greatly improved the book to help CWAP students and security professional everywhere.

Author

Tom Carpenter is the CTO at CWNP and provides focus and direction for the certification exams offered. He has authored 18 books for the IT industry and more than 60 e-learning programs. Having worked in the IT industry for 25 years, he brings a wealth of background knowledge to any project. He lives in Ohio and is the proud father of Faith, Rachel, Thomas, and Sarah. Tom is a CWNE and holds many other industry certifications.

Technical Reviewer

Lee Badman provided technical review and feedback on the content of this book. As a long time wireless network professional, classroom instructor, and technical writer, his work can be seen in the networks he has designed and currently supports at dozens of sites internationally, and in the hundreds of articles he has published for several online periodicals. A number of current industry professionals have sat in his network classes as students at the private university where Lee is an adjunct faculty member. Learn more about his professional activities at wirednot.net

Table of Contents

INTRODUCTION

CWAP-402 Exam Objectives

CWAP-402 Objectives

1.0 Troubleshooting Processes—5%

2.0 802.11 Communications—20%

3.0 WLAN Hardware—15%

4.0 Protocol and Spectrum Analysis—35%

5.0 Troubleshooting Common Problems—20%

Target Audience

Acknowledgements for Content

Author

Technical Reviewer

TABLE OF CONTENTS

CHAPTER 1: TROUBLESHOOTING PROCESSES

Objectives

Troubleshooting Methodologies

Vendor Methodologies

Industry Methodologies

Troubleshooting with the OSI Model

OSI Model Review

Why Is the OSI Model Important?

Troubleshooting Layers

Matching Tools to Problems

Networking Tools

Operating System Tools

Exercise 1

(a) Read the following article on troubleshooting methodology and answer the questions below.

Microsoft's Troubleshooting Methodology

(b) Read the following article on troubleshooting methodology and answer the questions below.

Cisco's Troubleshooting Methodology

(c): Read the following article on troubleshooting methodology and answer the questions below.

HP's Troubleshooting Methodology

Answer (a)

Answer (b)

Answer (c)

CHAPTER SUMMARY

REVIEW QUESTIONS

REVIEW QUESTION ANSWERS

CHAPTER 2: 802.11 COMMUNICATIONS

OBJECTIVES

TERMINOLOGY REVIEW

Bits, Bytes, and Octets

MAC & PHY

PHY Level Information

802.11 Architecture Terms

802.11 COMMUNICATIONS

Beacon Frames

802.11 State Machine

Authentication

Channel Access using CSMA/CA and DCF

802.11e and WMM

RTS/CTS

DATA-RATE FACTORS

WLAN ARCHITECTURES

Single MAC Model (Edge, Autonomous, or Standalone)

Split MAC Model (Centralized)

Wireless Mesh

Common Wireless Architectures

EXERCISE 2

CHAPTER SUMMARY

Review Questions
Review Question Answers
CHAPTER 3: 802.11 FRAMES
Objectives
Framing Review
Ethernet Frames
802.11 General Frame Format
Frame Control
Duration/ID
Address 1, 2, 3, and 4
Sequence Control
QoS Control
HT Control
Frame Body
FCS
802.11 Frame Types
Management Frames
Control Frames
Data Frames
PCF Frames
Important 802.11 Frames
Beacon Frames
Probe Request and Probe Response Frames
Authentication and Deauthentication Frames
Association and Disassociation Frames
Reassociation Request and Response Frames
Request to Send (RTS) and Clear to Send (CTS) Frames
Acknowledgement (ACK) Frames
Null Data and PS-Poll Frames
Beacon Frame Timing
Security Communications
WPA and WPA2 Personal

WPA2 Enterprise
EAP Frames
RADIUS Packets
LDAP Packets
802.11 PHY
802.11 PHY Preamble
802.11 PHY (PLCP) Header
EXERCISE 3
CHAPTER SUMMARY
REVIEW QUESTIONS
REVIEW QUESTION ANSWERS
CHAPTER 4: WLAN HARDWARE
OBJECTIVES
CLIENT DEVICE TYPES AND FUNCTIONS
Device Internals
EXERCISE 4
Device Form Factors
ACCESS POINTS
Common Features
AP Configuration Processes
AP Spec Sheet
WLAN CONTROLLERS AND MANAGERS
WLAN Controller Common Features
WLAN Controller Configuration Process
WIRELESS ANALYSIS HARDWARE
Spectrum Analysis Hardware
Protocol Analysis Hardware
WIRED HARDWARE
Ethernet Switches
IP Routers
Servers and Services

Chapter Summary
Review Questions
Review Question Answers
CHAPTER 5: PROTOCOL ANALYSIS
Objectives
WLAN Analysis Hardware and Software
Protocol Analysis Hardware
Protocol Analysis Software
Protocol Analysis
Common Features
Installing and Configuring
Capturing WLAN Traffic
Analyzing WLAN Traffic
Exercise 5
Applied Analysis
Wired Traffic
Capturing Wired Traffic
Analyzing Wired Traffic
Chapter Summary
Review Questions
Review Question Answers
CHAPTER 6: SPECTRUM ANALYSIS
Objectives
Spectrum Analysis Hardware
Hardware
Software
Terminology
CWNA Terminology Review and RF Math
Additional Spectrum Analysis Terminology
Spectrum Analyzer Features
Views

Reports
Wi-Fi Integration
INSTALLING AND CONFIGURING
Install a Spectrum Analyzer
Configure a Spectrum Analyzer
PERFORMING SPECTRUM ANALYSIS
Recognizing Patterns
Locating Devices
EXERCISE 6
CHAPTER SUMMARY
REVIEW QUESTIONS
REVIEW QUESTION ANSWERS
CHAPTER 7: WIRED ISSUES
OBJECTIVES
COMMON PROBLEMS
DNS
DHCP
Switch Configuration
WLAN Controller Access
PoE
TROUBLESHOOTING ISSUES
Troubleshooting Tools
DNS Issues
DHCP Issues
WLAN Controller Issues
Switching and Routing Issues
PoE Issues
QoS Issues
Additional Wired-Side Problems
EXERCISE 7
CHAPTER SUMMARY

Review Questions
Review Question Answers
CHAPTER 8: COMMON WLAN ISSUES
Objectives
Common Issues
Insufficient Capacity
Co-Channel and Adjacent-Channel Interference
RF Noise and Noise Floor
RF Interference
Multipath
Hidden Nodes
Near-Far Problem
Weather
Troubleshooting Voice-over-WLAN (VoWLAN) Issues
QoS Configuration Problems
Security Issues
SSIDs
Default Configuration Settings
Rogue Equipment
RF Cell Sizing
SNMP Community Strings
Discovery Protocols
Remote Configuration
Client Security
Staging and Testing
Equipment Installation
Client Issues
Drivers
Adapter Limitations
Hardware Switches
Configuration Errors
Supplicant Issues

Operating System Bugs and Vulnerabilities

Modern Issues

EXERCISE 8

CHAPTER SUMMARY

REVIEW QUESTIONS

REVIEW QUESTION ANSWERS

APPENDIX A: INSTALLING WLAN ANALYSIS SOFTWARE

INSTALLING WIRESHARK

INSTALLING COMMVIEW FOR WIFI

GLOSSARY

INDEX

Chapter 1:

Troubleshooting Processes

Objectives

1.1 Understand industry and vendor recommended troubleshooting processes and implement the same to resolve common 802.11 wireless networking problems.

1.2 Apply the OSI Model to the troubleshooting processes and problem resolution methods used in 802.11 wireless networks.

1.3 Use the appropriate tools (network analysis tools and operating system tools) to troubleshoot specific problems including no network connectivity, slow network performance, unavailable resources, and unavailable services.

The Certified Wireless Analysis Professional (CWAP®) exam is focused on wireless analysis and troubleshooting within 802.11 networks. Such processes depend heavily on common techniques used in the technology sector, regardless of the system or problem being addressed. For example, troubleshooting a network performance problem relies on many of the same principles as are required when troubleshooting an application performance problem. A key element is asking the right questions. Troubleshooting methodologies help us remember to do that.

This chapter introduces troubleshooting processes that are commonly used in the networking industry, or that are recommended by specific vendors. With an understanding of these processes, you can better grasp the remaining chapters and how the knowledge they provide will help you in the troubleshooting process. I learned very early on in my IT career that processes make life easier, and I hope the information in this chapter will help you both in preparing for the CWAP exam and in real-world troubleshooting scenarios in which you find yourself.

Troubleshooting Methodologies

The networking industry, in general, has developed troubleshooting methodologies (processes and tools) to assist the wireless administrator with problem resolution. When you understand these methodologies, you can better troubleshoot a problem and ensure the proper steps have been taken as you work towards resolution. In this section, I will review the processes recommended by a few vendors and also discuss industry methods commonly used.

Vendor Methodologies

For the purposes of this study guide, I will use the troubleshooting processes recommended by both Cisco® and Microsoft as examples. They represent two of the largest software and hardware vendors in the world, and between the two of them they touch in some way nearly every network communication that occurs, and this is particularly true for Internet communications. Microsoft® is mostly a client and server vendor (with applications and hardware, as well), and Cisco is mostly a network hardware vendor (with server and client applications, as well).

<u>The Cisco Troubleshooting Process</u>

Cisco defines a specific troubleshooting model at `http://bit.ly/1Tjd3qF`. This basic model is their recommended troubleshooting process and can be applied to wired and wireless problems. In this book, the focus is primarily on wireless troubleshooting, but some wired troubleshooting must be introduced as well because the wireless network depends heavily on services that are nearly always provided by the wired network.

The Cisco troubleshooting process is as follows:

1. Define a clear problem statement with symptoms and potential causes.
2. Gather the facts to help isolate the possible causes.

3. Consider possible problems based on the facts discovered.
4. Create an action plan based on the remaining potential problems and the most likely cause.
5. Implement the action plan.
6. As changes are made, gather results.
7. Analyze the results and determine whether the problem has been resolved.
8. If the problem is not resolved, create a new action plan based on the next most likely cause and proceed with steps 5–8. Repeat until resolved or escalated.

Each of these steps is considered in detail in the pages that follow. For our purposes, a common WLAN problem will be analyzed. The scenario is simple: a user connects to the WLAN, but receives a message indicating that the connection is limited. The user cannot browse the Internet or even access local network resources. Using the Cisco process, we will analyze this connection problem.

1 - Define a clear problem statement with symptoms and potential causes.

The first step is to define a clear problem statement. A problem statement should plainly state the problem experienced by the user and any related symptoms that would be helpful in the troubleshooting process. This problem statement will become the foundation for the troubleshooting process. Without it, the wrong problem may be solved or the problem may be incompletely solved. The problem statement is essential—even if it exists only in the analyst's mind.

Many organizations have documentation systems where analysts are expected to document problem statements such as the ones discussed here. If such a system does not exist, the analysis must still go through this thinking process to ensure that she is addressing the appropriate problem. Users will often use phrases to describe a problem that the analyst can easily misinterpret. The problem statement, when created using steps 1–3 of Cisco's process, can help to remove any misunderstandings between the user and the support analyst.

At step one of this process for the scenario in question, the following problem statement (repeated in part from above) will suffice:

A user connects to the WLAN, but receives a message indicating that the connection is limited. The user cannot browse the Internet or even access local network resources. This may be caused by a misconfiguration or a network problem.

2 - Gather the facts to help isolate the possible causes.

Now that you have a problem statement, you can further clarify the details and improve on the statement. This step involves the use of open-ended questions and possibly some verification procedures.

Open-ended questions are those that cannot properly be answered with a yes or no response. For example, most questions that begin with *are, was, were, is, will, do, can,* and *may* are answered with a yes or no response. However, most questions that begin with *who, when, where, why, how,* and *what* cannot be answered with just a yes or no response.

In general, open-ended questions solicit more useful information from the user. Here are some example fact-gathering questions for our scenario:

- When did the problem begin?
- What changes have been made to the system recently, if any?
- What are you trying to do that is failing?
- How are you trying to do it?

Consider the following four answers to the preceding questions, in the same order the questions are listed:

- It started happening yesterday afternoon.
- I haven't made any, but Fred worked on my computer yesterday.
- Access my email and two Internet Web sites.
- I use Outlook for email, and I was using Chrome™ as the Web browser.

An additional important question to ask in all such scenarios is a yes or no question: Are any other users experiencing the problem? We will assume, in this scenario, that no other users on the same subnet are experiencing the problem.

In addition to questioning the user, the analyst should attempt to replicate the problem at the user's computer if possible. In a scenario like this, going through the steps the user would normally take allows the analyst to verify the process and to view any error messages or notifications that may appear. In this scenario, when the analyst repeats the process, the notification in Figure 1.1 is displayed:

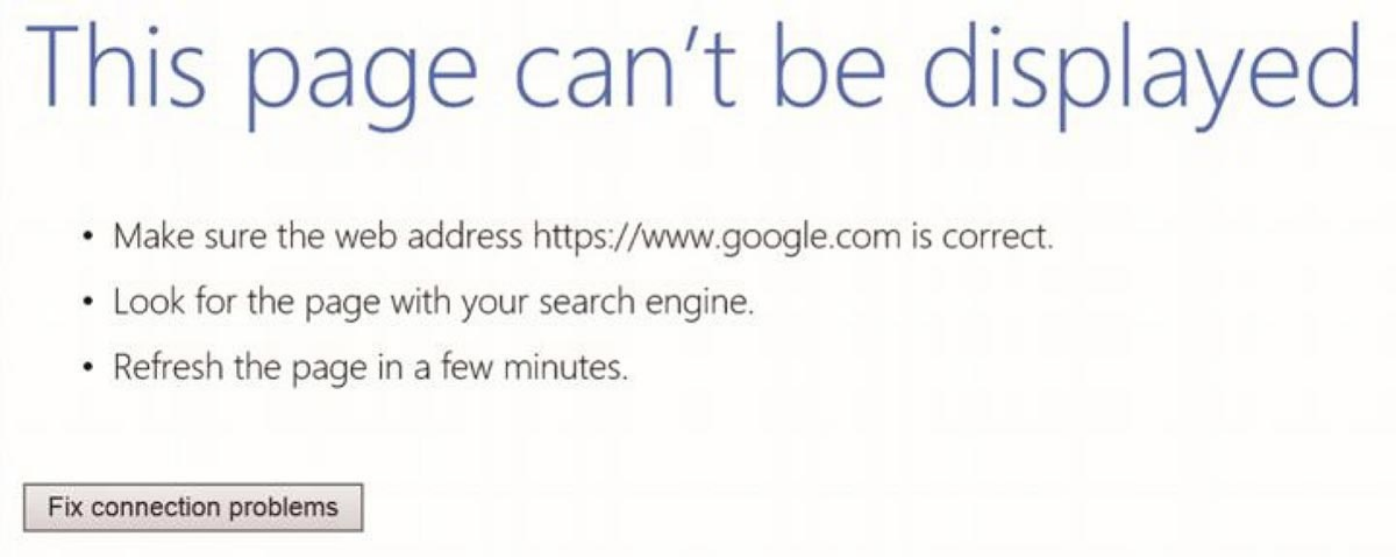


Figure 1-1: Internet Browser Error

Additionally, when the analyst attempts to access other Web sites, the same error is displayed. An exclamation mark is also shown periodically on the wireless client icon in the Notification Tray of Windows® as shown in Figure 1.2.

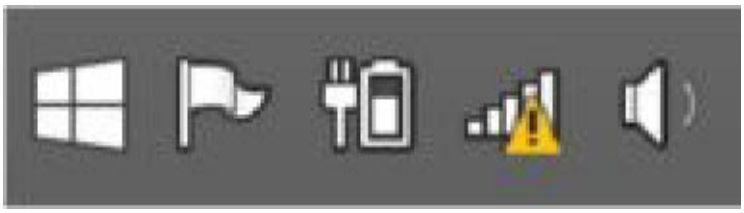


Figure 1-2: Network Notification Icon with Error

3 - Consider possible problems based on the facts discovered.

After gathering the facts, the analyst can then list likely causes of the problem. With a list of potential causes, the analyst can prioritize them in order of most likely and work through them to resolve the problem. The list will come from past experience, vendor literature (FAQs, troubleshooting guides, support videos, etc.), internal documentation of past problems, and information shared by peers. For the given scenario, the following list includes common causes of such problems:

- Supplicant misconfiguration
- Improper static IP settings
- DHCP pool depletion
- DHCP server unreachable
- Improper DHCP pool settings
- DNS server failure or misconfiguration

Based on experience and other sources of information, the analyst may determine the following as the most likely order of causality:

1. DHCP server unreachable
2. Improper static IP settings
3. Supplicant misconfiguration
4. DNS server failure or misconfiguration
5. DHCP pool depletion
6. Improper DHCP pool settings

Finally, with the list generated, you can consider the facts gathered more closely to see if any can be eliminated. For example, it is not likely a DHCP pool settings problem as other users on the subnet have functioning connections. This fact also rules out DNS server failure or misconfiguration, as well as most scenarios that would result in the DHCP server being unreachable (due to router failure or DHCP server failure). These further considerations result in the following prioritized list:

1. Improper static IP settings
2. Supplicant misconfiguration
3. DHCP pool depletion

4 - Create an action plan based on the remaining potential problems and the most likely cause.

With a refined and prioritized list, the analyst is ready to create an action plan for the most likely cause. In this case, the most likely cause is improper static IP settings (which may not be the most likely cause in all environments). The plan of action may look something like this (assuming that DHCP should be in use instead of static IP configuration):

1. Check the IP settings on the client adapter to verify appropriate settings.
2. If configured for static IP settings, change the configuration to use DHCP.
3. Save the changes.
4. Verify network connectivity.

The action plan, as illustrated in the preceding four steps, is simply the list of actions you will take to resolve the issue if the problem were caused by your candidate root problem. In some cases, an action plan will be more complex and involve many more steps. In such scenarios, documenting the action plan becomes more important because you can more easily reverse the steps if they do not resolve the problem. In production environments, standard configurations are often used. If a device has been configured differently than the standard, it may indicate the need for user education. The user needs to understand the ramifications of making unauthorized changes. Additionally, configurations may be locked down so that changes cannot be made without an administrative password.

5 - Implement the action plan.

Now that the action plan is documented, or at least thought through in your mind, you can implement it. This step simply involves performing the actions in sequence to verify a theoretical cause.

6 - As changes are made, gather results.

As the action plan’s steps are taken, results must be gathered. For example, when changing from static to DHCP configuration, did the Internet connectivity begin working? Did the device receive an IP configuration set correctly from the DHCP server?

7 - Analyze the results and determine whether the problem has been resolved.

After completing the steps in the action plan, the analysis must verify that all problems are resolved. For example, in this scenario, are both Web sites and the email application working? If the Web sites are working, but the email application is not, it could indicate that the IP configuration is only part of the overall problem. It may also reveal that additional changes were made, such as the email server settings, which prevent the email application from working properly.

8 - If the problem is not resolved, create a new action plan based on the next most likely cause and proceed with steps 5–8. Repeat until resolved or escalated.

If the problem was resolved, in step 7, the analyst should document the problem and solution in detail and close the trouble ticket, if such a support system is in use. If the problem is not resolved, the next most likely cause should be considered and an action plan created. In this scenario, it was determined that the next most likely cause was supplicant misconfiguration. The supplication settings could be verified, and if the problem is still not resolved, the third most likely cause should be considered, and so on.

In the end, this process will lead to either a solution or escalation. If you have exhausted all possible software and configuration settings in relation to a given problem, hardware failure could be related. In some organizations, the wireless analyst would not be responsible for hardware failures, so the problem would be escalated to the hardware group. Now, let us move from Cisco's process to Microsoft's.

The Microsoft Troubleshooting Process

The Microsoft recommended troubleshooting process can be found at http://bit.ly/1Hy5paJ. The process is divided into five phases as follows:

- **Phase 1:** Discovery—Gather information about the problem.
- **Phase 2:** Planning—Create a plan of action.
- **Phase 3:** Problem Reproduction—Reproduce the problem, or determine that you cannot reproduce it. If you cannot reproduce the problem, then you might not have enough information to confirm that there is a problem.
- **Phase 4:** Problem Isolation—Isolate the variables that relate directly to the problem.
- **Phase 5:** Analysis—Analyze your findings to determine the cause of the problem.

The Microsoft methodology will not be explored in as much detail as the Cisco methodology was. This does not mean one process is better than the other, but both are represented here simply to expose you to variances in vendor methodologies. For example, notice that the Cisco methodology suggests creating an action plan after listing likely causes. The Microsoft methodology suggests creating the action plan before problem reproduction and isolation. However, when the Microsoft methodology is studied in more detail (at the URL provided previously), it is clear that defining possible causes is part of Phase 1.

Additionally, the Microsoft methodology is very focused on finding solutions to problems that occur on a larger scale. For example, if you have deployed 10,000 computers running Windows 10 and find that 1,500 of them are having the same problem, it is very beneficial to reproduce the problem and ensure that the reproduced problem is consistently caused by the same collection of settings and actions. With such assurance, the analyst can then come up with a plan to repair all 1,500 problem clients and trust that the plan will work even on such a large scale. For this reason, the Microsoft methodology places greater emphasis on reproduction of the problem (though the Cisco methodology could include this) and not in creating a list of likely causes.

Industry Methodologies

Industry methodologies are those recommended by independent organizations (non-vendor or vendor-neutral). For example, CompTIA lists varying methodologies for A+ and Network+ certifications. CWNP recommends a troubleshooting methodology for WLANs, which is covered in more detail later in this section. First, I will provide a brief overview of the CompTIA methodologies.

CompTIA Methodologies

The A+ objectives (220-902) list the following steps for a troubleshooting methodology:

1. Identify the problem.
2. Establish a theory of probable cause (question the obvious).
3. Test the theory to determine cause.
4. Establish a plan of action to resolve the problem and implement the solution.
5. Verify full system functionality, and if applicable implement preventive measures.
6. Document findings, actions, and outcomes.

As you can see, the A+ recommended methodology is very similar to the Cisco and Microsoft methodology, with some areas of additional action. I am particularly fond of the extra recommendation to "implement preventive measures," which I feel is an often overlooked step that leads to a much more stable environment when executed. It is important to have a standard configuration and to also ensure that the standard configuration evolves as needed. Many troubleshooting methodologies overlook this action.

The Network+ objectives (N10-005) list the following steps for a troubleshooting methodology:

1. Identify the problem.
2. Establish a theory of probable cause.
3. Test the theory to determine cause.
4. Establish a plan of action to resolve the problem and identify potential effects.
5. Implement the solution or escalate as necessary.
6. Verify full system functionality, and if applicable implement preventative measures.
7. Document findings, actions, and outcomes.

The Network+ methodology includes the process of escalation. This is, in part, due to the fact that A+ is mostly focused on single-machine troubleshooting and Network+ is focused on troubleshooting parts of a system. Network troubleshooting is more complex in many cases as you must consider local systems, devices along the route of communication, and the end systems involved in the transaction. WLAN troubleshooting is similar, and this is the reason escalation is addressed in the CWNP methodology.

> **EXAM MOMENT:** The preceding methodologies were covered to expose you to general troubleshooting concepts. You will be tested against the CWNP methodology covered in the following section and not against the above mentioned methodologies specifically.

CWNP Methodology

Because CWNP exams are focused on WLANs, and the CWAP exam is focused on

WLAN analysis and troubleshooting, the CWNP methodology includes the steps and actions that should be performed in such an environment. It is based on industry experience and feedback and will aid the WLAN professional in resolving network issues quickly and effectively.

The CWNP methodology includes the following steps:

1. Identify the problem.
2. Discover the scale of the problem.
3. Define the possible causes of the problem.
4. Narrow to the most likely cause.
5. Create a plan of action or escalate the problem.
6. Perform corrective actions.
7. Verify the solution.
8. Document the results.

The first step is to *identify the problem*, which is shared by nearly all troubleshooting methodologies. The worst mistake a troubleshooter can make is to assume the specifics of a given problem. Think of identifying the problem as defining the objective. When you define objectives for a WLAN design, for example, you lay the foundation on which the entire design and implementation is built. Without this foundation, the design is sure to fail. The same is true in troubleshooting. Many hours can be wasted by troubleshooting an assumed problem. Assumptions can come from faulty communications with the users experiencing the problem. The problem must always be verified. Ask questions like the following to identify the problem:

- Do you see any error messages?
- Specifically what results are you experiencing that make you feel the network is down?
- Has this happened before and, if so, how often?
- Where are you located?
- Have you moved since your initial connection to the wireless network?
- What device are you using?
- What software are you using?
- Does any other software work on the network?
- Is the problem related to time of day?

As you can see from these questions, you are narrowing the problem to the location, the device and the application. These questions, and others like them, can reveal the true problem.

The second step is to *discover the scale of the problem*. This step is very important as it can reveal a local network outage that impacts all users as opposed to a single-user

problem. If you are receiving reports from multiple users in a coverage area, it is likely a network problem or application problem and not an issue with individual user device configuration. If you are addressing the first report of a problem, ask the user if other users in his or her area are experiencing the same or a similar problem.

> **EXAM MOMENT:** Remember that application problems can be larger in scale than a single individual, as well. For example, if users use a PC-based softphone for VoIP on their laptops, and the first user calls to inform you that the network is down, the reality may be that the call manager is down for that segment and only the VoIP application is experiencing problems. In this case, it is not an actual network problem, but an application problem with scale impact.

The third step is to *define the possible causes of the problem*. A single problem can occur because of many different potential causes. The troubleshooter must narrow the pool of potential causes to the most likely for a given scenario, but first the common causes must be identified. For example, if a user cannot connect to the WLAN, many issues could cause this problem, including:

- The client is configured improperly.
- The AP is down.
- The controller is down.
- The DHCP pool is depleted.
- The DHCP server is down.
- The DNS server is down.
- The switch or router is experiencing problems.
- The Internet connection is down.
- The application server is down or overloaded.
- The client hardware is failing.
- The switch for the wireless adapter is turned off on their laptop.

The point is simple: all of these potential causes, and more, tell the user that they cannot connect to the WLAN. In reality, with many of these causes the device is in fact connected to the WLAN, but something else is wrong. This truth is why step one is so important. The real problem must be identified. If it is, the cause list will shrink dramatically for this third step.

In these first three steps, you will also use technical methods to define the problem and its causes. For example, you may use the OSI model troubleshooting methods described later in this chapter. You may use networking tools to identify possible causes, such as spectrum analyzers, protocol analyzers, and operating system commands like PING, IPCONFIG, TRACEROUTE, and NETSH.

The fourth step is to *narrow to the most likely cause*. One cause is more likely than the others for a given problem in a given environment. Stated differently, each production environment includes a set of devices and standard configurations. A specific environment

will experience common problem causes that another environment may not experience as frequently. For this reason, step four is experiential. Over time, you will learn the most likely cause or causes for a given problem in the environments you support.

For example, when using Aruba Networks® WLAN solution, you will have access to configuration options that do not even exist in a Cisco solution (and vice versa). Therefore, you will experience configuration-related problems in one network that you would not experience in another. After having experience with a solution in your environment you will develop the experiential expertise that allows for faster troubleshooting. This reality is why step eight is so important. The documentation will allow you to determine the most common causes of problems over time, and therefore, make you a better troubleshooter.

The fifth step is to *create a plan of action or escalate the problem*. In the real world of network support, you will not always have the required access to resolve an issue. In such scenarios, you must escalate the problem to the appropriate individual or group. For example, if you determine that your WLAN users are experiencing problems only with VoIP and that it is likely the call manager that is causing the problem, you may not have the appropriate administration permissions to do anything about it. This issue should be escalated to the call manager administrator with all of the details that you have gathered. When you can resolve the issue yourself (assuming you have identified the appropriate cause), you should create a plan of action.

The plan of action may or may not be documented, but you should know what you are going to do and the results that you expect. For example, the plan of action may be to reinstall the device drivers for the WLAN adapter on a client device. You expect that this will result in the repair of corrupted driver files and allow for connectivity to the WLAN. Given a system that supports recoverability features, the following action plan may be in mind:

1. Create a backup of the current configuration.
2. Uninstall the drivers completely from the device.
3. Reinstall the drivers.
4. Attempt to connect to the WLAN.

The sixth step is to *perform corrective* actions. If the previous plan of action results in a working system, you have resolved the issue and are ready for step seven, *verify the solution*. The reality is that you may cycle through steps four through seven many times before finding the solution. In cases where you have altered configuration settings and the problem is not resolved, it is often best to reconfigure the system back to the original settings before moving on to the next possible cause. Otherwise, the system may experience different problems related to the unneeded changes, and you can lose track of where you are in the process.

The eighth and final step is to *document the results*. I would argue that this is equal in importance to the first step, *identify the problem*. If you do not document the results, you do not learn from the experience as you should. Additionally, if you have shared documentation within the organization, others can benefit from your knowledge, as well. I

call this OPK (other people's knowledge). It is for this reason that, immediately after identifying the problem and its scale, you should research your own documentation and possibly online resources to see if others have experienced the same problem and found a solution.

Today, with the global scale of the Internet, it is very unlikely that you are the first one to experience a given problem. Do some research to help focus your *step three* process of defining possible causes. In many scenarios, this research can save you dozens of hours of effort. Use OPK to enhance your troubleshooting abilities. Many WLAN professionals blog, participate in forums, and write other online content that will help you. Additionally, vendors often have troubleshooting guides that provide insightful information for their specific solutions. Take advantage of these resources and of your internal documentation to reduce your troubleshooting time and to become a better WLAN analyst.

In the end, the primary benefit of a troubleshooting methodology is that it ensures the right problem is solved and time is not wasted. In other words, it brings focus to the troubleshooting process.

Troubleshooting with the OSI Model

You may recall use of the OSI Model from both CWNA® and CWSP® curriculum. The Open Systems Interconnection (OSI) Model is a documented conceptual networking model that is not directly implemented in a production protocol; however, it is very useful as a reference model. In fact, the foundational standard document is aptly named the Open Systems Interconnection—Basic Reference Model. As a reference model, it allows network support professionals to speak a shared language. This section will first review the OSI Model layers and then provide guidance for troubleshooting at each layer.

OSI Model Review

The OSI model allows us to think about our network in chunks or layers. You can focus on securing each layer, optimizing each layer and troubleshooting each layer individually. This model allows you to take a very complex communications process apart for analysis and to evaluate its components. The OSI model is segmented into seven layers. The seven layers are (from top to bottom):

- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical

Note: **Many resources suggest mnemonics to help you memorize the OSI model layers. I recommend that you fully understand what each layer does as presented in this chapter, and then you will find memorizing it is much easier. Use a mnemonic if you must, but do not allow this to be a substitute for understanding the functions performed at each layer. One example mnemonic is All People Seem To Need Data Processing, with the first letter of each word in the phrase reminding you of a layer.**

Each layer is defined as both providing services and receiving services. For example, the Data Link Layer provides a service to the Physical Layer (PHY) and receives a service from the Physical Layer. How is this? In a simplified explanation, the Data Link Layer converts packets into frames for the Physical Layer and the Physical Layer transmits these frames as bits on the chosen medium. The Physical Layer reads bits from the chosen medium and converts these into frames for the Data Link Layer.

The layered model allows for abstraction. The higher layers do not necessarily have to know how the lower layers are doing their work. In addition, the lower layers do not necessarily have to know what the upper layers are actually doing with the results of the lower layers' labors. The abstraction gives you the ability to use the same Web browser and HTTP protocol to communicate on the Internet whether the lower layer connection is a dial-up modem, a high-speed Internet connection, or somewhere in between. The resulting speed or performance will certainly vary, but the functionality will remain the same.

Figure 1.3 illustrates the concept of the OSI model. As you can see, data moves down through the layers on the sending machine, across the medium, and then back up through the layers on the receiving machine. Remember, most networking standards allow for the substitution of nearly any Data Link and Physical layer. While this example shows a wired Ethernet connection between the two machines, it could have just as easily been a wireless connection using the 802.11 standard for the descriptions of the Data Link and Physical Layers. This example uses the 802.3 Ethernet standard and the 802.2 LLC standard (a layer within the Data Link Layer) for the lower layers. The point is that the most popular upper layer protocol suite, TCP/IP, can work across most lower layer standards such as 802.2 (Logical Link Control), 802.3 (Ethernet), 802.5 (Token Ring), 802.11 (Wireless LANs), and 802.16 (WiMAX).

In order to fully understand the OSI model and be able to relate to it throughout the remaining chapters of this book, it is important that you explore each layer. You will need to understand the basic description of each layer and the services it provides to the networking process. I will define each layer and then give examples of its use starting with the topmost layer, which is the Application Layer, since this is the order in which they are documented in the standard.

> **EXAM MOMENT:** It is important that you understand the basic operations that take place at each layer of the OSI model. It is also useful to know the primary

components, such as switches, routers, and hubs that function at each level. While not tested directly, indirect references to the OSI model will require this understanding.

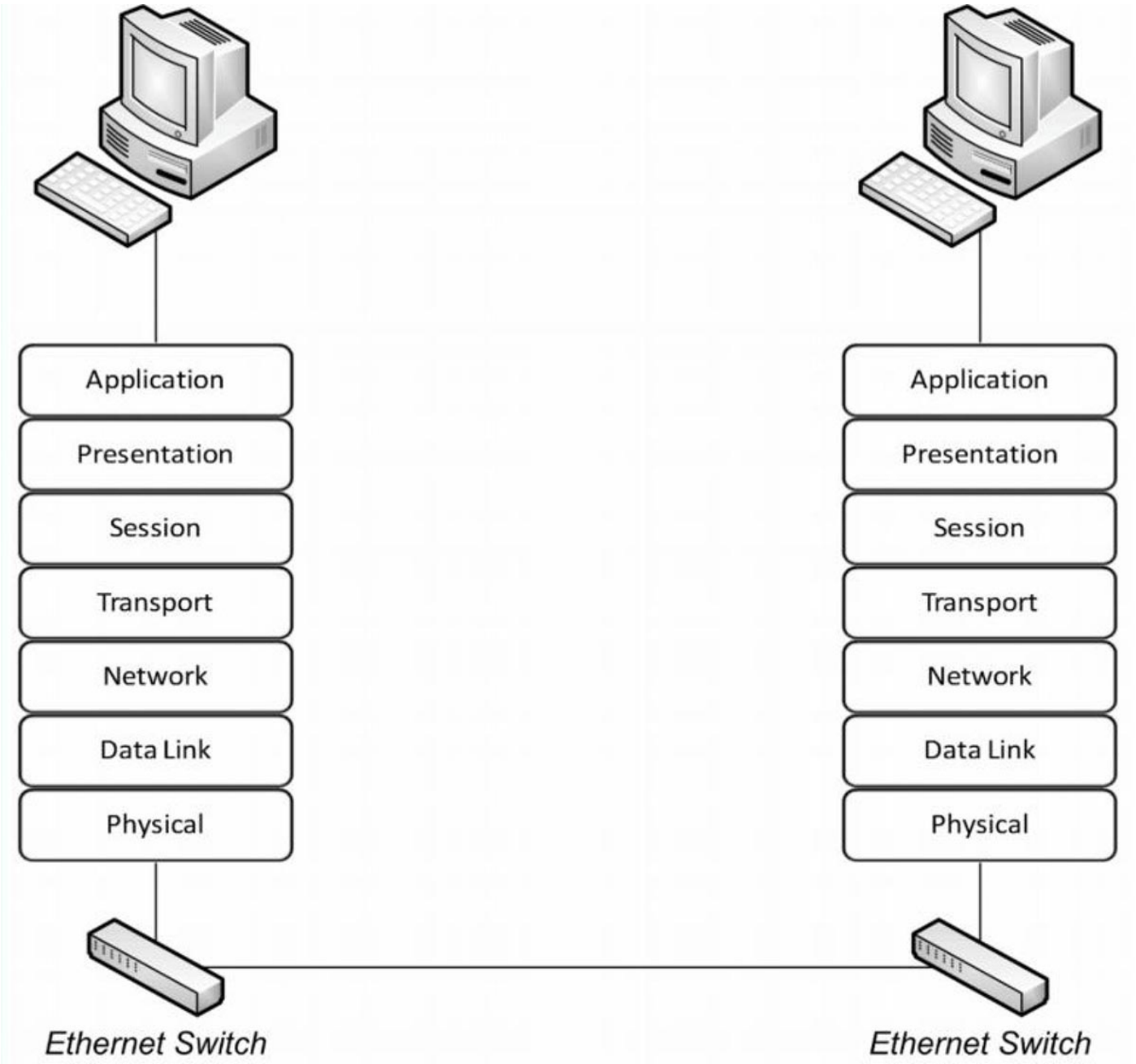


Figure 1-3: The OSI Model Illustrated

The seven layers of the OSI model are defined in clause 7 of the document ISO/IEC 7498-1. The *Application Layer* is defined in sub-clause 7.1 as the highest layer in the reference model and as the sole means of access to the OSIE (Open System Interconnection Environment). The Application Layer is the layer that provides access to the other OSI layers for applications and to applications for the other OSI layers. Do not confuse the Application Layer with the general word application, that is used to reference programs like Microsoft Excel, Adobe Photoshop, and so on. The Application Layer is the OSI layer that these applications communicate with when they need to send or receive data across the network. You could say that the Application Layer exposes the higher-level protocols used for that communication. For example, Microsoft Outlook may need to talk to the SMTP protocol in order to transfer email messages.

Examples of Application Layer protocols and functions include Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Simple Mail Transport Protocol (SMTP). HTTP is used to transfer HTML, ASP, PHP, and other types of documents from

one network host to another. It is the most heavily used Application Layer protocol on the Internet and possibly in the world. FTP is used to transfer binary and ASCII files between a server and a client. Both the HTTP and FTP protocols can transfer any file type. The SMTP is used to move email messages from one server to another and usually works in conjunction with other protocols for mail storage.

Application Layer processes fall into two general categories: user applications and system applications. Email (SMTP), file transfer (FTP), and Web browsing (HTTP) functions fall into the user application category as they provide direct results to applications used by users such as Outlook (email), WS_FTP (file transfer), and FireFox (Web browsing). Notice that the applications or programs used by the user actually take advantage of the application services in the Application Layer or Layer 7. For example, Outlook takes advantage of SMTP. Outlook does not reside in Layer 7, but SMTP does. As examples of system applications, consider DHCP and DNS. The Dynamic Host Configuration Protocol (DHCP) provides for dynamic TCP/IP configuration, and the Domain Name Service (DNS) protocol provides for name to IP address resolution. Both of these are considered system-level applications because they are not usually directly accessed by the user (though this is open for debate since administrators are users too, and they use command line tools or programs to directly access these services quite frequently).

The processes operating in the Application Layer are known as application-entities. An application-entity is defined in the standard as an active element embodying a set of capabilities, which is pertinent to OSI and which is defined for the Application Layer. Application-entities are the services that run in Layer 7 and communicate with lower layers while exposing entry points to the OSI model for applications running on the local computing device. SMTP is an application-entity, as is HTTP and other Layer 7 protocols.

Imagine that you are sending an email using Simple Mail Transport Protocol (SMTP), which is the most popular method of sending an email message. Your email application will connect to an SMTP server in order to send the email message. Interestingly, from the email application’s perspective, it is connecting directly to the SMTP server and is completely unaware of all the other layers of operation that allow this connection to occur. Figure 1.4 shows the email as it exists at Layer 7.

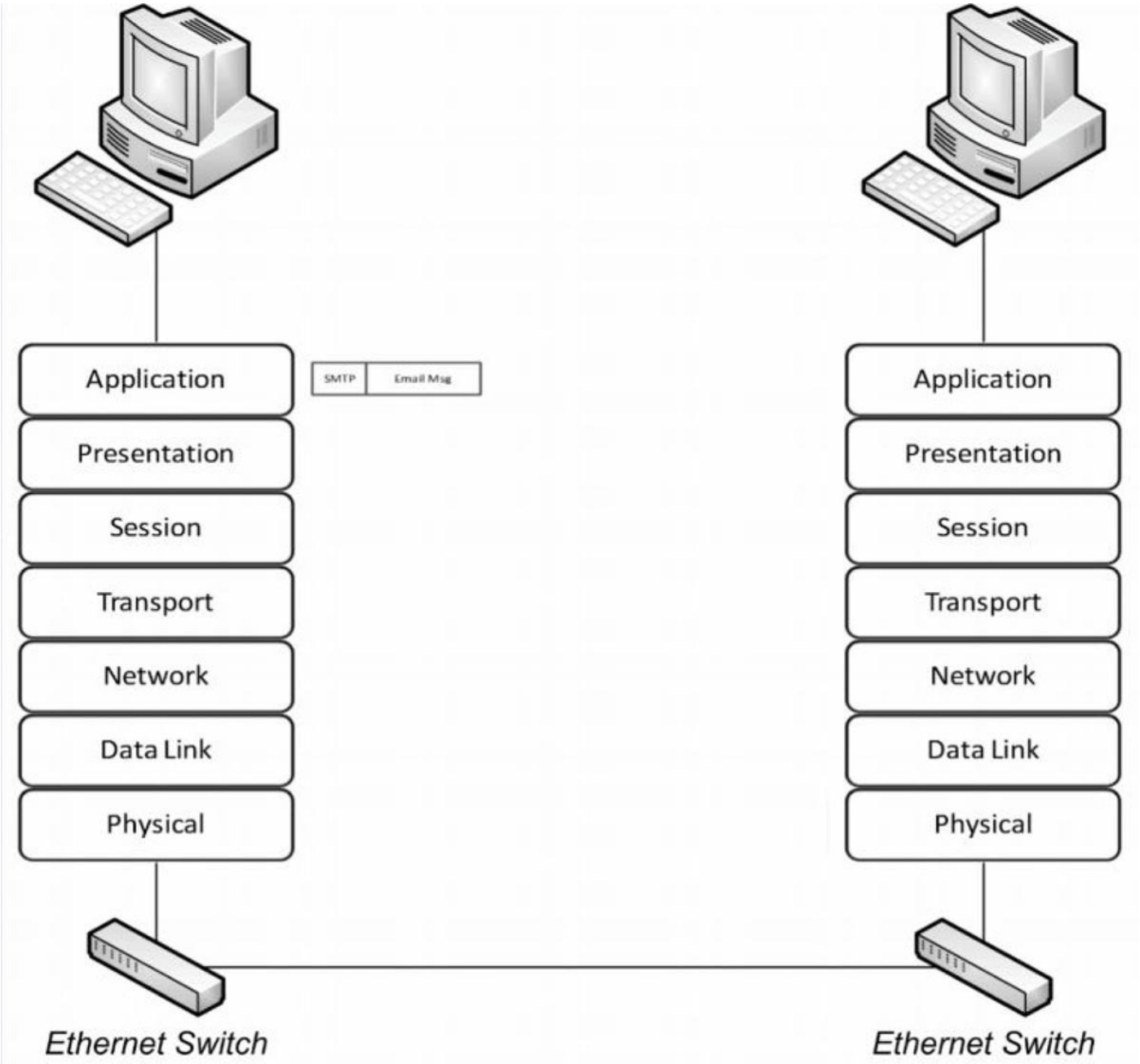


Figure 1-4: Data at the Application Layer (Layer 7)

Devices that operate at Layer 7 include content filtering devices, Web proxies, Layer 7 firewalls, and of course all client devices (laptops, desktops, mobile phones, and even inventory scanners).

The *Presentation Layer* is defined in sub-clause 7.2 of the standard as the sixth layer of the OSI model and it provides services to the Application Layer above it and the Session Layer below it. The Presentation Layer, or Layer 6, provides for the representation of the information communicated by or referenced by application-entities. The Presentation Layer is not used in all network communications and it, as well as the Application Layer and Session Layer, is similar to the single Application layer of the TCP/IP model. The Presentation Layer provides for syntax management and conversion as well as encryption services. Syntax management refers to the process of ensuring that the sending and receiving hosts communicate with a shared syntax or language. When you realize this, you will realize why encryption is often handled at this layer. After all, encryption is really a modification of the data in such a way that must be reversed on the receiving end. Therefore, both the sender and receiver must understand the encryption algorithm in order

to provide the proper data to the program that is sending or receiving on the network.

Examples of Presentation Layer protocols and functions include any number of data representation and encryption protocols. For example, if you choose to use HTTPS instead of HTTP, you are indicating that you want to use Secure Sockets Layer (SSL) encryption. SSL encryption is related to the Presentation Layer or Layer 6 of the OSI model. SSL, the Netscape solution, and TLS, the IETF solution, both operate at Layer 6 of the OSI model.

Ultimately Layer 6 is responsible, at least in part, for three major processes: data representation, data security, and data compression. Data representation is the process of ensuring that data is presented to Layer 7 in a useful way and that it is passed to Layer 5 in a way that can be processed by the lower layers. Data security usually includes authentication, authorization, and encryption. Authentication is used to verify the identity of the sender and receiver. With solid authentication, we gain a benefit known as non-repudiation. Non-repudiation simply means that the sender cannot deny the sending of data. This is often used for auditing and incident handling purposes. Authorization ensures that only valid users can access the data, and encryption ensures the privacy and integrity of the data as it is being transferred.

The processes running at Layer 6 are known as presentation-entities in the OSI model documentation. Therefore, an application-entity is said to depend on the services of a presentation-entity and the presentation-entity is said to serve the application-entity.

As your email message moves down to the Presentation Layer, and since it uses SMTP, it is sent as clear text by default. This is accomplished today using the Layer 6 Multipurpose Internet Mail Extensions (MIME) representation protocol that allows for binary attachments to SMTP messages. The Presentation Layer is converting your email message, whatever its origination, into the standard MIME format or syntax. If you wanted to secure the message, the Secure/MIME (S/MIME) protocol could also be used. The S/MIME protocol, still operating at Layer 6, uses encryption to secure the data as it traverses the network. The encrypted data is sometimes said to be enveloped data. You can see the email now as it exists at Layer 6 in Figure 1.5.

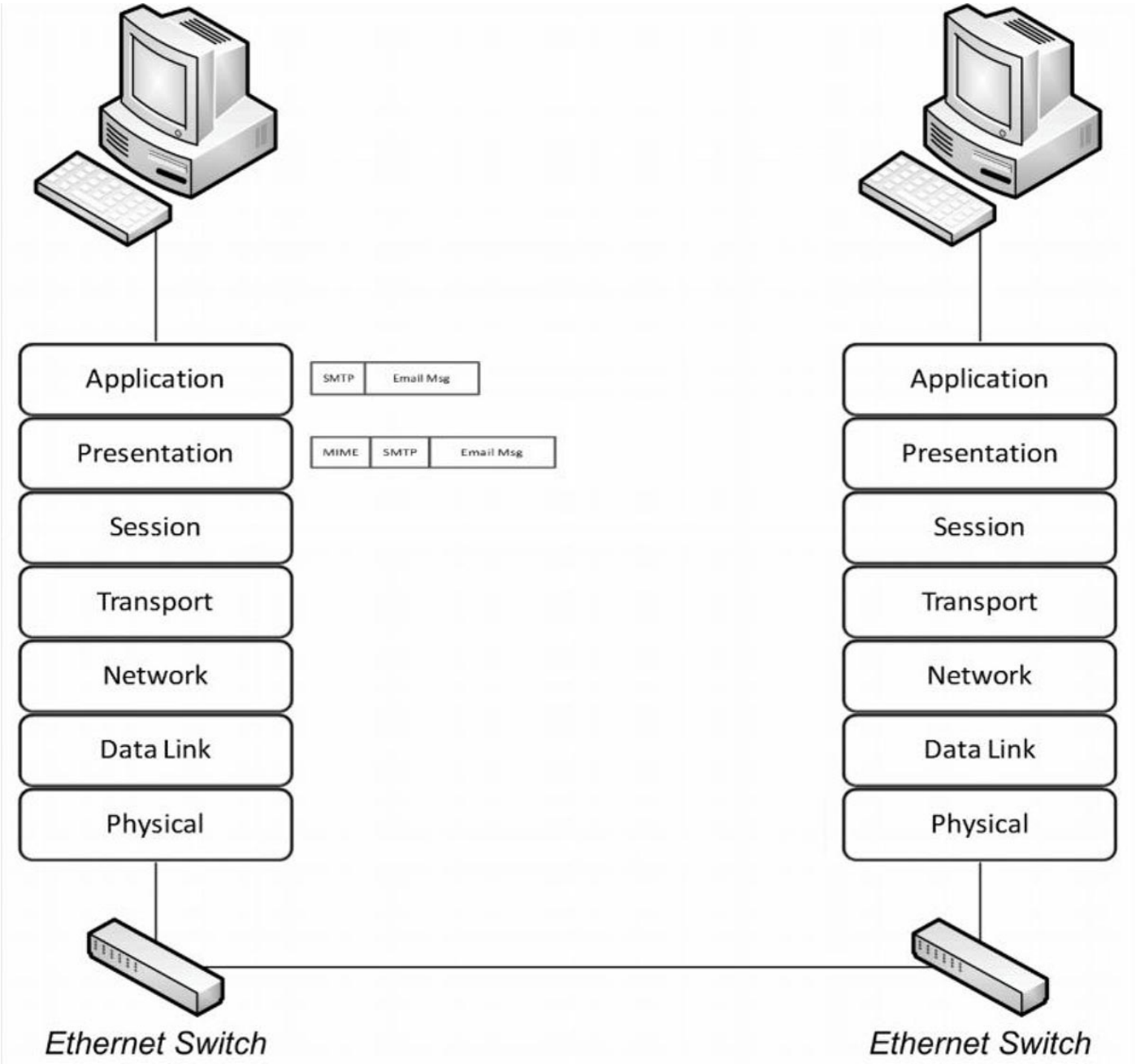


Figure 1-5: Data at the Presentation Layer

The *Session Layer* is defined in sub-clause 7.3 of the standard as providing the means necessary for cooperating presentation-entities to organize and to synchronize their dialog and to manage their data exchange. This is accomplished by establishing a connection between two communicating presentation-entities. The result is simple mechanisms for orderly data exchange and session termination.

A session includes the agreement to communicate and the rules by which the communications will transpire. Sessions are created, communications occur, and sessions are destroyed, torn down, or ended. Layer 5 is responsible for establishing the session, managing the dialogs between the endpoints, and the proper closing of the session.

Examples of Session Layer protocols and functions include the iSCSI protocol, RPC, and NFS. iSCSI is a protocol that provides access to SCSI devices on remote computers or servers. The protocol allows SCSI commands to be sent to the remote device. The Remote Procedure Call (RPC) protocol allows subroutines to be executed on remote computers. A programmer can develop an application that calls the subroutine in the same way as a local

subroutine. RPC abstracts the network layer and allows the application running above Layer 7 to execute the subroutine without knowledge of the fact that it is running on a remote computer. The Network File System (NFS) protocol is used to provide access to files on remote computers as if they were on the local computer. NFS actually functions using an implementation of RPC known as Open Network Computing RPC (ONC RPC) that was developed by Sun Microsystems for use with NFS; however, ONC RPC has also been used by other systems since that time. Remember that these protocols are provided only as examples of the protocols available at Layer 5 (as were the other protocols mentioned for Layers 6 and 7). By learning the functionality of protocols that operate at each layer, you can better understand the intention of each layer.

The services and processes running in Layer 5 are known as session-entities. Therefore, RPC and NFS would be session-entities. These session-entities will be served by the Transport Layer.

At the Session layer, your email message begins to be transmitted to the receiving mail server. The reality is that SMTP email uses the TCP protocol from the TCP/IP suite to send emails, and so the analogy is not perfect at this point. This is because the TCP/IP protocol does not map directly to the OSI model, in fact, it existed before the OSI model. For now, know that Layer 5 is used to establish sessions between these presentation-entities. In Windows, the Winsock API provides access to the TCP/IP protocol suite. We could, therefore, say that your email is passed through to the TCP/IP suite using Winsock here at Layer 5. Figure 1.6 shows the email as it is passed through the Winsock API at Layer 5.

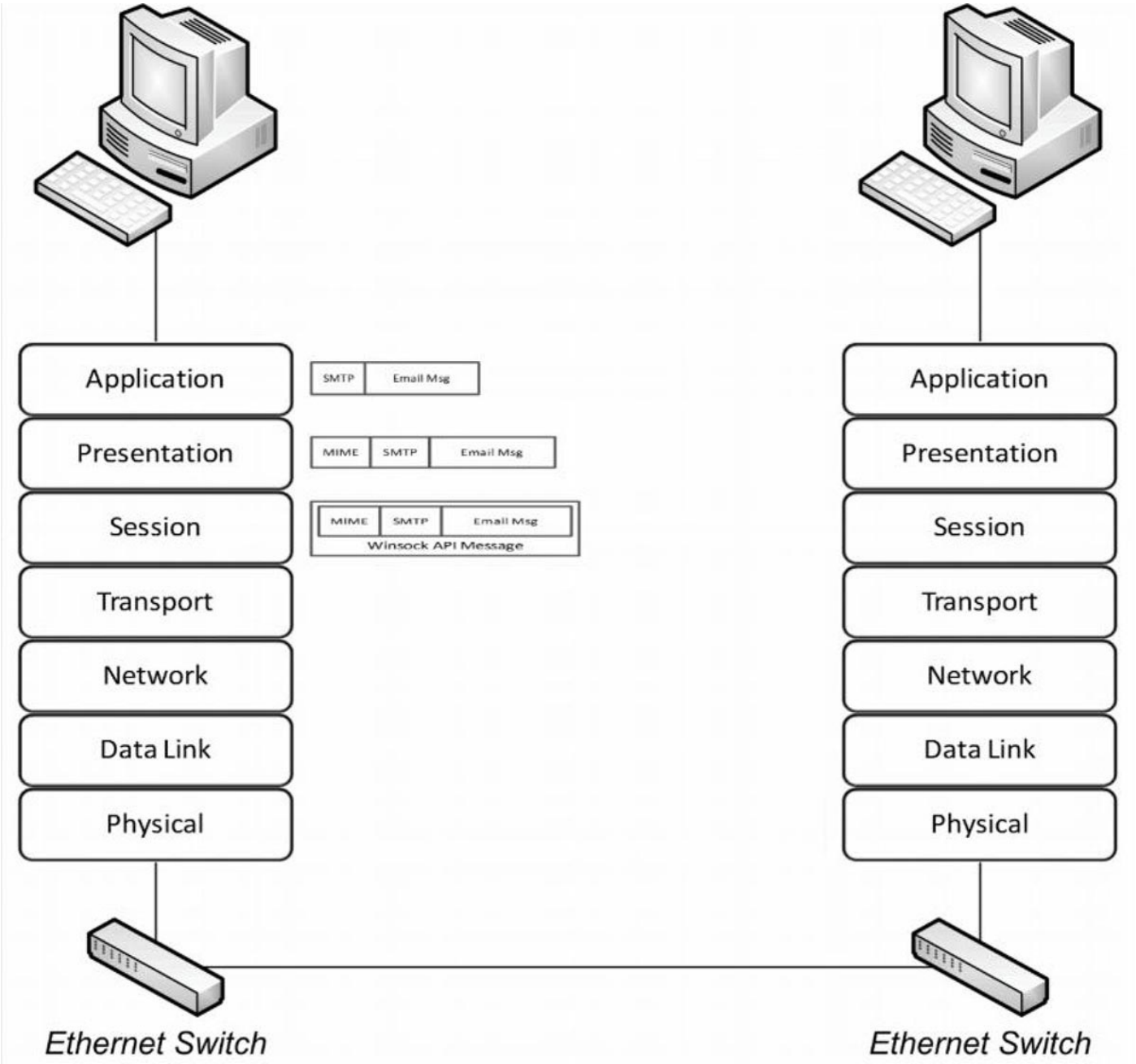


Figure 1-6: Data at the Session Layer

Layer 4, the *Transport Layer* is defined as providing transparent transfer of data between session entities and relieving them from any concern with the detailed way in which reliable and cost effective transfer of data is achieved. This simply means that the Transport Layer, as its name implies, is the layer where the data is segmented for effective transport in compliance with Quality of Service (QoS) requirements and shared medium access.

Examples of Transport Layer protocols and functions include TCP and UDP. The Transmission Control Protocol (TCP) is the primary protocol used for the transmission of connection-oriented data in the TCP/IP suite. HTTP, SMTP, FTP, and other important Layer 7 protocols depend on TCP for reliable delivery and receipt of data. The User Datagram Protocol (UDP) is used for connectionless data communications. For example, when the speed of communications is more important than reliability, UDP is frequently used. Because voice data either has to arrive or not arrive (as opposed to being allowed to arrive late), UDP is frequently used for the transfer of voice and video data.

TCP and UDP are examples of transport-entities at Layer 4. These transport-entities will be served by the Network Layer. At the Transport Layer, the data is broken into segments if necessary. If the data will fit in one segment, then the data becomes a single segment. Otherwise, the data is broken into multiple segments for transmission.

The Transport Layer takes the information about your email message from the Session Layer and begins dividing it (segmenting) into manageable chunks (packets) for transmission by the lower layers. Figure 1.7 shows the email after the processing at the Transport Layer.

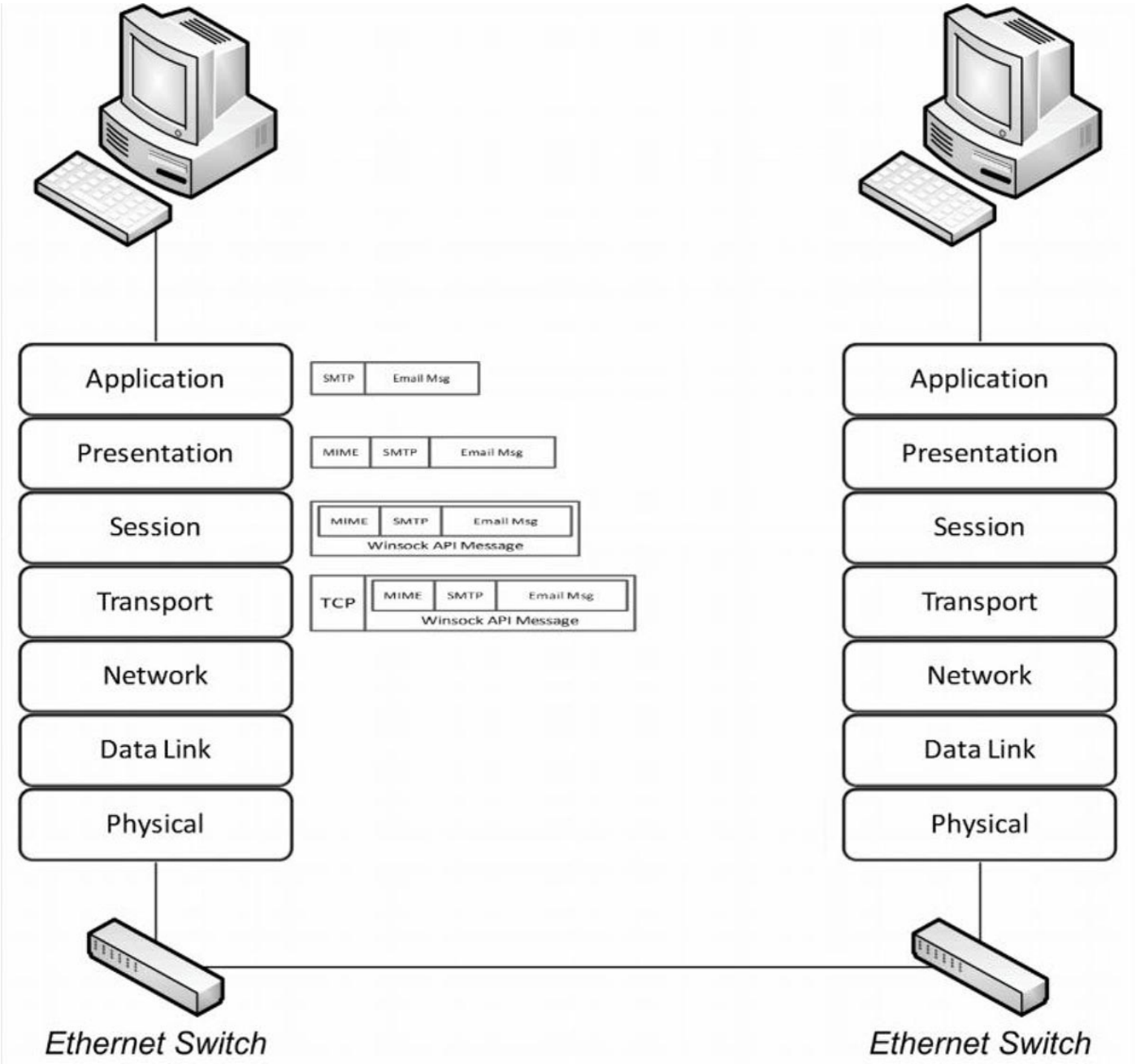


Figure 1-7: Data at the Transport Layer

The *Network Layer* is defined as providing the functional and procedural means for connectionless-mode (UDP) or connection-mode (TCP) transmission among transport-entities and, therefore, provides to the transport-entities independence of routing and relay considerations. In other words, the Network Layer says to the Transport Layer, “You just give me the segments you want to be transferred and tell me where you want them to go. I’ll take care of the rest.” This is why routers do not usually have to expand data beyond Layer 3 to route the data properly. For example, an IP router does not care if it’s routing an email message or voice conversation. It only needs to know the IP address for which the packet is destined and any relevant QoS parameters in order to move the packet along.

Examples of Network Layer protocols and functions include IP, ICMP, and IPSec. The Internet Protocol (IP) is used for addressing and routing of data packets in order to allow them to reach their destination. That destination can be on the local network or a remote network. The local machine is never concerned with this with the exception of the required knowledge of an exit point, or default gateway, from the local machine’s

network. The Internet Control Message Protocol (ICMP) is used for testing the TCP/IP communications and for error message handling within Layer 3. Finally, IP Security (IPSec) is a solution for securing IP communications using authentication and/or encryption for each IP packet. While security protocols such as SSL, TLS, and SSH operate at Layers 4 through 7 of the OSI model, IPSec sits solidly at Layer 3. The benefit is that, since IPSec sits below Layer 4, any protocols running at or above Layer 4 can take advantage of this secure foundation. For this reason, IPSec has become more and more popular since it was first defined in 1995.

The services and processing operating in the Network Layer are known as network-entities. These network-entities depend on the services provided by the Data Link Layer. At the Network Layer, Transport Layer segments become packets. These packets will be processed by the Data Link Layer.

At the Network Layer, your email message that was broken into segments at Layer 4 is now appended with appropriate destination and source addressing information in order to ensure that it arrives at the destination. The results of Layer 3 processing are shown in Figure 1.8

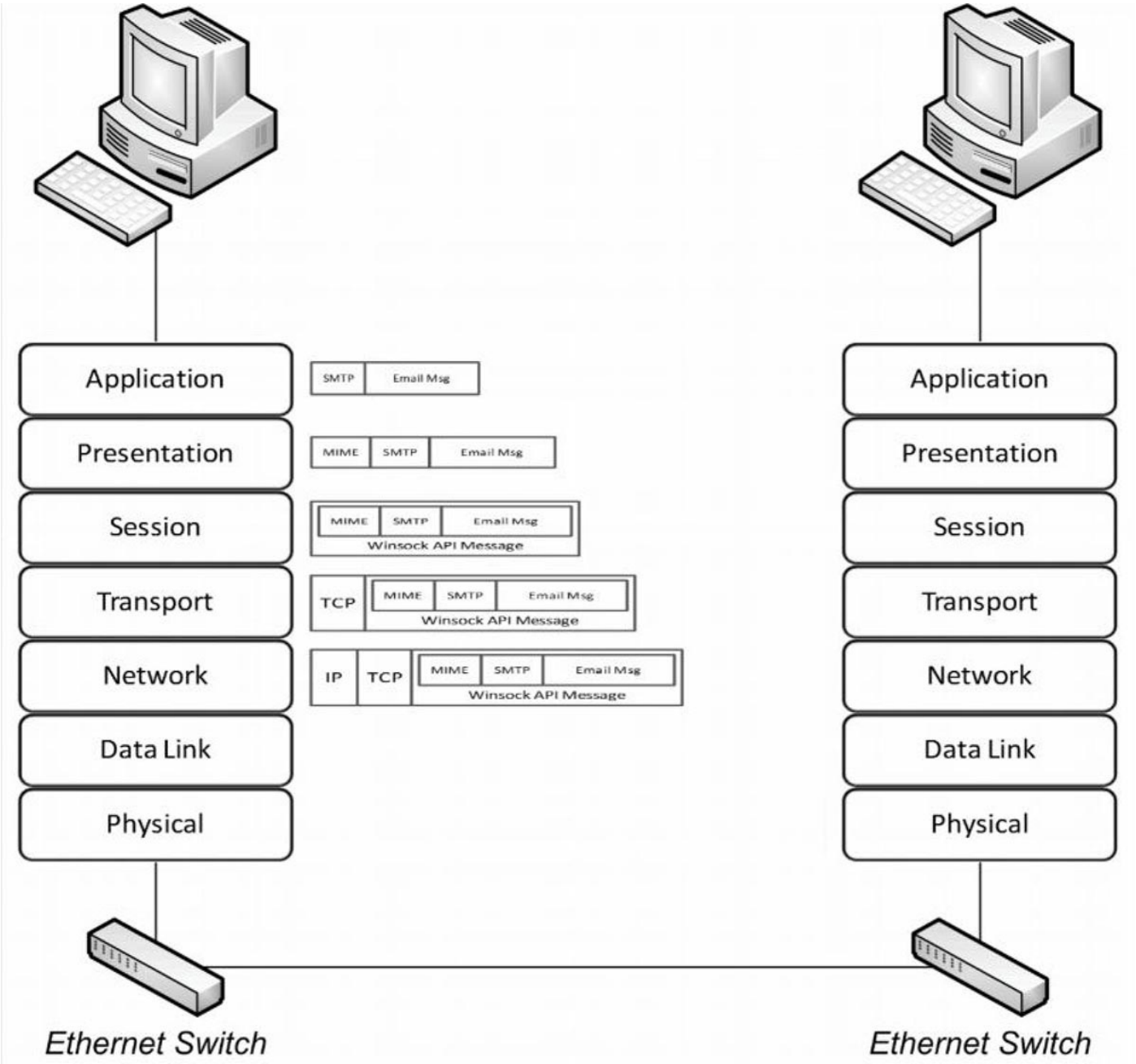


Figure 1-8: Data at the Network Layer

The *Data Link Layer* is defined as providing communications between connectionless-mode or connection-mode network entities. This may include the establishment, maintenance, and release of connections for connection-mode network entities. The Data Link Layer is also responsible for detecting errors that may occur in the Physical Layer. Therefore, the Data Link Layer provides services to Layer 3 and Layer 1. The Data Link Layer, or Layer 2, may also correct errors detected in the Physical Layer automatically.

> **EXAM MOMENT:** Layers 1–4 are the most important layers to understand well for the CWAP exam. Most of the testable information is related to the TCP/IP suite, 802.11 MAC (Medium Access Control), and PHY and 802.3 MAC and PHY operations.

Examples of Data Link Layer protocols and functions include Wi-Fi (802.11), Ethernet (802.3), PPP (RFC 1661), and HDLC (ISO 3309). As you know, Wi-Fi is the common name given to the 802.11 standard and is the primary topic of this book. Ethernet is the most widely used protocol for Local Area Networks (LANs), and will be the type of LAN

you deal with when using most modern LAN technologies. Ethernet comes in many different implementations from 10 Mbps (megabits per second or million bits per second) to 10 Gbps (gigabytes per second) in common implementation. Faster Ethernet technologies are being developed and implemented on a small scale today. The Point-to-Point Protocol (PPP) is commonly used for Wide Area Network (WAN) links across analog lines and other tunneling purposes across digital lines. The High-Level Data Link Control (HDLC) protocol is a solution created by the ISO for bit-oriented synchronous communications. It is a very popular protocol used for WAN links and is the default WAN link protocol for many Cisco routers.

The IEEE has divided the Data Link Layer into two sublayers: the Logical Link Control (LLC) sublayer and the Medium Access Control (MAC) sublayer. The LLC sublayer is not actually used by many transport protocols, such as TCP. The varied IEEE standards identify the behavior of the MAC sublayer within the Data Link layer and the behavior of the PHY layer, as well.

The results of the processing in Layer 2 are that the packet becomes a frame that is ready to be transmitted by the Physical Layer or Layer 1. So the segments became packets in Layer 3 and now the packets have become frames. Remember, this is just the set of terms that we use; the data is really a collection of ones and zeros all the way down through the OSI layers. Each layer is simply manipulating or adding to these ones and zeros in order to perform that layer’s service. Like the other layers before it, the services and processes within the Data Link Layer are named after the layer and are called data-link-entities.

The Data Link Layer adds the necessary header to the email packets received from Layer 3 and your email message, in its one or many parts, is now a frame or set of frames. The frames are ready to be transmitted by the Physical Layer. In Figure 1.9 we see the email message after the Data Link Layer processing is complete.

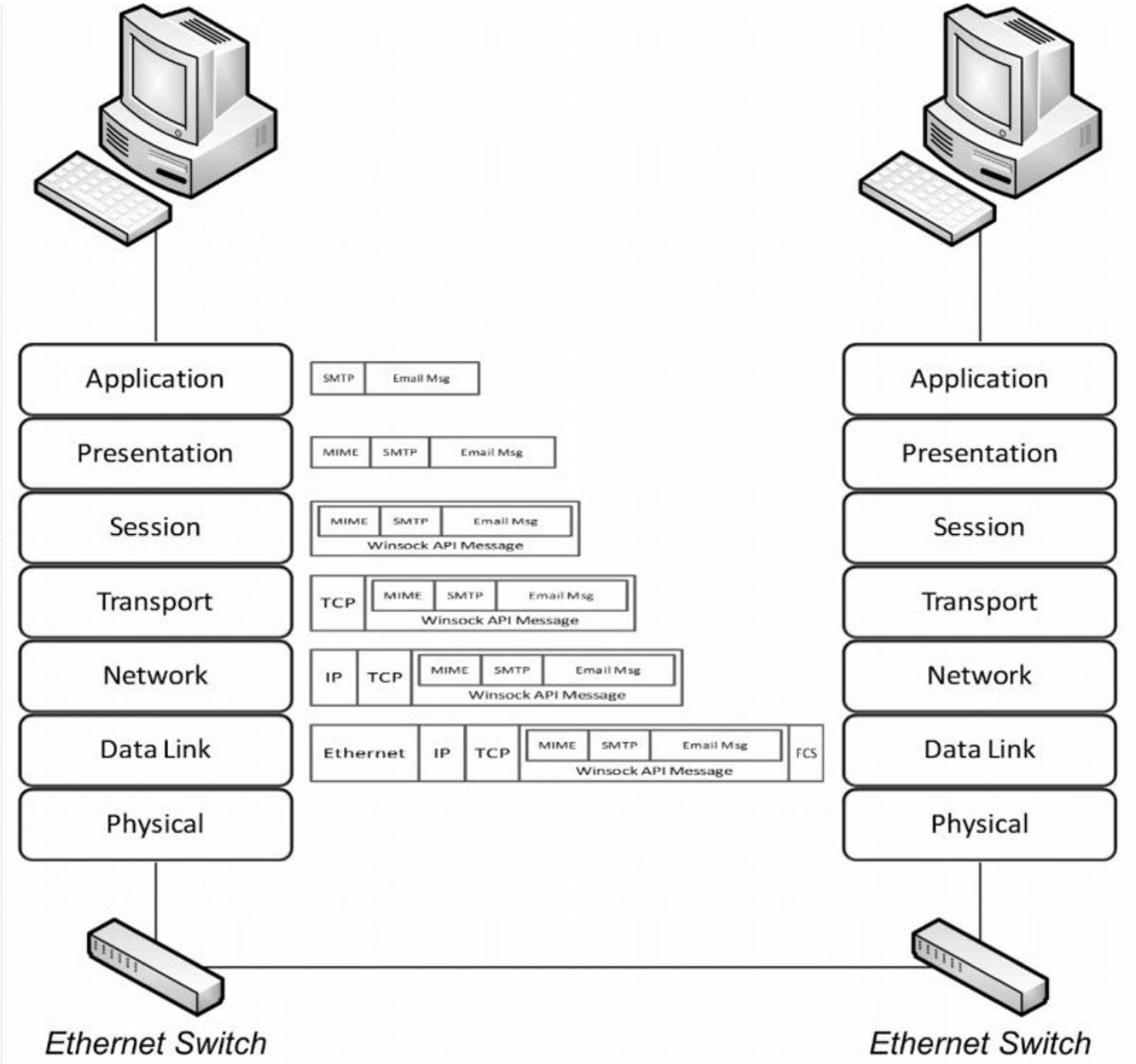


Figure 1-9: Data at the Data-Link Layer

The *Physical Layer*, sometimes called the PHY, is responsible for providing the mechanical, electrical, functional, or procedural means for establishing physical connections between data-link entities. The connections between all other layers are really logical connections as the only real physical connection that results in true transfer of data is at Layer 1—the Physical Layer. For example, we say that the Layer 7's HTTP protocol on a client creates a connection with the Layer 7's HTTP protocol on a web server when a user browses an Internet website. In reality this connection is logical, and the real connections happen at the Physical Layer within a segment of the network and one segment is connected to another, and so on until the final destination is reached.

It is really amazing to think that my computer—the one I am using to type these words—is connected to a wireless access point (AP) in my office, which is connected to my local network, that is in turn connected to the Internet. Through connections—possibly both wired and wireless—I can send signals (that what happens at Layer 1) to a device on the other side of the globe. To think that there is a potential electrical connection path between

these devices and millions of others is really quite amazing.

It is Layer 1 that is responsible for taking the data frames from Layer 2 and transmitting them on the communications medium as binary bits (ones and zeros). This medium may be wired or wireless. It may use electrical signals or light pulses (both actually being electromagnetic in nature). Whatever you have chosen to use at Layer 1, the upper layers can communicate across it as long as the hardware and drivers abstract that layer so that it provides the services demanded of the upper layer protocols.

Examples of Physical Layer protocols and functions include Ethernet, Wi-Fi, and DSL. You probably noticed that Ethernet was mentioned as an example of a Data Link Layer protocol. This is because Ethernet defines both the MAC sub-layer functionality within Layer 2 and the PHY for Layer 1. Wi-Fi technologies (802.11) are similar in that both the MAC and PHY are specified in the standard. Therefore, the Data Link and Physical Layers are often defined in standards together. You could say that Layer 2 acts as an intermediary between Layers 3 through 7 so that you can run IPX/SPX (though hardly anyone uses this protocol today) or TCP/IP across a multitude of network types (network types being understood as different MAC and PHY specifications).

Your email is finally being transmitted across the network. First a one and then a zero, then maybe another one or zero, and on and on until the entire email message is transmitted. Figure 1.10 shows the final results with the email, now broken into frames, being transmitted on the medium.

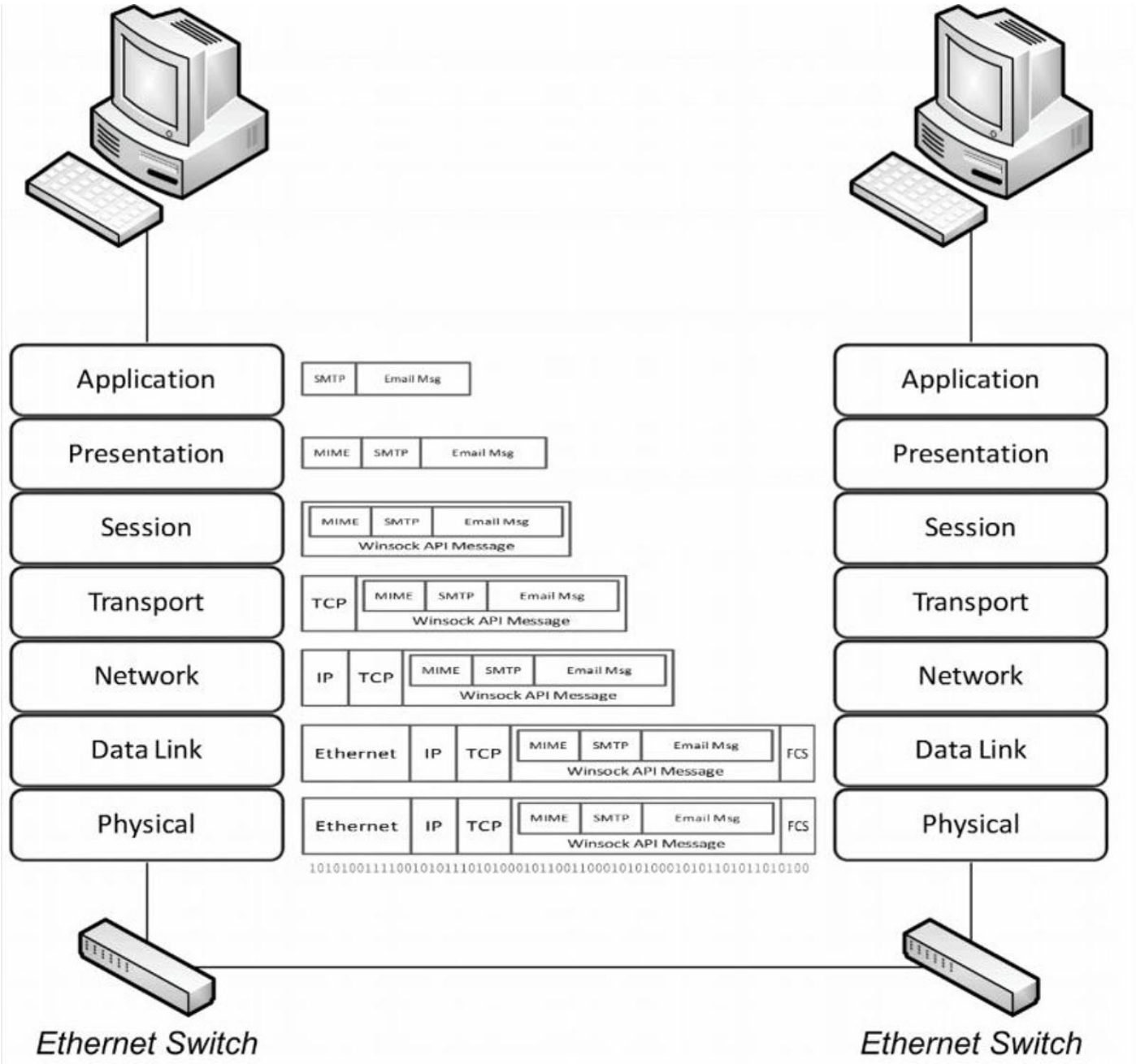


Figure 1-10: Data at the Physical Layer

The example of the email transmission has been simplified in comparison to what really takes place. For example, each packet (from Layer 3) will be transmitted by Layer 1 (after being converted to frames by Layer 2), and then the next packet may be sent or the Network Interface Card (NIC) may need to process incoming data. That incoming data may be a confirmation of a past outgoing packet that was part of the email message, it may be a retry request, or it may be completely unrelated data. Due to the nature of varying underlying Layer 1 technologies, the actual transfer may differ from network to network. However, this example simply illustrates how the data is modified as it passes down through the OSI model.

Now, on the receiving machine, exactly the opposite would transpire. Frames become packets, which become segments, which become the data that may need to be represented, decompressed, or decrypted before being forwarded upstream to the user’s program. When the data is sent, it is formatted, chunked, and transmitted. On the receiving end the data is received, aggregated, and possibly reformatted. This is what the OSI layers do for

us. It is also what many actual network protocols do for us, such as TCP/IP.

Note: **The examples presented here use Ethernet as the communications for Layers 1 and 2. The process is the same for 802.11 networks. However, even 802.11 networks eventually run into Ethernet when the APs bridge Wi-Fi to the wired LAN.**

Why Is the OSI Model Important?

The OSI model is more than a set of facts that you memorize for certification exams. It has become the most common method for referencing all things networking. Many resources assume that you understand this model and reference it without explanation. You may read statements like the following:

Web authentication is a Layer 3 security feature that causes the controller to not allow IP traffic (except DHCP-related packets) from a particular client until that client has correctly supplied a valid username and password. When you use web authentication to authenticate clients, you must define a username and password for each client. When the clients attempt to join the wireless LAN, their users must enter the username and password when prompted by a login window.

This statement is quoted from an article at Cisco's website. Within the article there is no explanation of what is meant by Layer 3. It is simply assumed that you know what this means. The OSI model, therefore, has become required foundational knowledge for anyone seeking to work in the computer or data networking industry. Many certification exams will not test you on the OSI model directly, but will phrase questions in such a way so that you will have to understand the OSI model—as well as some other set of facts—in order to answer the question correctly. CWNP® exams do this, as well.

For example, it is not uncommon to see questions like this, "You are a network administrator working for a manufacturing company. You want to enable secure Voice Over IP communications at Layer 3. What technologies can you use to implement this security?"

The possible answers will, of course, be a list of protocols. You will have to know which of these protocols provide both security and operate at Layer 3 of the OSI model. While you will not see an exact question such as this on the CWAP examination, you will benefit greatly by learning the OSI model for both your certification examination and for your everyday workload. Not to mention the fact that you will actually be able to understand all those articles, whitepapers, and books that refer to various layers of the OSI model.

Now that you understand the layers of the OSI model, it is important for you to understand the communications process utilized within the model. Each layer is said to communicate with a peer layer on another device. The Application Layer on one device communicates with the Application Layer on the other device. In the same way, each layer communicates with its peer layer. This is accomplished through segmentation and encapsulation.

Segmentation is the process of segmenting or separating the data into manageable or allowable sizes for transfer. As an example, the standard Ethernet frame can include a payload (the actual data to be transferred) of no more than 1500 octets. An octet is eight bits and is usually called a byte. Therefore, data that is larger than 1500 bytes will need to be segmented into chunks that are 1500 bytes or smaller before they can be transmitted. Segmentation actually begins at Layer 4 where TCP segments are created, and may continue at Layer 3 where IP fragmentation can occur in order to reduce packet sizes so that they can be processed by Layer 2 as Ethernet frames.

Encapsulation is the process of enveloping information within headers so that the information can be passed across varied networks. For example, IP packets (also called datagrams) are encapsulated inside of 802.11 frames to be transmitted on an 802.11 network. The IP packet is surround by header and possibly footer information that allows the data to be transmitted. 802.11 frames consist of a header that includes the destination and source MAC addresses (and possibly other addresses) and the type of frame in the header. The frames also have a footer that consists of a Frame Check Sequence (FCS) used for error correction. Figures 1.4 through 1.10 depict the way the data changes as it travels down through the OSI model. Notice how encapsulation begins to occur at Layers 5–7 in an almost vague way (this is because there is no direct mapping of TCP/IP to the OSI model) and then becomes very clear as we approach Layers 1–4.

The most important thing to remember about all of this is that, in actuality the Application Layer on one device never talks directly to the Application Layer on another device even though they are said to be peers. Instead, the communications travel through many intermediaries (OSI layers) on the way to the final destination. This is really no different than human communications. Layering is seen in human interactions, as well.

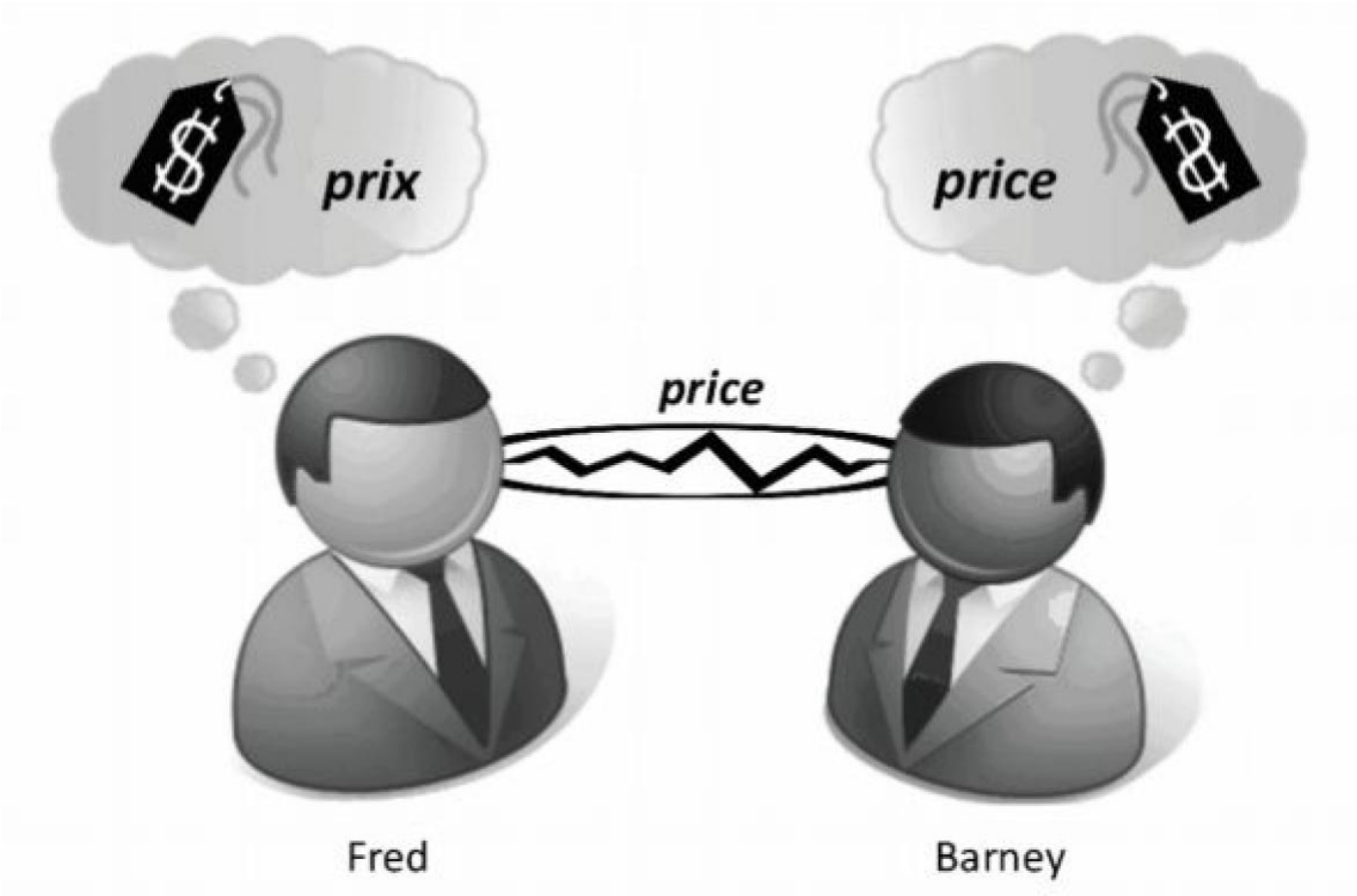


Figure 1-11: Layering in Human Communications

Notice, in Figure 1.11, that we have two humans communicating. Behind the communications is an initial thought that needs to be transferred from the Fred to Barney. The thought may or may not already be in a language that Fred and Barney know. In this case, we assume that Fred's native speaking language is French and Barney's is English. The result is that Fred's thought is in French, and he must translate it into English before he speaks it. After the thought is translated into English, his brain must send signals to the vocal chords and mouth to transmit the signals of sound that result in English enunciation. Now the signals (sound waves) travel through the environment (medium) in which they are spoken until they reach Barney's ears. The eardrums receive these signals and send the received information to the brain. Here the information is interpreted and may or may not have been received correctly. Barney can send back a signal (verbal, visual, or kinesthetic) to let Fred know of his understanding so that Fred can be sure Barney received the communication properly.

Do you see the similarities? Much like the Session Layer represents data in a way that the remote machine can understand it, Fred's brain had to translate the original French thought into a shared language. Similar to the way the Physical Layer has to transmit electrical signals on a wired network, the vocal cords and mouth had to transmit signals as sound waves to Barney's ears. The point is that we could break human communications into layers that are similar to that which is defined in the OSI model. Also, the goal here is to provide peer communications from the "thought area" of the brain to another person's "thought area."

The most important thing for you to remember is that the OSI model is a reference tool and not an actual implementation. It is also useful to remember that data travels down

through the OSI model on the sending machine and up through the OSI model on the receiving machine. Finally, remember that every device on a network will not need to extract everything within the encapsulated data in order to do its job. For example, a Layer 3 router can extract only to the point of the Layer 3 data and still route the data packets just fine.

Troubleshooting Layers

Now that you understand the OSI model, you can utilize it for troubleshooting purposes. Most OSI model troubleshooting is performed at layers 1, 2, 3, 4, and 7 with very little reference to layers 5 and 6 as they are sometimes considered the “mysterious” layers. That is, what occurs at the other five layers is very well defined, and many of them are well understood because the TCP/IP model maps well to layers 1, 2, 3, 4 and 7, but not so well to layers 5 and 6. For this reason, in this section, examples will be given of troubleshooting problems at layers 1–4 and 7 only.

A common Layer 1 problem is lack of connectivity. That is, the user cannot connect to the WLAN. This problem is caused by many different issues, including configuration errors, insufficient signal strength, interference, and more. If you suspect interference as the cause of the problem, you are about to troubleshoot a Layer 1 issue. The medium used by WLANs is radio frequency (RF) and the PHY is implemented through various modulation and coding schemes used to transmit bits on the medium. When interference occurs at the receiver, the RF signal cannot be sufficiently separated from the interfering signal (or noise) to demodulate the bits and process them for Layer 2. PHY problems can be analyzed using spectrum analyzers (covered in detail in Chapter 6) and protocol analyzers (covered in detail in Chapter 7).

The question is this: how do you know if the lack of connection is due to a configuration error, signal strength issues, or interference? The answer is to determine the most likely cause. For example, if you have a stable environment with great control over RF generators (Wi-Fi and non-Wi-Fi devices) that come into your environment, you may determine that the problem is more likely to be a configuration issue or a signal strength issue. If you are, instead, close to another company and have little control over the addition of RF devices in the space, you may determine that the problem is likely to be an interference issue. A quick scan with a spectrum analyzer near the problem receiver can reveal any sources of interference. When using a spectrum analyzer, you are troubleshooting at Layer 1. Additionally, when using a protocol analyzer with a radio tap header that shows signal strength and noise, you are troubleshooting at Layer 1.

Wired network connections include Layer 1 troubleshooting when you are evaluating the cables. Cable testers can be leveraged and the simple replacement of a CAT5e or CAT6 cable can be used to troubleshoot such PHY problems. Additionally, a failing NIC or port in a switch or router would be considered a Layer 1 problem and can be evaluated using the light emitting diodes (LEDs) on the switch or vendor-specific switch commands.

Layer 2 problems have to do with addressing (MAC addresses), framing, and encryption/security in WLANs. For example, an improperly entered or incorrect pre-shared key would fall into the category of a Layer 2 problem because no communications

outside of the AP are required in an autonomous deployment. All of the communications happen between the AP and the client in such an environment. In a controller-based environment, the frames will be sent to the controller in a tunnel, but the pre-shared key is an entirely Layer 2 configuration parameter. This is not completely true when WPA2-Enterprise is used, as communications must happen between the AP and RADIUS server using higher layer protocols. However, the communications between the AP and the client STA are still at Layer 2 using Extensible Authentication Protocol (EAP) over LAN (EAPOL). A protocol analyzer can be used to evaluate EAPOL communications and for troubleshooting authentication issues.

Layer 3, the Network Layer, is all about IP addressing in modern networks. Therefore, routing issues, location of servers and other network devices, and IP configuration errors are common causes of problems. Troubleshooting of Layer 3 is performed mostly using tools like PING, IPCONFIG, TraceRoute (TraceRT in Windows), NETSH, and others. Consider that when a device on one segment can communicate with other devices on the same segment but cannot communicate with devices on another segment, either routing configuration or default gateway settings are common causes. Using IPConfig on the local device to ensure proper default gateway configuration and verifying the route configuration in the router will usually lead to a solution.

An example of a common Layer 4 (Transport Layer) problem is a blocked port on a local device. Many devices have endpoint security solutions, such as client firewalls, that block specific ports or all ports except those that are explicitly opened. If such a scenario exists, the client device will be unable to use an application that requires the use of the blocked ports. The user may feel that a network error is occurring when the actual problem is an improper configuration in the client firewall.

Layer 7, the Application Layer, is where protocols like HTTP and SMTP reside. Example causes of problems include malformed HTTP requests; improperly configured Layer 7 firewalls, proxy servers or proxy settings on the client; and server unresponsiveness. Troubleshooting Layer 7 is beyond the scope of this book; however, it is important to remember that many problems are caused by Layer 7 issues.

The key here is to always ask, is this a Layer 1, 2, 3, or 4 problem when dealing with lower-level networking issues, and is this a Layer 7 problem when dealing with application issues. Focusing on the most likely layer of the OSI model that would cause the problem can lead to quick resolution. As you study the remaining chapters in this book, it will become clear that an awareness of the OSI model and troubleshooting with this knowledge in mind is extremely helpful.

Matching Tools to Problems

When it comes to troubleshooting WLANs, the professional’s toolbox is important. The focus here is not on screw drivers and pliers, but on protocol analyzers, spectrum analyzers, throughput testers, and native operating system tools. Of course, traditional tools are important for mounting, remounting, and removal of physical hardware, but the majority of network problems are resolved using more technical tools of the trade. In this

section, networking tools and operating system tools are explained and matched to common problems. These problems include the lack of network connectivity, slow network performance, unavailable resources, and unavailable services.

Networking Tools

Networking tools are used to analyze and troubleshoot network connection and throughput issues. They include throughput testers, protocol analyzers, and spectrum analyzers. These tools are covered in greater detail in later chapters but are introduced here to provide a foundation for understanding. These tools are not included as native parts of operating systems, and therefore exist in their own category as they must be installed before use.

```
C:\Windows\System32\cmd.exe
C:\iperf>iperf3 /?
iperf3: parameter error - must either be a client (-c) or server (-s)

Usage: iperf [-s|-c host] [options]
       iperf [-h|--help] [-v|--version]

Server or Client:
  -p, --port      #         server port to listen on/connect to
  -f, --format    [kmgKMG]  format to report: Kbits, Mbits, KBytes, MBytes
  -i, --interval  #         seconds between periodic bandwidth reports
  -F, --file name           xmit/recv the specified file
  -B, --bind      <host>    bind to a specific interface
  -V, --verbose             more detailed output
  -J, --json                output in JSON format
  --logfile f               send output to a log file
  -d, --debug               emit debugging output
  -v, --version             show version information and quit
  -h, --help                show this message and quit
Server specific:
  -s, --server              run in server mode
  -D, --daemon              run the server as a daemon
  -I, --pidfile file        write PID file
  -1, --one-off             handle one client connection then exit
Client specific:
  -c, --client    <host>    run in client mode, connecting to <host>
  -u, --udp                 use UDP rather than TCP
  -b, --bandwidth #[KMG][/#] target bandwidth in bits/sec (0 for unlimited)
                            (default 1 Mbit/sec for UDP, unlimited for TCP)
                            (optional slash and packet count for burst mode)
  -t, --time      #         time in seconds to transmit for (default 10 secs)
  -n, --bytes     #[KMG]    number of bytes to transmit (instead of -t)
  -k, --blockcount #[KMG]   number of blocks (packets) to transmit (instead of -
t or -n)
  -l, --len       #[KMG]    length of buffer to read or write
                            (default 128 KB for TCP, 8 KB for UDP)
  --cport         <port>    bind to a specific client port (TCP and UDP, default
: ephemeral port)
  -P, --parallel  #         number of parallel client streams to run
  -R, --reverse             run in reverse mode (server sends, client receives)
  -w, --window    #[KMG]    set window size / socket buffer size
  -M, --set-mss   #         set TCP/SCTP maximum segment size (MTU - 40 bytes)
  -N, --no-delay            set TCP/SCTP no delay, disabling Nagle's Algorithm
  -4, --version4            only use IPv4
  -6, --version6            only use IPv6
  -S, --tos N               set the IP 'type of service'
  -Z, --zerocopy            use a 'zero copy' method of sending data
  -O, --omit N              omit the first n seconds
  -T, --title str           prefix every output line with this string
  --get-server-output       get results from server
  --udp-counters-64bit      use 64-bit counters in UDP test packets

[KMG] indicates options that support a K/M/G suffix for kilo-, mega-, or giga-

iperf3 homepage at: http://software.es.net/iperf/
Report bugs to:     https://github.com/esnet/iperf

C:\iperf>
```

Figure 1-12: Help for the Windows-based iPerf Command

Throughput testers are used to evaluate the useful data bits that can pass through a network. They typically test at Layer 4 but may be able to test at higher layers, as well. At

Layer 4, the Network Layer, they are testing TCP and UDP traffic. TCP is used for standard data communications and UDP is used for real-time communications. Figure 1.12 shows the help output for the Windows iperf command (specifically iperf3, available at: `bit.ly/1Ut2fs7`). Figure 1.13 shows the output of an executed command.

```
C:\Windows\System32>iperf -s -i 1
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size: 8.00 KByte (default)
------------------------------------------------------------
[292] local 10.0.0.106 port 5001 connected with 10.0.0.40 port 1105
[ ID] Interval       Transfer     Bandwidth
[292]  0.0- 1.0 sec  11.0 MBytes  92.1 Mbits/sec
[292]  1.0- 2.0 sec  11.1 MBytes  93.0 Mbits/sec
[292]  2.0- 3.0 sec  10.6 MBytes  89.1 Mbits/sec
[292]  3.0- 4.0 sec  10.9 MBytes  91.6 Mbits/sec
[292]  4.0- 5.0 sec  11.1 MBytes  93.3 Mbits/sec
[292]  5.0- 6.0 sec  11.1 MBytes  93.1 Mbits/sec
[292]  6.0- 7.0 sec  11.0 MBytes  92.3 Mbits/sec
[292]  7.0- 8.0 sec  11.0 MBytes  92.1 Mbits/sec
[292]  8.0- 9.0 sec  11.1 MBytes  93.0 Mbits/sec
[292]  9.0-10.0 sec  11.3 MBytes  94.6 Mbits/sec
[292]  0.0-10.0 sec   110 MBytes  92.3 Mbits/sec
```

Figure 1-13: Output from the Windows iPerf Command

Throughput testers typically work on a client/server model. That is, one machine will act as the server and another as the client. GUI-based throughput testers provide a graphical interface used to configure the server and the client and to execute the testing. Command-based throughput testers work at the Command Prompt in Windows or at the shell in Linux environments. They use commands with switches to configure the server and to execute the test on the client.

The default behavior of iperf is to test the throughput from the client to the server. Therefore, when testing a wireless client, to test the downlink, the wireless client should be configured as the iperf server. To test the uplink, the wireless client should be configured as the iperf client. Some versions of iperf allow for bidirectional testing so that this concern no longer exists. You will find when working with wireless links that downlink traffic often performs better than uplink traffic

An example of a GUI-based throughput tester is TamoSoft® Throughput Tester shown in Figure 1.14. This tool can test both TCP and UDP traffic and supports reporting on packet loss with visual graphs showing moment-by-moment throughput performance. The tool is available for both Windows and Mac OS X®.

When testing throughput, it is important to remember that you are not testing the data rate. The data rate is the rate at which bits can be sent across the wireless medium, and is entirely dependent on signal quality and the modulation and coding used. Higher data rates use more sophisticated modulation and coding schemes and require better signal conditions than lower data rates. The data rate is a significant factor in determining network throughput for a user, but it does not stand alone. In addition, the contention for the wireless medium must be considered. Chapter 2 will review wireless communications, including contention algorithms used in WLANs.

For example, if a single client has a data rate of 866.7 Mbps with an 802.11ac connection

to the AP using the Very High Throughput (VHT) PHY, this does not mean that the client will achieve performance values as if it were the only client connected. Other clients may be connected to the same AP at 54 and 48 Mbps. Those clients will gain access to the medium as well, and the super-fast 802.11ac client will simply have to wait its turn. This impacts Layer 4 throughput significantly, and it impacts it even more on busier WLANs with more varied clients and more activity from those clients. The point is that throughput is not a simple factor of data rate, and this will be discussed more as you continue through the book.

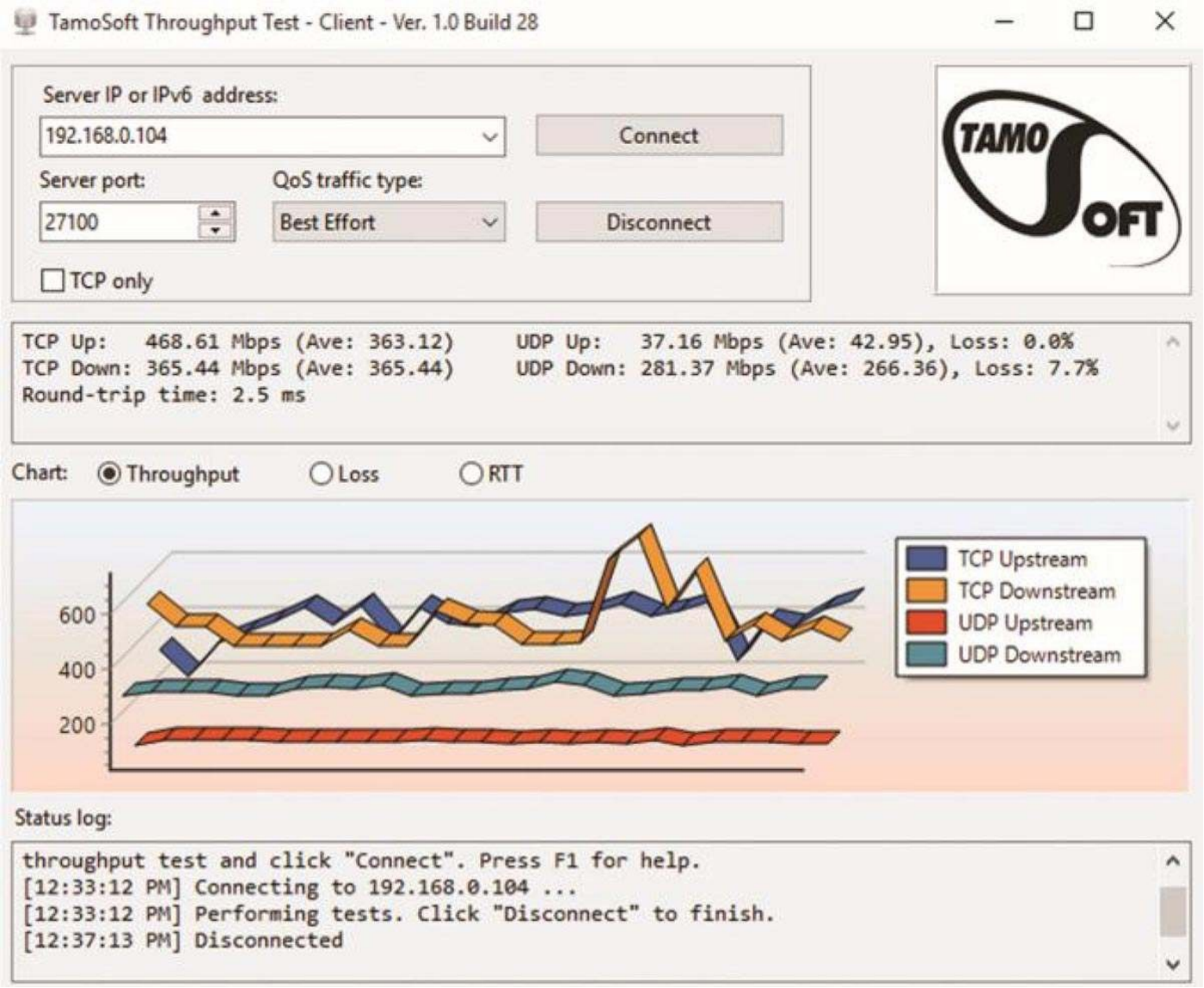


Figure 1-14: TamoSoft Throughput Tester

Throughput testers are useful to the WLAN analyst for the following:

- Verifying application performance problems
- Locating intermittent performance issues
- Validating the performance of a new WLAN
- Proactively locating problem areas of the WLAN
- Ensuring continued and consistent performance

The next networking tool is the protocol analyzer. Protocol analyzers have existed for more than two decades. They are tools that allow you to capture and decode networking

frames and packets. Wired protocol analyzers are very easy to use as they work with practically any network adapter. Wireless protocol analyzers are different as they require specifically compatible adapters. Given that an entire chapter is dedicated to protocol analyzers later in this book, I will not cover them in more detail here.

> **EXAM MOMENT:** Know that throughput testers evaluate the useful data throughput and not the data rate of the WLAN link. The useful throughput is always less than the data rate on WLANs because of management overhead.

For now, just know that protocol analyzers are useful to the WLAN analyst for the following:

- Analyzing network settings
- Gathering details about unsupported networks
- Checking for frame corruption and retransmissions
- Locating the source of authentication and other communication problems
- Identifying overloaded service sets or channels
- Identifying devices on the network
- Validating compliance with requirements
- Discovering supported features and behaviors of wireless devices

Spectrum analyzers are used to monitor and analyze the RF activity in an area. They show all RF activity, and not just WLAN activity like a protocol analyzer does. For example, non-W-Fi devices like microwave ovens, phones, wireless peripherals, and more will show up as long as they operating in the monitored frequency. Spectrum analyzers are also covered in extensive detail in a later chapter of this book.

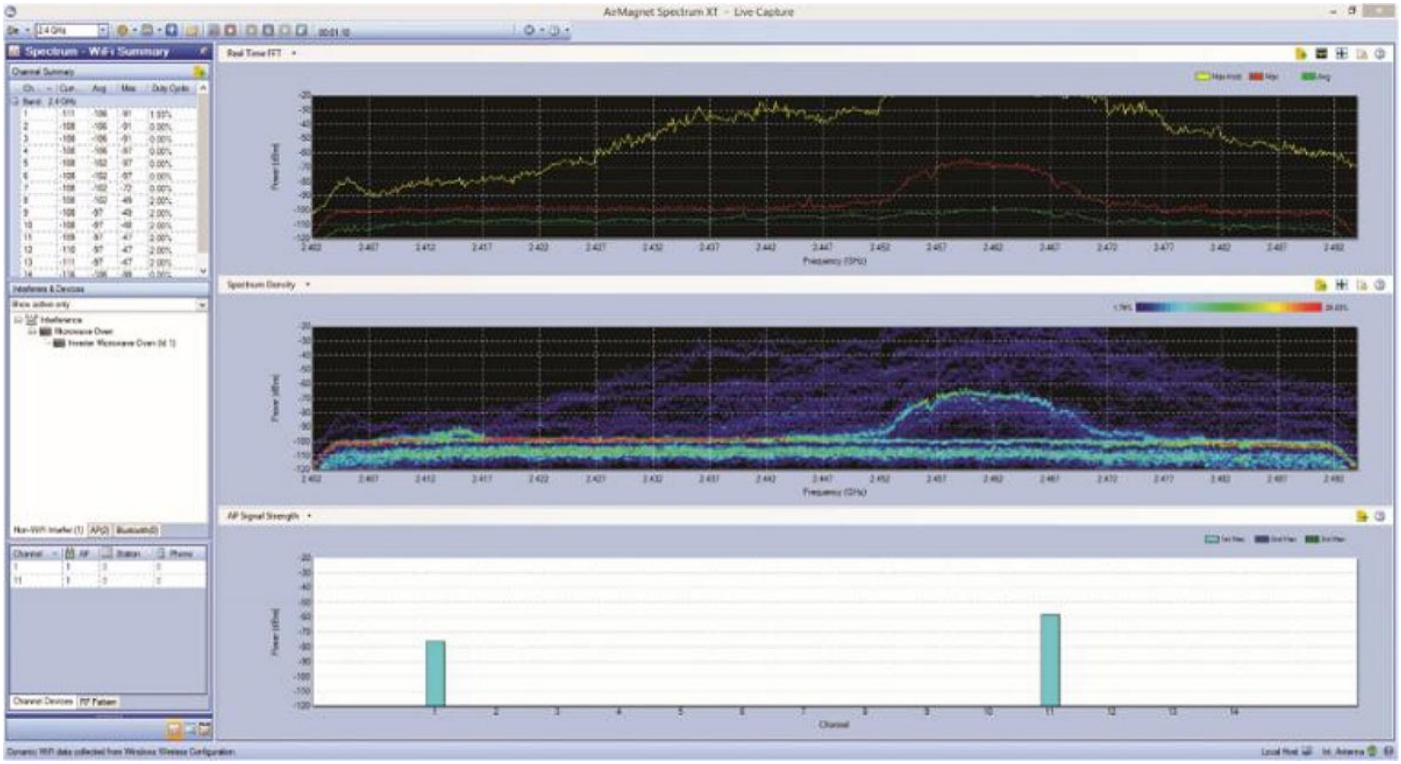


Figure 1-15: AirMagnet Spectrum XT USB-Based Spectrum Analyzer

For now, just know that spectrum analyzers are useful to the WLAN analyst for:

- Locating sources of interference
- Determining channel utilization for Wi-Fi and non-Wi-Fi devices
- Detecting poorly constructed hardware with improper spectral masks or inconsistent spectral masks
- Discovering the presence of non-Wi-Fi activity, including incidental activity
- Viewing signal strength in important coverage areas
- Selecting the least busy channel for a new BSA (Basic Service Area)

Operating System Tools

Operating System (OS) tools come with the OS and help in the troubleshooting process. These tools are also used to analyze connection issues and view client device parameters, settings, and capabilities. These include ping, traceroute, pathping, nslookup, netstat, and netsh (in Windows). They are introduced here to provide a foundation for understanding, and some of them are evaluated in more detail in later chapters.

The ping command is available in most OSes and even in many embedded OSes such as those in switches and routers. The command is used to attempt an Internet Control Message Protocol (ICMP) communication with a remote host based on the IP address. While a DNS host name may be used, the name is simply resolved to the IP address, and the IP address is the actual target of the ICMP ping request. The sender (the machine on which the ping command is executed) sends an ECHO ICMP message (a TYPE 8 ICMP message) to the target IP address. If the target IP address both receives the request and is configured to allow responses, it will send back an ECHO REPLY ICMP message (a TYPE 0 ICMP message, see RFC 792 for more detail).

When using this command, the size of the ping response packet is based on the size of the data field in the ECHO message. The ECHO REPLY message simply sends back the same data sent in the ECHO message. This behavior is defined in the RFC and can be validated in a simple protocol capture of a ping process as shown in Figure 1.16. Most ping commands provide a switch to change the size of the ECHO message, like the `-l` switch in Windows.

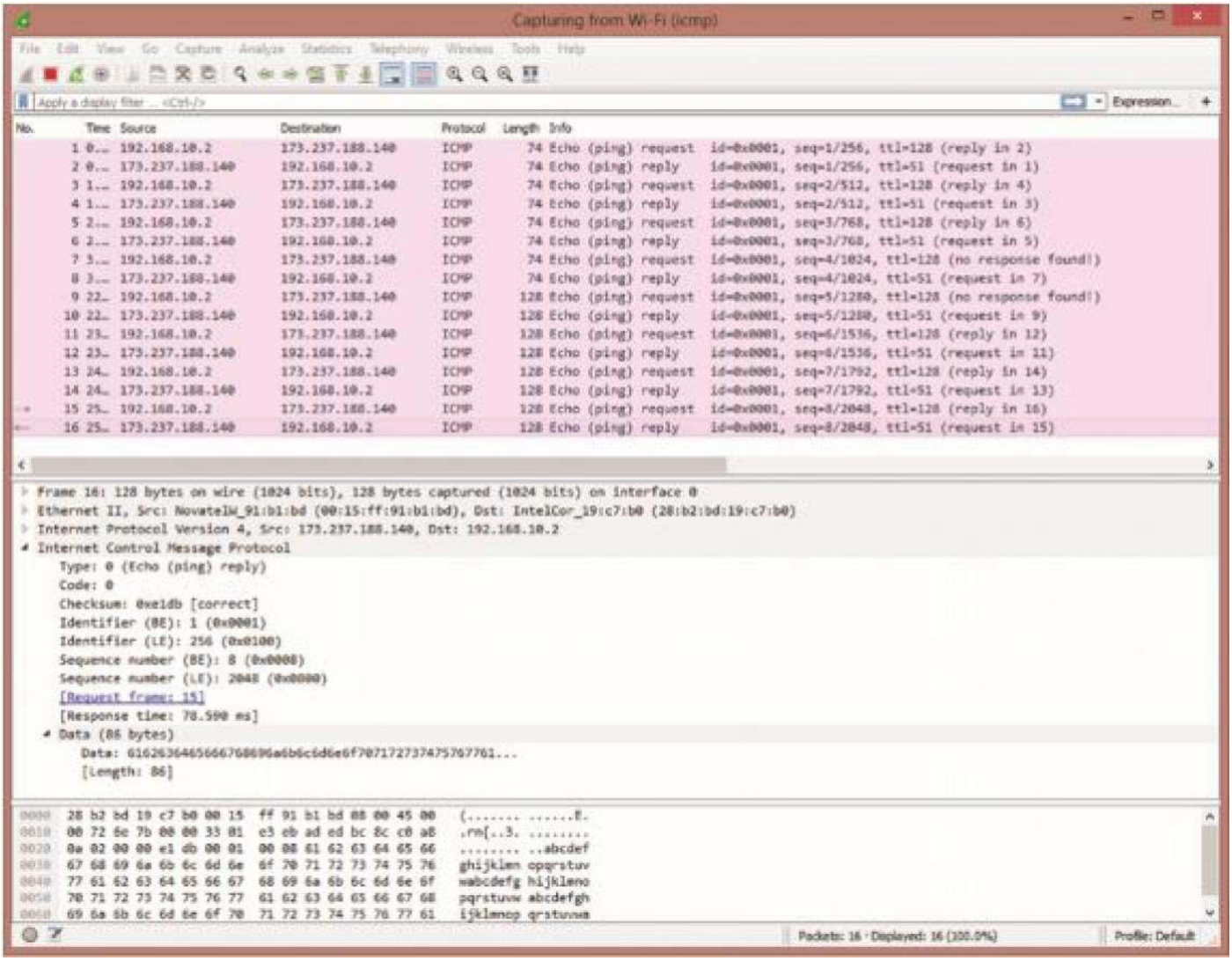


Figure 1-16: PING Captured in a Protocol Analyzer

In Windows, PING supports the parameters shown in Figure 1.17. Two important parameters for testing are `-t` and `-l`. The `-t` parameters is used to specify that the ping operation should run until interrupted (with a `CTRL + C` keystroke). This function is useful when testing for intermittent connectivity problems. Simply run the command, like `ping 192.168.10.7 -t`, and then watch for lost ECHO REPLY messages during the process.

The `-l` parameter is used to change the data size in the ECHO message (the sent message) and therefore in the ECHO REPLY message. This function is useful when you wish to force more data through the network, which can reveal problems that a small 32 byte message (the Windows default size) will not reveal.

```
C:\Windows\System32\cmd.exe

C:\Windows\System32>ping /?

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
            [-4] [-6] target_name

Options:
    -t             Ping the specified host until stopped.
                   To see statistics and continue - type Control-Break;
                   To stop - type Control-C.
    -a             Resolve addresses to hostnames.
    -n count       Number of echo requests to send.
    -l size        Send buffer size.
    -f             Set Don't Fragment flag in packet (IPv4-only).
    -i TTL         Time To Live.
    -v TOS         Type Of Service (IPv4-only. This setting has been deprecated
                   and has no effect on the type of service field in the IP
                   Header).
    -r count       Record route for count hops (IPv4-only).
    -s count       Timestamp for count hops (IPv4-only).
    -j host-list   Loose source route along host-list (IPv4-only).
    -k host-list   Strict source route along host-list (IPv4-only).
    -w timeout     Timeout in milliseconds to wait for each reply.
    -R             Use routing header to test reverse route also (IPv6-only).
                   Per RFC 5095 the use of this routing header has been
                   deprecated. Some systems may drop echo requests if
                   this header is used.
    -S srcaddr     Source address to use.
    -c compartment Routing compartment identifier.
    -p             Ping a Hyper-V Network Virtualization provider address.
    -4             Force using IPv4.
    -6             Force using IPv6.

C:\Windows\System32>
```

Figure 1-17: PING Command Parameters

The traceroute command differs from the ping command in that it sends ICMP ECHO messages to each node along the path to a destination. This function is accomplished with creative use of the time-to-live (TTL) field in the IP packet. First, the command sends three ICMP ECHO messages to the “ping” target with a TTL of 1. Therefore, when the first router receives it, it sends back a TTL Timeout message and, of course, this means the traceroute command now knows that router’s address. Next, the command sends three more ICMP ECHO messages with a TTL of 2. The result, as you might imagine, is that the next router in the path receives the packets, but the TTL will be 0, and it therefore responds with a TTL Timeout message. The traceroute command now knows that IP address. This process continues until the “ping” target is reached.

The benefit of the traceroute command (again, tracert in Windows) is that it checks each device along the path. On your internal network, assuming all routers are configured to respond to ICMP ECHO messages with ICMP ECHO REPLY messages, the traceroute command will help you ensure availability of all routers along the path. On the Internet, it is not uncommon to see request timeout errors from some nodes along the path. Some organizations disable ICMP ECHO REPLY messages on Internet facing devices for performance and security reasons. Figure 1.18 shows a protocol analyzer capture of the ICMP messages sent and received by a traceroute command. Remember, when using TraceRT and other IP tools, all communications with private addresses (10.x.x.x, 192.168.x.x and 172.16.x.x-172.31.x.x) stay within your network under normal

conditions.

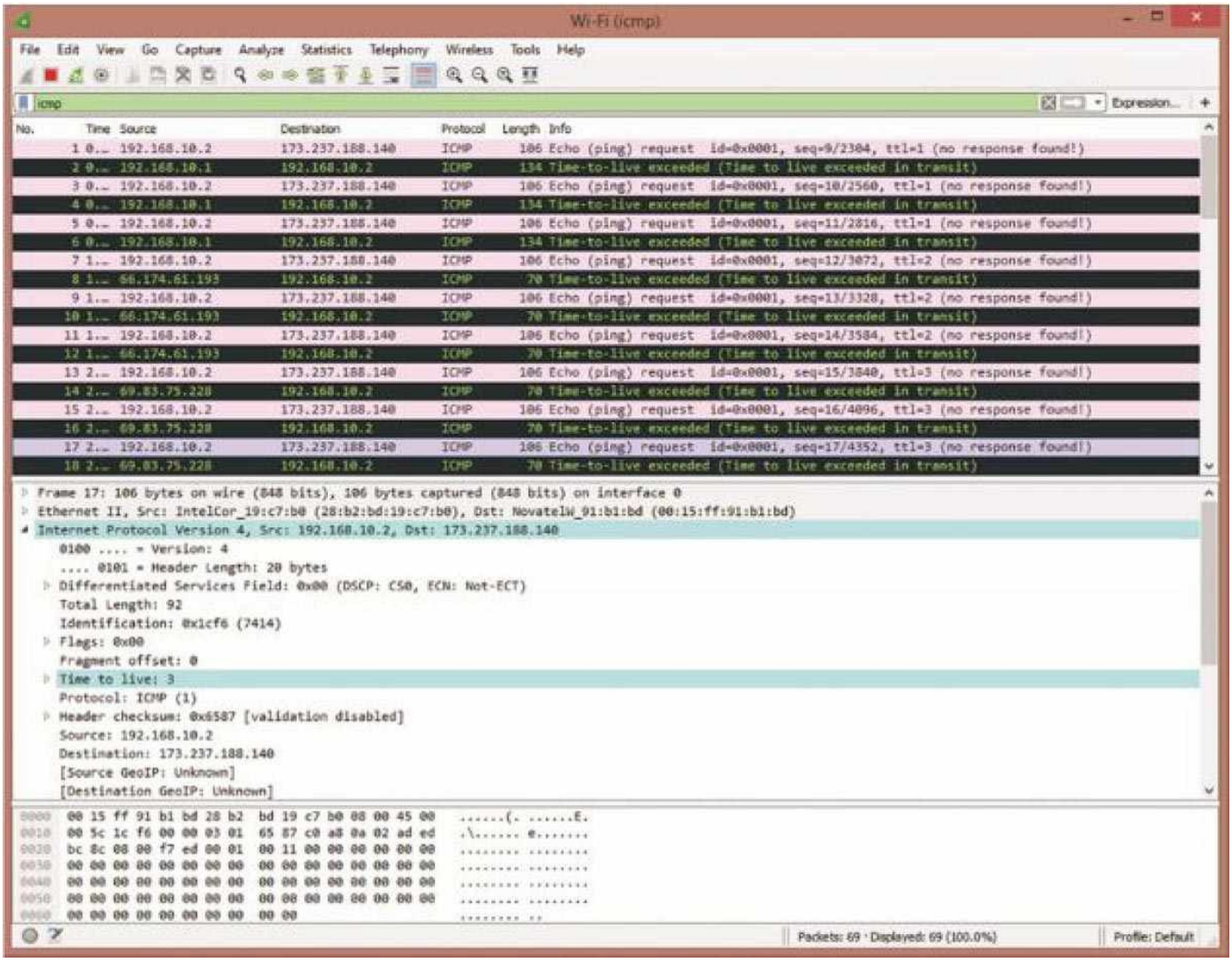


Figure 1-18: Traceroute Process Captured in WireShark

The pathping command is a somewhat enhanced implementation of traceroute in Windows. It not only determines the route taken but also responds with useful statistics about the performance along the path. The pathping command sends ICMP ECHO messages to each hop in the same manner as traceroute and then sends multiple ICMP ECHO messages to each hop to calculate performance over time for each hop. Figure 1.19 shows sample output from the pathping command.

```
C:\Windows\System32\cmd.exe

C:\Windows\System32>pathping www.cwnp.com -q 20 -p 50

Tracing route to www.cwnp.com [173.237.188.140]
over a maximum of 30 hops:
  0  Lenovo-flip [192.168.10.2]
  1  VerizonBRV [192.168.10.1]
  2  193.sub-66-174-61.myvzw.com [66.174.61.193]
  3  228.sub-69-83-75.myvzw.com [69.83.75.228]
  4  18.sub-69-83-75.myvzw.com [69.83.75.18]
  5  194.sub-69-83-68.myvzw.com [69.83.68.194]
  6  208.sub-69-83-64.myvzw.com [69.83.64.208]
  7  1.sub-69-83-66.myvzw.com [69.83.66.1]
  8  ae55.bar2.Cincinnati1.Level3.net [4.59.42.13]
  9     *        *        *
Computing statistics for 8 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           Lenovo-flip [192.168.10.2]
                                       0/  20 =  0%   |
  1    1ms     0/  20 =  0%            0/  20 =  0%  VerizonBRV [192.168.10.1]
                                       0/  20 =  0%   |
  2  ---      20/  20 =100%           20/  20 =100%  193.sub-66-174-61.myvzw.com [66.174.61.193]
                                       0/  20 =  0%   |
  3   60ms     0/  20 =  0%            0/  20 =  0%  228.sub-69-83-75.myvzw.com [69.83.75.228]
                                       0/  20 =  0%   |
  4  ---      20/  20 =100%           20/  20 =100%  18.sub-69-83-75.myvzw.com [69.83.75.18]
                                       0/  20 =  0%   |
  5  ---      20/  20 =100%           20/  20 =100%  194.sub-69-83-68.myvzw.com [69.83.68.194]
                                       0/  20 =  0%   |
  6  ---      20/  20 =100%           20/  20 =100%  208.sub-69-83-64.myvzw.com [69.83.64.208]
                                       0/  20 =  0%   |
  7  ---      20/  20 =100%           20/  20 =100%  1.sub-69-83-66.myvzw.com [69.83.66.1]
                                       0/  20 =  0%   |
  8   61ms     0/  20 =  0%            0/  20 =  0%  ae55.bar2.Cincinnati1.Level3.net [4.59.42.13]

Trace complete.

C:\Windows\System32>_
```

Figure 1-19: PATHPING Command Output

NSLookup is used to query DNS servers. It is a useful command to use when clients cannot resolve host names to IP addresses or when a lightweight AP is unable to locate its controller and DNS is intended to be used for such location services.

Netstat is used to show statistics for network connections. Simply running Netstat with an interval in seconds, like 10, will show active connections and, if you leave it running, it will show new connections you create. This can be useful to analyze targets for TCP sessions on the network. Figure 1.20 shows the active connections reported by Netstat.

```
C:\Windows\System32\cmd.exe - netstat 10

  TCP    127.0.0.1:49156        Lenovo-flip:5354       ESTABLISHED
  TCP    127.0.0.1:49157        Lenovo-flip:5354       ESTABLISHED
  TCP    127.0.0.1:49167        Lenovo-flip:27015      ESTABLISHED
  TCP    192.168.10.2:49901     40.122.129.128:https   TIME_WAIT
  TCP    192.168.10.2:49903     a23-62-239-11:http     ESTABLISHED
  TCP    192.168.10.2:49904     a23-62-239-11:http     ESTABLISHED
  TCP    192.168.10.2:49905     a23-62-239-11:http     ESTABLISHED
  TCP    [2600:1009:b011:fe70:e912:db9:7fd9:a844]:49358  bn1wns2012011:https    ESTABLISHED
  TCP    [2600:1009:b011:fe70:e912:db9:7fd9:a844]:49359  bn1wns1011320:https    ESTABLISHED

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:5354         Lenovo-flip:49156      ESTABLISHED
  TCP    127.0.0.1:5354         Lenovo-flip:49157      ESTABLISHED
  TCP    127.0.0.1:27015        Lenovo-flip:49167      ESTABLISHED
  TCP    127.0.0.1:49156        Lenovo-flip:5354       ESTABLISHED
  TCP    127.0.0.1:49157        Lenovo-flip:5354       ESTABLISHED
  TCP    127.0.0.1:49167        Lenovo-flip:27015      ESTABLISHED
  TCP    192.168.10.2:49901     40.122.129.128:https   TIME_WAIT
  TCP    192.168.10.2:49903     a23-62-239-11:http     ESTABLISHED
  TCP    192.168.10.2:49904     a23-62-239-11:http     ESTABLISHED
  TCP    192.168.10.2:49905     a23-62-239-11:http     ESTABLISHED
  TCP    [2600:1009:b011:fe70:e912:db9:7fd9:a844]:49358  bn1wns2012011:https    ESTABLISHED
  TCP    [2600:1009:b011:fe70:e912:db9:7fd9:a844]:49359  bn1wns1011320:https    ESTABLISHED

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:5354         Lenovo-flip:49156      ESTABLISHED
  TCP    127.0.0.1:5354         Lenovo-flip:49157      ESTABLISHED
  TCP    127.0.0.1:27015        Lenovo-flip:49167      ESTABLISHED
  TCP    127.0.0.1:49156        Lenovo-flip:5354       ESTABLISHED
  TCP    127.0.0.1:49157        Lenovo-flip:5354       ESTABLISHED
  TCP    127.0.0.1:49167        Lenovo-flip:27015      ESTABLISHED
  TCP    192.168.10.2:49903     a23-62-239-11:http     ESTABLISHED
  TCP    192.168.10.2:49904     a23-62-239-11:http     ESTABLISHED
  TCP    192.168.10.2:49905     a23-62-239-11:http     ESTABLISHED
  TCP    [2600:1009:b011:fe70:e912:db9:7fd9:a844]:49358  bn1wns2012011:https    ESTABLISHED
  TCP    [2600:1009:b011:fe70:e912:db9:7fd9:a844]:49359  bn1wns1011320:https    ESTABLISHED
```

Figure 1-20: Netstat Reporting Active Connections

The final command, unique to Windows systems, is the network shell (NETSH) command. This command reveals many things about network connections and configurations on the Windows computer. It provides extensive information about the wireless adapter and connection when in WLAN mode. Unlike many other Command Prompt commands, the NETSH command has different modes with difference commands in those modes. For example, you can execute many commands specific to WLANs when in the WLAN mode, accomplished with the NETSH command followed by the embedded WLAN command. Next execute the ? command to view options as shown in Figure 1.21.

```
C:\Windows\System32\cmd.exe - netsh
namespace       - Changes to the 'netsh namespace' context.
nap             - Changes to the 'netsh nap' context.
netio           - Changes to the 'netsh netio' context.
offline         - Sets the current mode to offline.
online          - Sets the current mode to online.
p2p             - Changes to the 'netsh p2p' context.
popd            - Pops a context from the stack.
pushd           - Pushes current context on stack.
quit            - Exits the program.
ras             - Changes to the 'netsh ras' context.
rpc             - Changes to the 'netsh rpc' context.
set             - Updates configuration settings.
show            - Displays information.
trace           - Changes to the 'netsh trace' context.
unalias         - Deletes an alias.
wcn             - Changes to the 'netsh wcn' context.
wfp             - Changes to the 'netsh wfp' context.
winhttp         - Changes to the 'netsh winhttp' context.
winsock         - Changes to the 'netsh winsock' context.
wlan            - Changes to the 'netsh wlan' context.

Commands in this context:
?               - Displays a list of commands.
add             - Adds a configuration entry to a table.
connect         - Connects to a wireless network.
delete          - Deletes a configuration entry from a table.
disconnect      - Disconnects from a wireless network.
dump            - Displays a configuration script.
export          - Saves WLAN profiles to XML files.
help            - Displays a list of commands.
refresh         - Refresh hosted network settings.
reportissues    - Generate WLAN smart trace report.
set             - Sets configuration information.
show            - Displays information.
start           - Start hosted network.
stop            - Stop hosted network.

To view help for a command, type the command, followed by a space, and then
 type ?.

netsh wlan>
```

Figure 1-21: The NETSH WLAN Mode of Operation

Important NETSH WLAN commands include:

- SHOW INTERFACES
- SHOW NETWORKS
- SHOW DRIVERS
- SHOW PROFILES

EXAM MOMENT: You should take some time to explore the difference `NETSH WLAN` command available and the output they generate. These commands are useful for troubleshooting WLAN configuration issues. Specifically, familiarize yourself with the output of the `SHOW INTERFACES`, `SHOW NETWORKS`, `SHOW DRIVERS`, and `SHOW PROFILES` commands.

Additional netsh commands of interest include:

- NETSH WLAN SHOW ALL
- NETSH INTERFACES IPV4 SHOW ADDRESSES
- NETSH INTERFACES IPV4 SHOW IPSTATS

- NETSH INTERFACES IPV4 SHOW CONFIG
- NETSH INTERFACES IPV4 SHOW ICMPSTATS
- NETSH INTERFACES IPV4 SHOW TCPSTATS
- NETSH INTERFACES IPV4 SHOW TCPCONNECTIONS

The netsh shell is a powerful interface for viewing and configuring network settings and statistics and is very useful to the network troubleshooter.

```
C:\Windows\System32\cmd.exe
C:\Windows\System32>netsh wlan show drivers

Interface name: Wi-Fi

    Driver                  : Intel(R) Dual Band Wireless-AC 7260
    Vendor                  : Intel Corporation
    Provider                : Intel
    Date                    : 5/26/2014
    Version                 : 17.0.3.3
    INF file                : C:\windows\INF\oem14.inf
    Files                   : 3 total
                              C:\windows\system32\DRIVERS\Netwbw02.sys
                              C:\windows\system32\DRIVERS\Netwfw02.dat
                              C:\windows\system32\drivers\vwifibus.sys
    Type                    : Native Wi-Fi Driver
    Radio types supported   : 802.11b 802.11g 802.11n 802.11a 802.11ac
    FIPS 140-2 mode supported : Yes
    802.11w Management Frame Protection supported : Yes
    Hosted network supported  : Yes
    Authentication and cipher supported in infrastructure mode:
                              Open            None
                              Open            WEP-40bit
                              Open            WEP-104bit
                              Open            WEP
                              WPA-Enterprise  TKIP
                              WPA-Enterprise  CCMP
                              WPA-Personal    TKIP
                              WPA-Personal    CCMP
                              WPA2-Enterprise TKIP
                              WPA2-Enterprise CCMP
                              WPA2-Personal   TKIP
                              WPA2-Personal   CCMP
                              Open            Vendor defined
    Authentication and cipher supported in ad-hoc mode:
                              Open            None
                              Open            WEP-40bit
                              Open            WEP-104bit
                              Open            WEP
                              WPA2-Personal   CCMP
    IHV service present     : Yes
    IHV adapter OUI         : [00 80 86], type: [00]
    IHV extensibility DLL path: C:\windows\System32\IWMSSvc.dll
    IHV UI extensibility CLSID: {1bf6cb2d-2ae0-4879-a7aa-a75834fbd0e3}
    IHV diagnostics CLSID   : {00000000-0000-0000-0000-000000000000}

C:\Windows\System32>
```

Figure 1-22: NETSH WLAN SHOW DRIVERS Output

The `NETSH WLAN SHOW DRIVERS` command reveals the driver files used, such as netwbw02.sys, netwfw02.dat, and vwifibus.sys files shown in Figure 1.22. Additionally, it reveals the security methods provided by the adapters, the radio PHYs supported and other features of importance like Management Frame Protection (MFP) and driver versions.

```
C:\Windows\System32\cmd.exe
C:\Windows\System32>netsh wlan show profiles

Profiles on interface Wi-Fi:

Group policy profiles (read only)
---------------------------------
    <None>

User profiles
-------------
    All User Profile     : OFFICE24
    All User Profile     : Verizon-4GLTE-BRV-B1BD
    All User Profile     : OFFICE5

C:\Windows\System32>
```

Figure 1-23: NETSH WLAN SHOW PROFILES Output

The `NETSH WLAN SHOW PROFILES` command is useful for evaluating the profiles installed and configured on the local machine. These profiles include pre-shared key

(PSK) passphrases, when WPA- or WPA2-Personal is used in the profiles. When the name of a specific profile is provided, such as `NETSH WLAN SHOW PROFILES NAME="OFFICE24"`, the output will reveal additional information about the specified profiles; however, PSK passphrases are not shown in the output. If you want to see the stored key, you can add the `KEY=clear` parameter to the command.

```
C:\Windows\System32\cmd.exe
C:\Windows\System32>netsh wlan show interfaces

There is 1 interface on the system:

    Name                   : Wi-Fi
    Description            : Intel(R) Dual Band Wireless-AC 7260
    GUID                   : f2fa55b9-b844-42ca-98e9-458404cda228
    Physical address       : 28:b2:bd:19:c7:b0
    State                  : connected
    SSID                   : Verizon-4GLTE-BRV-B1BD
    BSSID                  : 00:15:ff:91:b1:bd
    Network type           : Infrastructure
    Radio type             : 802.11n
    Authentication         : WPA2-Personal
    Cipher                 : CCMP
    Connection mode        : Profile
    Channel                : 11
    Receive rate (Mbps)    : 72
    Transmit rate (Mbps)   : 72
    Signal                 : 99%
    Profile                : Verizon-4GLTE-BRV-B1BD

    Hosted network status  : Not started

C:\Windows\System32>_
```

Figure 1-24: NETSH WLAN SHOW INTERFACES Output

The `NETSH WLAN SHOW INTERFACES` command reveals the current profiles operation, including the authentication and key management (AKM) protocol (listed as Authentication), the encryption method (listed as Cipher and CCMP, which means AES is used), the channel, the signal strength, and data rates (including transmit and receive rates, which may vary and is a useful measurement). Since this is a WLAN client, the transmit data rate would be the uplink rate and the receive data rate would be the downlink rate.

```
C:\Windows\System32\cmd.exe
C:\Windows\System32>netsh wlan show networks

Interface name : Wi-Fi
There are 2 networks currently visible.

SSID 1 : Verizon-4GLTE-BRV-B1BD
    Network type            : Infrastructure
    Authentication          : WPA2-Personal
    Encryption              : CCMP

SSID 2 :
    Network type            : Infrastructure
    Authentication          : Open
    Encryption              : WEP

C:\Windows\System32>_
```

Figure 1-25: NETSH WLAN SHOW NETWORKS Output

The `NETSH WLAN SHOW NETWORKS` command provide information about visible networks that the client STA (station) can see. To get more or alternate information about a network, use the `NETSH WLAN SHOW NETWORKS MODE=BSSID` command.

Exercise 1

In this exercise, you will review various troubleshooting methodologies. Given that these methodologies are provided online, no demonstration video is available at the CWNPTV YouTube channel for Exercise 1.

(a) Read the following article on troubleshooting methodology and answer the questions below.

Microsoft's Troubleshooting Methodology

https://technet.microsoft.com/en-us/library/cc786052(v=ws.10).aspx

Question 1: What would be the next step of your troubleshooting methodology in case you are not able to reproduce the problem?

Question 2: List the methods that you can use to collect information about the problem?

Question 3: How does creating an action plan as a part of your troubleshooting methodology help in resolving the problem?

(b) Read the following article on troubleshooting methodology and answer the questions below.

Cisco's Troubleshooting Methodology

http://www.cisco.com/en/US/docs/internetworking/troubleshooting/guide/tr1901.html

Question 1: Briefly list each step of the troubleshooting methodology as mentioned in the above article?

Question 2: List the top five considerations that you would need to take to prepare for network failure?

Question 3: Give three reasons why documenting problems is essential?

(c): Read the following article on troubleshooting methodology and answer the questions below.

HP's Troubleshooting Methodology

https://redmondmag.com/articles/2006/02/01/troubleshooting—the-hp-way.aspx

Question 1: List and briefly explain the troubleshooting methodology followed at HP?

Question 2: List the top 10 reasons for a system failure?

Question 3: What can you do to minimize the reoccurrence of a problem?

Answer (a)

Answer 1: What would be the next step of your troubleshooting methodology if you are not able to reproduce the problem?

Typically, when a problem is identified, you should attempt to replicate the steps that were performed up to the time when the problem occurred. However, there might be instances where you are not able to replicate the steps, and therefore not able to replicate the problem. What is your next step to troubleshoot such a problem? Troubleshooting such a problem can be difficult, and the next phase of isolating the problem can be tedious or, in some cases, impossible to perform. Therefore, the best way to troubleshoot a problem that cannot be replicated is:

- Gather as much information as you can, about the problem. This will enable you to write additional code, implement an improved event tracking method, or develop a solution for the problem without replicating it.
- Implement a detailed event tracking method. This will enable you to back track the steps that were performed till the step at which the problem occurred.
- Ask the users to watch out for the problem if it occurs again, and if possible, document the steps that they were performing when the problem occurred.
- Develop additional code that can be implemented as a service patch or an update that can identify the problem if it occurs again.

Answer 2: List the methods that you can use to collect information about the problem?

When a problem occurs, an essential requirement is to collect as much relevant information about the problem as possible. Here are some of the methods of collecting information:

- Interview the user who reported the problem, and create a document with the details of the steps he/she was performing when the problem occurred. Record all minute details, such as was the Web page refreshed, or did the user accidently click a button displayed on the screen.
- Create a questionnaire with relevant questions, and share it with the user(s) who reported the problem. The questionnaire should have specific and closed-ended questions.
- Ask the users to take screen shots of the error message displayed on the screen when the problem occurred. However, if the problem is behavioral, then you can use the questionnaire with specific and closed-ended questions to gather information. Examples of specific and closed-ended questions can be:
    - Did you click the Refresh button?
    - Which link did you click?
    - At what time did the problem occur?

- Analyze the log files that were generated by the system or the application at the time the problem occurred. Most applications and operating systems generate log files and log events that include event or problem details. These details can be extremely helpful in understanding and replicating the problem.

Answer 3: How does creating an action plan as a part of your troubleshooting methodology help in resolving the problem?

One of the steps in troubleshooting a problem is to create an action plan to resolve the problem and avoid its reoccurrence, if possible. Creating an action plan involves identifying and listing the subsequent steps or processes you will perform to resolve the identified problem. Since in a troubleshooting process the next steps depends on the outcome of the previous step, an action plan keeps you on track and ensures that you do not waste time and effort in performing irrelevant steps. Also, having an action plan ensures that all the steps are documented and can be used for future reference.

Answer (b)

Answer 1: Briefly list each step of the troubleshooting methodology as mentioned in the above article?

The troubleshooting methodology discussed in this article comprises the following steps:

1. *Create a problem statement:* When you have a wireless network problem or a network problem in general, start with analyzing the problem and create a problem statement. The problem statement should include a set of symptoms available and the probable causes of these symptoms.
2. *Collect the facts to isolate the problem:* After you have analyzed the problem, gather facts and information about the problem. You can use various methods to collect information such as error logs, error messages, protocol analyzer traces, and to ask questions of affected users, network administrators, and other people who might be able to share information about the problem.
3. *Identify possible causes:* On the basis of your analysis and the information gathered, identify the possible causes that can result in the problem you are trying to troubleshoot. This step will enable you to identify most of the probable causes, eliminate the causes that are not related to the problem at hand, and to narrow down the probable causes of the problem.
4. *Create and implement an action plan:* The fourth step in this troubleshooting methodology is to create an action plan to troubleshoot the problem by manipulating one probable cause or one variable at a time. This step would ensure that you troubleshoot the problem in a systematic manner.
5. *Collect results:* Every time you change a variable to resolve the problem, make sure that you collect the results that need to be analyzed as the next step.
6. *Analyze the results:* After you have implemented the action plan and collected the results, every time you change a variable, analyze the results to understand if the problem has been resolved. If the problem has not been resolved, repeat the

process by changing a different variable.

Answer 2: List the top five considerations that you would need to prepare for network failure?

The top five considerations to prepare for a network failure are:

1. Prepare a detailed and accurate logical and physical map of your network. The physical map would include the physical location of all network devices and how these devices are connected. The logical map comprises network addresses, network numbers, and subnets. Share this list with the concerned teams and stakeholders.
2. Prepare a list of all network protocols used and implemented in your network. Also, this list should include all network numbers, subnets, IP addresses, and zones, associated with each protocol. This list should also include information about all the protocols that are routed, with their complete router configuration.
3. Prepare a list of all the protocols that are bridged, along with the complete configuration.
4. Prepare a list of all the points of contact to external networks, including any connections to the Internet. This list should also include all the routing protocols used.
5. Establish, maintain, and document a baseline for your network and its performance. You need to have a documented baseline for your network's performance at different times during business and off-business hours. This will help you monitor and compare the network performances with the baselined performance.

Answer 3: Give three reasons why documenting problems is essential?

Documentation is an essential part of any process, whether it is software product development, network implementation, or troubleshooting. For a troubleshooting process, documenting a problem is essential for the following reasons:

- Documenting a problem ensures that you are on track while troubleshooting the problem, and that you do not deviate from the problem at hand. While you document a problem, you also document the symptoms and probable causes that might have resulted in the problem. This documentation gives you a clear picture of what the problem is and what probable causes can be the reason of this problem on the basis of the symptoms. Therefore, documentation provides a more systematic approach to troubleshoot problems.
- Documenting a problem is not limited to just documenting the trouble and its symptoms. You also document the probable causes, the steps taken to resolve the problem, result of each step, and the final solution to the problem. All this documentation serves as a ready reference for any similar problem, and reduces the amount of time, effort, cost, and rework that would be spent on a similar problem in future.
- Documenting a problem requires that all details related to the problem are

recorded. This ensures that while you are attempting to resolve a problem, all facts and figures are available so that you can make an informed decision on how to resolve the problem, and it helps you select the best solution among the available alternatives.

Answer (c)

https://redmondmag.com/articles/2006/02/01/troubleshooting—the-hp-way.aspx

Answer 1: List and briefly explain the troubleshooting methodology followed at HP?

The troubleshooting methodology followed at HP comprises the following steps:

1. Gather data: The first step is to gather data for the identified problem. Data can be gathered using surveys and questionnaires from error logs and helpdesk tickets and by conducting interviews of the people who reported the problem. After the data is collected and collated it is analyzed to identify the potential cause of the identified problem.
2. Evaluate and analyze data: The second step is to evaluate and analyze the data gathered as the part of the first step, and then try to isolate the potential cause of the problem. During this analysis, identify the most probable cause of the problem and eliminate all non-probable causes.
3. Develop an optimized action plan: The third step involves creating an action plan to resolve the problem. The action plan comprises the three most-likely scenarios that might have caused the problem and the steps that will be taken in each scenario to resolve it.
4. Execute the action plan: The fourth step is to execute and implement the action plan. This involves executing the steps to resolve the problem, as identified for each scenario, in the action plan.
5. Determine whether the problem is solved: The fifth step is to determine whether the problem is resolved on the basis of the result of the executed action plan. If the problem is resolved, document the steps and the measures taken to reproduce and resolve the problem.
6. Preventive measures: The last step of the troubleshooting process involves identifying and implementing measures to ensure that the problem does not happen again. At times problems occur due to simple mistakes such as improper cabling or incorrect drivers. The last step of the troubleshooting process also involves creating proper documentation of the problem, analysis of the data gathered, an action plan, probable scenarios, and the steps taken to resolve the problem.

Answer 2: List the top five reasons for a system failure?

A system failure can happen due to the following:

1. The system’s ROM and the drivers have not been updated.
2. The Network Interface Cards (NICs) have not been updated.

3. There is a mismatch between the driver and the hardware in the system.
4. The components of a server have been dislodged during movement or are non-functional.
5. The system maintenance might have caused the problem.

Answer 3: What can you do to ensure that the problem does not reoccur?

To ensure that a problem you have recently resolved does not occur again, identify the preventive measures during the troubleshooting process, and implement these measures as soon as the problem is resolved. For example, if the problem has been caused by mishandling of cables, then educate the team in cable handling procedures, by organizing training or sending an email memo with the required cable handling details.

Also, it is essential that the problem and its resolution, along with analysis of the probable causes and the steps taken to resolve the problem, are accurately documented for future reference.

Chapter Summary

In this chapter, you explored the various troubleshooting methodologies suggested by vendors and the specific methodology recommended by CWNP. You learned about the OSI model as it applies to troubleshooting and the many tools used by the WLAN professional in his or her work. In the next chapter, you will begin to explore the foundational knowledge required to use these troubleshooting processes and tools to resolve real-world issues.

Review Questions

1. When troubleshooting a Wi-Fi problem, what is the first step that should be taken?
    a. Document the solution
    b. Determine probable causes
    c. Identify the problem
    d. Develop a theory
2. Why is it important to document incidents and the solutions discovered when troubleshooting?
    a. Documentation ensures the problem will not occur again.
    b. Documentation can be used to troubleshoot similar problems later.
    c. Documentation helps to ensure you understand why the problem occurred.
    d. Documentation is required for the proper arbitration of 802.11 networks.
3. What is the primary benefit of a troubleshooting methodology?
    a. It ensures that the problem is resolved according to vendor requirements.
    b. It ensures that the problem is resolved and will not occur again.
    c. It ensures that the right problem is resolved and time is not wasted.
    d. It ensures that the analyst cannot be blamed for the problem.
4. What protocol suite implements the OSI model and is in use in modern networks?
    a. TCP/IP
    b. IPX/SPX
    c. 802.11
    d. No protocol implements the OSI model
5. The 802.11 standard defines the functions described in what two layers of the OSI model?
    a. Layers 6 and 7
    b. Layers 1 and 2
    c. Network and Data Link Layers
    d. Transport and Network Layers
6. At what layer of the OSI model does the IP protocol operate?
    a. Layer 4
    b. Network Layer
    c. Layer 2

d. Data Link Layer

7. You are tasked with troubleshooting a problem related to the frames used in 802.11 networks. When analyzing frames, what layer of the OSI model is being evaluated?

   a. Layer 2
   b. Network Layer
   c. Layer 3
   d. Physical Layer

8. In a WLAN, what layer performs the transmission of bits through modulation on RF waves?

   a. Data Link Layer
   b. Layer 3
   c. Session Layer
   d. Layer 1

9. As data moves down the OSI model layers, bits are added for management and transmission of the data. What is this process called?

   a. Encapsulation
   b. Encryption
   c. Interpretation
   d. Modulation

10. You must resolve problems with routing protocols on the network infrastructure. What layer of the OSI model are you troubleshooting?

    a. Layer 1
    b. Layer 6
    c. Layer 4
    d. Layer 3

11. What kind of expertise is created by ensuring that all problems are documented with their solutions over time?

    a. Grammar
    b. Experiential
    c. Classroom learning
    d. Referential

12. You have modified a configuration setting in an attempt to resolve a problem. The problem was not resolved. What is typically considered the proper next action?

a. Try the next configuration setting that may help to resolve the problem.
b. Report the problem to someone else.
c. Inform the user that the problem cannot be resolved.
d. Return the system to the previous configuration before attempting another change.

13. What helps the analyst remember to ask the right questions?
    a. A troubleshooting methodology
    b. A spectrum analyzer
    c. A protocol analyzer
    d. The netsh command
14. What Windows command shows the cipher suite used in a wireless connection?
    a. IPCONFIG
    b. PING
    c. TRACERT
    d. NETSH
15. When executing a PING command, what packet type is transferred to the target?
    a. UDP
    b. TCP
    c. ICMP
    d. SMTP
16. What determines the size of the PING response?
    a. The data size in the ECHO message
    b. The length field in the IP header
    c. The duration field in the MAC header
    d. The –t switch at the Windows Command Prompt
17. What is the primary difference between PING and PATHPING?
    a. PING is used to determine the IP addresses of the routers along the path and PATHPING is not.
    b. PATHPING computes statistics for each hop along the route and PING does not.
    c. PING sends HTTP GET requests to the target and PATHPING uses only ICMP.
    d. PATHPING sends HTTP GET requests to the target and PING uses only ICMP.

18. You execute the TRACERT command against the target IP address of 192.168.12.45. No VPN or other tunnel connections are in use. What kind of routers will be reported in the trace results?
    a. Internet routers
    b. University routers
    c. Internal routers
    d. External routers
19. You are seeking to view the RF activity in an area where a WLAN has been deployed. What is the appropriate tool?
    a. Protocol analyzer
    b. NETSH
    c. CAT5 cable tester
    d. Spectrum analyzer
20. You wish to view the different 802.11 WLANs in an area and see the capabilities of those WLANs. What tool will work best?
    a. Protocol analyzer
    b. Spectrum analyzer
    c. NETSH
    d. PING
21. What NETSH WLAN mode command will show the security features supported by the WLAN adapter?
    a. SHOW INTERFACES
    b. SHOW NETWORKS
    c. SHOW DRIVERS
    d. SHOW PROFILES
22. You have executed a NETSH command that shows the signal strength of the current WLAN connection at 80%. What command was executed?
    a. NETSH WLAN SHOW INTERFACES
    b. NETSH WLAN SHOW NETWORKS
    c. NETSH WLAN SHOW DRIVERS
    d. NETSH WLAN SHOW PROFILES
23. You wish to view all of the stored WLAN configurations on a Windows computer. What command will reveal this information?
    a. IPCONFIG

b. NETSH WLAN SHOW PROFILES

c. NETSTATS

d. NSLOOKUP

24. You purchased a 2.4 GHz and 5 GHz spectrum analyzer the year before 802.11n was ratified. What PHYs that are part of 802.11, according to your CWNA and CWAP knowledge can be viewed with this spectrum analyzer?

    a. ERP, HR/DSSS, DSSS and FHSS

    b. OFDM and ERP

    c. HR/DSSS, DSSS and FHSS

    d. All PHYs that operate in the supported frequency bands

25. You wish to discover non-Wi-Fi interfering devices. What tool should be used?

    a. Protocol analyzer

    b. Spectrum analyzer

    c. Cable tester

    d. Throughput tester

Review Question Answers

1. **C** is correct. The first step in any troubleshooting process is to identify or verify the problem. Without this step, the analyst may be troubleshooting a non-existing issue.
2. **B** is correct. When analysts document problems and solutions, the resulting documentation becomes a wealth of information for later troubleshooting processes. This documentation should be searched as new problems are encountered to see if a solution already exists.
3. **C** is correct. When a troubleshooting methodology is used, it begins with problem identification and, therefore, ensures the right problem is resolved. Additionally, time is not wasted because actions are not taken against the wrong issues.
4. **D** is correct. The OSI model is just that, a model. No actively used protocol implements the OSI model though all known protocols are related to it.
5. **B** is correct. Layer 1 is the PHY and Layer 2 is the MAC, both defined in the 802.11 standard.
6. **B** is correct. The Internet Protocol (IP) is a Layer 3 or Network Layer protocol.
7. **A** is correct. Frames are encapsulated at Layer 2 (Data Link Layer) of the OSI model. The MAC sublayer of Layer 2, specifically, is where 802.11 frames are created.
8. **D** is correct. Layer 1 is the Physical Layer or the PHY. The PHY is responsible for modulating bits onto the RF medium.
9. **A** is correct. Encapsulation is the process of adding bits to the front and back of upper layer data for transmission on the LAN and possibly the WAN. The prepended bits are considered the header of the layer. Any appended bits are typically integrity check bits.
10. **D** is correct. Routing is configured at Layer 3. Many routers decapsulate only to Layer 3 and no more. Some look at higher layers, but routing is a Layer 3 operations.
11. **B** is correct. Experiential expertise is developed through documenting problems and their solutions. Even if they are only documented in the mind, they must be considered with lessons learned to build expertise over time.
12. **D** is correct. Given that the configuration change did not resolve the problem, it is typically best to return the system to the previous configuration. This is particularly true in enterprise environments where standard configurations are used.
13. **A** is correct. A troubleshooting methodology helps the analyst remember to ask the right questions as it provides steps in the process requiring information gathering.
14. **D** is correct. NETSH WLAN SHOW INTERFACES will reveal the cipher suite used in the current connection. NETSH WLAN SHOW DRIVERS will show the

supported cipher suites by the adapter, but not the one used in a wireless connection.

15. **C** is correct. ICMP ECHO messages are sent to the target, and ICMP ECHO REPLY messages are returned to the source.
16. **A** is correct. The data size in the ECHO message determines the size of the response because the response simply duplicates this data in the ECHO REPLY message.
17. **B** is correct. PATHPING determines the IP addresses of the routers along the path and computes statistics for each hop along the route. PING does not perform either function.
18. **C** is correct. Given that a private IP address is used, the command will only reveal internal routers. Private addresses are not routable on the Internet.
19. **D** is correct. A spectrum analyzer shows RF activity (energy) detectable at a location.
20. **A** is correct. A protocol analyzer will show the WLANs in an area.
21. **C** is correct. The SHOW PROFILES sub-command reveals all supported security modes of the adapter.
22. **A** is correct. The SHOW INTERFACES subcommand shows the current connection and the signal strength of that connection as reported to Windows by the drivers.
23. **B** is correct. The NETSH WLAN SHOW PROFILES command will show all stored configurations (profiles) on the Windows client.
24. **D** is correct. A spectrum analyzer reports on raw RF energy detected (though it may integrate with a WLAN adapter to show more information) and will work with all PHYs in the frequency bands supported by the spectrum analyzer regardless of when the PHYs were released.
25. **B** is correct. A spectrum analyzer is best for discovering non-Wi-Fi interfering devices as it shows all RF energy in the operating area.

Chapter 2:

802.11 Communications

Objectives

2.1 Explain the 802.11 communications processes including authentication, association, security negotiation, frame transmission, and factors impacting data rates.

2.2 Understand the different WLAN architectures in use and their impact on performance and operations.

If you are going to analyze or troubleshoot any technology, you must first understand the details of its operations. This chapter is all about WLAN operations. It will include some review from your CWNA studies, but will also go deeper in important areas for the WLAN analyst. Remember that all of your CWNA knowledge is assumed for the professional level CWNP certifications (CWAP, CWDP, and CWSP). Therefore, it is important that you review key areas. You may want to use the CWNA study guide to brush up on foundational WLAN topics that you may be weak in as you study CWAP and before you take the CWAP exam.

This chapter begins with a terminology review to ensure you understand the language of network communications. Then you will explore 802.11 communications in-depth, including factors that impact data rates. Finally, you will review and go deeper into different WLAN architectures, as each can greatly impact the troubleshooting and analysis processes.

Terminology Review

The first terms I will cover relate to the conceptualization of data before it is transmitted onto the wire or RF medium. These terms are frames, packets, and datagrams. Figure 2.1 illustrates the OSI layers associated with these terms. As you can see, segments, packets, and datagrams reside at Layers 3 and 4 of the OSI model, and these objects are framed at Layer 2. At Layer 4 you work with segments (TCP) and datagrams (UDP). At Layer 3 you work with packets (that confusingly are also sometimes called datagrams).

Figure 2-1: OSI Layers Related to Common Terminology

What is the difference between a segment and a datagram at Layer 4? In many cases, they are incorrectly used interchangeably. The technical difference is that segments are connection-oriented communications that use TCP, and datagrams are UDP-based connectionless communications. Here I will speak only of segments to keep the discussion simple, but know that network traffic is generally always a mix of TCP and UDP.

Whatever data is communicated, Layer 4—the Transport Layer—usually breaks the data into TCP segments. These segments are sent to Layer 3 and become Internet Protocol (IP) packets. At this time, the destination IP address is attached to the data, and it is ready to be placed on the wire or RF medium using the Layer 2 and Layer 1 technologies implemented on this specific network. When these packets are passed on to Layer 2, they become frames.

What is a frame? Technically, a frame is the exact same thing as a packet or a TCP segment—a series of well-defined 1s and 0s. However, we usually think about frames at a higher level. At the higher level frames are collections of data and management information needed to carry the data from one place to another on the network. Different networking technologies use different frame formats, but all 802-based networks use framing concepts.

One way to conceptualize this is to think about the original data, which is the intentional information being sent across the network. Imagine this data is a Microsoft Excel spreadsheet being copied to a file share on the network. In order for the data to be transmitted across the network, it must be broken into manageable chunks known as packets. This has already happened by the time the Excel spreadsheet has reached Layer 3 of the OSI model. While the original spreadsheet was actually millions of 1s and 0s, it has now been broken down into chunks that are each just a few thousand 1s and 0s. The 1s and 0s that make up the data have been prefixed and suffixed with more information that is used to manage the transfer of the data. This information includes the destination IP address, error checking information, and more. The final step, at Layer 2, is to add the frame information, that includes a frame header including the destination and source MAC addresses. At this point an entire frame now exists. Remember, this frame is a series of 1s and 0s that started as an Excel spreadsheet, but it is now a chunk of an Excel spreadsheet (assuming the spreadsheet is larger than the typical 1500 bytes) with network management information added.

Bits, Bytes, and Octets

In the previous paragraph I stated that a frame is a series of well-defined 1s and 0s. We looked at the process of breaking a large piece of data into smaller, more manageable pieces of data for network transmission. Ultimately, the smallest element that can be transmitted on any network is a bit. A bit is a single value equal to 1 or 0. When you group these bits together, they form bytes. An 8-bit byte is the most commonly-referenced byte and is the base of most networking measurements. The 8-bit byte is specifically called an octet in most networking standards, even though vendors and networking professionals lean more toward the term byte. For example, one kilobyte is 1024 bytes, and one megabyte is 1,048,576 bytes. You will often see these numbers rounded to say that 1000 bytes is a kilobyte, or 1,000,000 bytes is a megabyte. The term octet could also be used in these statements; for example, one kilobyte is 1024 octets. These numbers relate to storage. When dealing with network throughput, 1 Mbps is 1 million bits per second and not 1,048,576 bits per second. This has caused some confusion over time, but network throughput is measured in rounded numbers like 1,000, 1,000,000, and 1,000,000,000.

Note: **This variation of numbering methods gets even more confusing when you consider the difference between Mbps and MBps. The first is megabits per second, while the second is megabytes per second. To calculate MBps, divide Mbps by 8. For example, 10 Mbps is roughly 1.2 MBps. The difference is that Mbps uses Information System of Units and MBps uses binary units. Information System of Units is purely a count of the bits per second. Binary units use exponents (powers of two) like hard drives in computers.**

You might be wondering how a simple bit, or even a byte, can represent anything. This is an important concept to understand. Otherwise, you may have difficulty truly understanding how a network works and thus how to analyze it. Let us consider just an 8-bit byte (also called an octet). If you have one bit, it can represent any two pieces of information. The 1 can represent one piece of information, and the 0 can represent another. When you have two bits, you can represent four pieces of information. You have the values 00, 01, 10, and 11 available to use as representative elements. When you have three bits, you can represent eight pieces of information and for every bit you add, you double the amount of information that can be represented. This means that an 8-bit byte can represent 256 elements.

Standard mapping systems exist that map a numeric value to a piece of information. For example, the ASCII system maps numbers to characters. Since we can represent up to 256 elements with an 8-bit byte, we can represent 256 ASCII codes, as well. A quick Internet search will reveal a number of sites that provide tables of ASCII codes. For example, the ASCII codes for the term “802.11” are 56, 48, 50, 46, 49, and 49 in decimal form. Since we can represent any number from 0 to 255 with an 8-bit byte, we can represent these numbers, as well. Table 2.1 shows a mapping of characters to ASCII decimal codes to 8-bit bytes.

In order for all this to work, both the sender and the receiver of the bytes must agree on how the bytes will be translated or interpreted. For information to be meaningful, both parties must agree to the meaning. Human languages are the same. If I speak a language that has meaning to me, but you do not understand that language, it is meaningless to you and communication has not occurred. When a computer receives information that it cannot interpret to be anything meaningful, it either sees it as noise or corrupted data.

Character	ASCII Decimal Codes	8-Bit Byte
8	56	00111000
0	48	00110000
2	50	00110010
.	46	00101110
1	49	00110001
1	49	00110001

Table 2.1: Representing Characters with Bytes

To understand how the binary bits in an octet, are translated to the ASCII decimal codes, consider Table 2.2. Here you can see that the first bit (the right-most bit) represents the number 1, the second bit represents the number 2, the third bit represents the number 4, and so on. The example in the table is 00110001. Where there is a 0, the bit is considered to be off. Where there is a 1, the bit is on. We add up the total values in the translated row, based on the represented number for each bit, and find the result of 49 because we only count the values where the bit is equal to 1. This is how the binary octet of 00110001 represents the ASCII decimal code of 49, which represents the number 1 in the ASCII tables.

Bit Position	8	7	6	5	4	3	2	1
Represented decimal number	128	64	32	16	8	4	2	1
Example binary number	0	0	1	1	0	0	0	1
Translated	0	0	32	16	0	0	0	1

Table 2.2: Converting Bytes to Decimal Values

So why do bits matter? When performing protocol analysis, you are using a tool that captures the 802.11 frames and decodes them. How does the tool know how to decode the bits in the frames? They are all defined in the 802.11 standard document. Chapter 3

explores 802.11 frames in-depth. For now, just know that 802.11 frames include a series of well-defined bits that represent meaningful information for the processing of data and BSS management.

MAC & PHY

Two other terms that are used heavily in the networking knowledge domain are MAC and PHY. MAC is an acronym for medium access control. By now, I hope you have often heard that within the Data Link Layer (Layer 2) of the OSI model, there are two sublayers known as the Logical Link Control sublayer and the Medium Access Control sublayer. The Logical Link Control sublayer is a shared sublayer, also known as 802.2, among all 802 standards such as 802.3 (Ethernet) and 802.11 (wireless).

PHY is an abbreviation for the Physical layer of the OSI model or a specific networking implementation. Phrases such as “802.11 PHY” or “that takes place at the PHY” refer to Layer 1 and the processes that occur at this layer. In order to provide for different physical technologies (DSSS, FHSS, OFDM, HT, VHT, etc.) in 802.11, the PHY is divided into two sublayers called the Physical Medium Dependent (PMD) and the Physical Layer Convergence Protocol (PLCP).

PMD and PLCP

The Physical Medium Dependent (PMD) is the portion of the 802.11 PHY that is responsible for actually transmitting the information using some form of modulation, such as BPSK or QAM. The Physical Layer Convergence Protocol (PLCP) is responsible for abstracting the PMD from the Data Link Layer protocols and abstracting the Data Link Layer protocols from the PMD. You might say that it acts as a translator or coordinator between the real physical medium dependent (PMD) and the MAC processes.

> **EXAM MOMENT:** The details of how BPSK and QAM work are beyond the scope of the CWAP exam. It is enough for you to know that there are different modulations used at different data rates and with different PHYs and the names of these modulation techniques. You are not required to describe the modulation in technical terms as this is the role of a WLAN chipset designer or programmer and not a WLAN troubleshooter.

The IEEE 802.11 standard and amendments that specify a PHY each provide different PMDs. The modulation techniques make up these different PMDs in large part. For example, there is one PMD for FHSS (using GPSK) and another for DSSS (using either BPSK or QPSK). The PMDs may add additional functions such as the scrambling of the data units before transmission. The MAC layer is mostly the same for all of the current 802.11 PHYs in production, but there are features peculiar to the PHY that will vary, such as ERP protection mechanisms for the ERP PHY. Additionally, the WLAN MAC standard offers optional features, like Quality of Service, that are not likely to be found with older PHY implementations or hardware.

Data-Link Layer and Logical Link (LLC) Sublayer

The Data Link Layer of the OSI model, like the Physical Layer, is divided into two sublayers. These sublayers in 802.11 systems are the 802.2 Logical Link Control (LLC)

sublayer that is the same for all 802-based networks, and the Media Access Control (MAC) sublayer that is the same for all current 802.11-based technologies. Figure 2.2 provides a visual representation of both the Physical and Data Link layers and how they are separated into sublayers. While IEEE 802 defines LLC for all its LAN types, including Ethernet, Ethernet is allowed to skip the LLC, and IP over Ethernet almost never uses LLC.

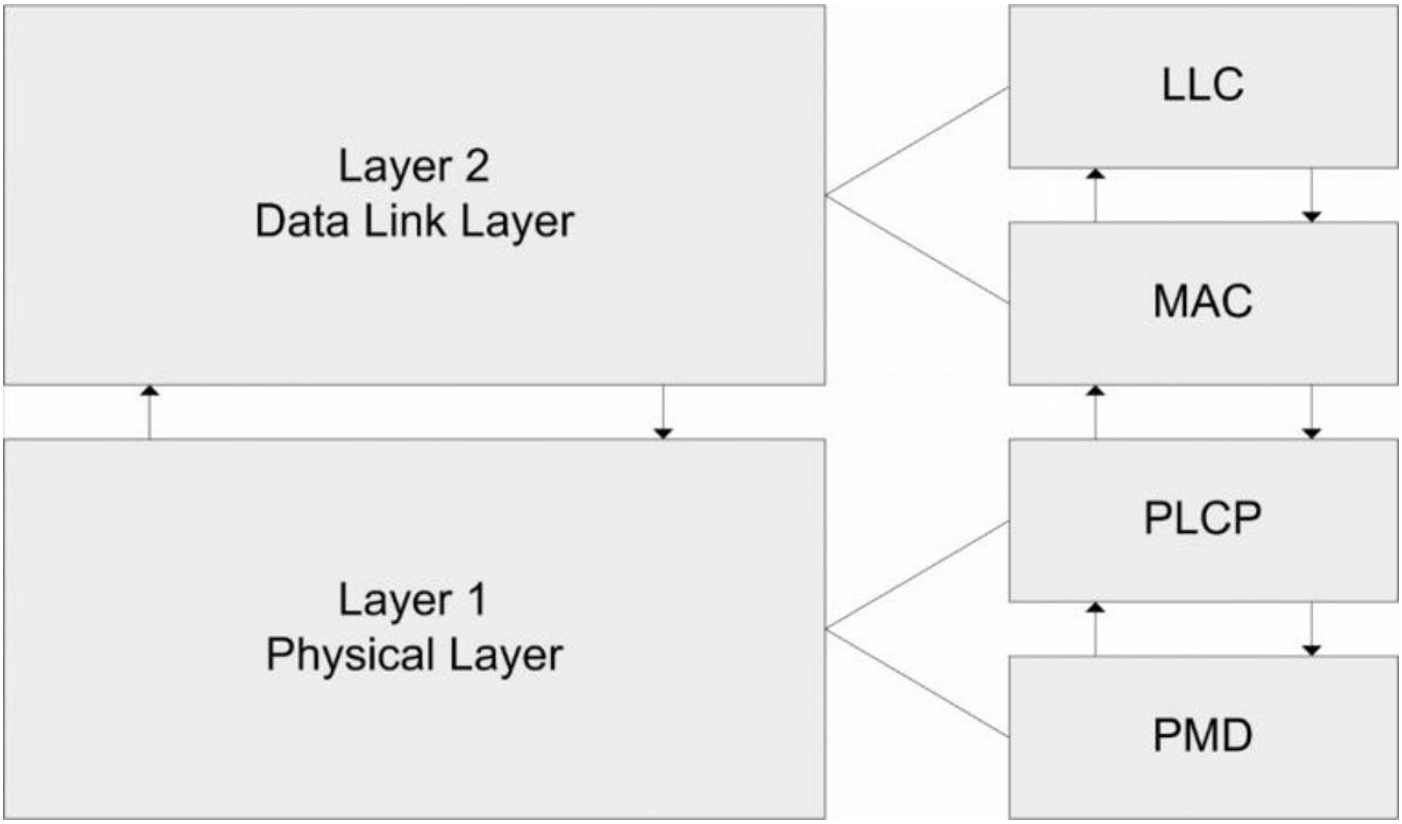


Figure 2-2: Layer 1 and Layer 2 Sublayers

MSDU

The data units, or frames, that are passed down through the layers have specific names. These names are used to distinguish the information at one layer from the information at another layer, and to distinguish the pre-serviced information from the serviced information at each layer. These names are: MSDU, MPDU, PSDU, and PPDU. Let us examine each.

MSDU stands for MAC Service Data Unit. The MSDU is that which is received from the upper layers (OSI layers 7–3 via the LLC sublayer) to be managed and transmitted by the lower layers (OSI layers 1–2). It is the data accepted by the MAC layer to be transmitted to the MAC layer of another station on the network. MSDUs are included in all wireless frames that carry upper layer data; however, 802.11 management frames do not contain MSDUs since no upper layer data exists for management frames. Technically, the MSDU is the LPDU received from the LLC.

MPDU

The MPDU, or MAC protocol data unit, is that which is delivered to the PLCP so that it can ultimately be converted into a PPDU and transmitted. Where the MSDU is received by the MAC, the MPDU is that which comes out of the MAC. The MPDU is delivered to the Physical Layer, and specifically to the PLCP. Another way of saying this is to say that

the MSDU is received by the MAC from upper layers, and the MPDU is provided by the MAC to the lower layer.

PSDU

The PSDU is the PLCP service data unit. The PSDU is that which the PLCP receives from the MAC sublayer. While the MAC sublayer calls it the MPDU, the Physical Layer references the exact same object as the PSDU. The PLCP adds information to the PSDU and provides the result to the PMD as a PPDU.

PPDU

The PPDU, or PLCP protocol data unit, is what is actually transmitted on the RF medium. The PPDU is that which the PMD receives from the PLCP. Ultimately, the PPDU is the culmination of all that has happened to the data from the time it left the application starting at Layer 7 of the OSI model to the time it is actually transmitted on the RF medium by the PMD at Layer 1.

Understanding Data Units at Layer 1 and Layer 2

The concept of the protocol data units and their relationships to Layer 1 and Layer 2 can become difficult to grasp, so I will explain them in sequence. First, I will explain it from the upper layers (the LLC component of Layer 2 and Layers 3–7) down to the physical medium, and then from the physical medium to the upper layers.

The life of a data unit begins as a TCP segment in most TCP/IP communications. This information is either passed directly to the MAC layer from the IP protocol, or is passed to the MAC layer through the LLC layer. Either way, when the information is passed to the MAC layer it is called a MSDU. The MSDU is always 2304 bytes or smaller, and this size limit is a constraint of the 802.11 MAC. The 802.11 MAC specifications limit the upper layer frame payload to 2304 bytes in Clause 8 of 802.11-2012. The MAC layer adds a header and a trailer and expands the frame for encryption overhead. At this point, the MAC layer has created an MPDU. The MPDU is the MSDU with the extra information added by the MAC layer.

Note: **The maximum MSDU size is still 2304 octets or bytes in the ratified 802.11n and 802.11ac amendments. However, support for Aggregate-MSDUs (A-MSDUs) allows for a total data size of up to 7935 octets or bytes in 802.11n depending on the station’s capabilities. 802.11ac supports even larger aggregate sizes. An A-MSDU is a collection of more than one MSDU transmitted in a single frame, and each MSDU in the frame is still limited to 2304 bytes.**

Next, the MAC layer hands off the MPDU to the PLCP component at the Physical layer. The PLCP component receives the MPDU and considers it a PSDU. The PSDU is the same thing as the MPDU; however, from the perspective of the PLCP, it must be serviced in some way. The PLCP and PMD sublayers work together to create a PLCP preamble, a PLCP header and an altered PSDU, in so doing, creates a PPDU out of the PSDU. This PPDU is transmitted as bits on the physical medium or RF by the PMD.

In reverse, the bits are received from the physical medium or RF and the PMD sends a PPDU up to the PLCP. The PLCP strips its header from the PPDU and passes the resulting PSDU up to the MAC layer. The MAC receives the PPDU and processes it as a MPDU by stripping away its header, trailer, and encryption frame expansion, and then passes the result to the upper layers as a MSDU.

In large part, the difference between an MPDU and a PSDU is a factor of perception. When looking at it from the perspective of the MAC layer, it is a MPDU. When looking at it from the perspective of the PLCP layer, it is a PSDU. However, there is a very important reason for the different naming schemes that CWAPs need to grasp. The “S” in MSDU and PSDU stands for service. A good way to remember this is to remember that the frame needs to be serviced by the specified layer, or to have been stripped of servicing during reception of a frame. This is why the MPDU is a PSDU when it is received by the PLCP. The frame must be serviced before sending it on to the PMD. The service offered is the exchange of an SDU with a peer entity in a source or destination system. This is usually accomplished by encapsulation and availing the service of a lower layer.

The common Logical Link Control (LLC) sublayer of the Data Link layer is shared among 802.3 and 802.11 networks. The primary LLC function is to allow for multiple upper layer protocols (such as TCP/IP and IPX/SPX), though most networks today are IP based. Technically, LLC has other capabilities, but they are not commonly used today outside of some WAN scenarios. Just as the MPDU is the PSDU to the PHY, the LPDU is the MSDU to the MAC. The LLC sits above the MAC sublayer. The LLC was initially designed for Token Ring networks, which are mostly defunct today.

LLC comes in three modes or types: Type 1, Type 2, or Type 3. Type 1, or LLC1, is connectionless. Type 2, or LLC2, is connection-oriented. Type 3, or LLC3, is an acknowledged connectionless mode. LLC Type 1 is required of all compliant systems and LLC Types 2 and 3 are optional. As the LLC is shared across 802.11 and 802.3 networks and is rarely a factor in troubleshooting, it is not addressed in greater detail here. However, a cursory reading of the 802.11 standard reveals that 802.11 is heavily dependent on LLC operations, and is in fact designed to transfer LPDUs between two LLC entities.

Note: **The 802.11-2012 standard specifies that an extended service set (ESS) is a set of one or more interconnected basic service sets (BSSs) that appears as a single BSS to the logical link control (LLC) layer at any station (STA) associated with one of those BSSs. It further states that 802.11 WLANs are required to appear as a wired 802 LAN to the LLC and, therefore, 802.11 networks must perform functions in the MAC sublayer that are not traditional for MAC sublayers. In this way, the LLC layer has certainly impacted the 802.11 standard in development.**

PHY Level Information

The PLCP framing results in a PLCP header and is followed by the MAC frame; however, prepended to the PLCP header in transmission is the PLCP preamble. The Sync and SFD fields are collectively known as the PHY or PLCP preamble. The 802.11 preamble precedes the rest of the frame (PPDU) on the air interface. The preamble begins with synchronization bits.

- The sync bits are not data, but they are a known pattern of 0s and 1s—they are not buffered by the receiver.
- They indicate to all nearby stations that a frame is forthcoming.
- They provide time for the receivers to detect the signal, choose diversity settings, synchronize with the signal, and perform other radio adjustments to prepare for receive.

The sync bits are followed by a start frame delimiter (SFD). The SFD is a series of bits that indicates the end of the Sync period and the beginning of the data. To be clear, the SFD is not followed by application data or the MAC frame but by the “meaningful” bits that must be interpreted by the receiver, starting with the PLCP header and followed by the 802.11 MAC, LLC data, network layer data, transport data, etc. The PLCP header that follows the SFD includes information revealing the length of time required to transmit the entire frame in microseconds and additional details.

The Network Allocation Vector (NAV) that you are familiar with from CWNA is not set by the length field in the PLCP header. Rather it is set from the DurationID field in the PSDU. (Remember, this is the MAC frame as it is seen by the PHY.) However, the 802.11 protocol dictates that a PHY will report CCA busy even if the signal is lost during the time it would take to transmit based on the PLCP header length field. This prevents a STA from counting down its backoff timer and beginning to communicate before the medium is truly idle. In some circumstances, particularly for distant low data rate clients, the client may be able to process the PLCP header but lose the signal due to some change in the environment during the PSDU transmission. In such cases the client would cause a collision if it attempted to transmit based on the lack of a current signal. This functionality is important as the client may not have received the DurationID field of the PSDU (MAC frame) to set its internal NAV. Therefore, the PHY is responsible for communicating to the MAC that the medium is busy rather than idle even if no signal is detected. It is very nuanced but important to grasp.

802.11 Architecture Terms

The following terms from your CWNA studies are provided for review:

- *Station (STA):* Any 802.11 wireless addressable unit (device that possesses an 802.11 PHY and MAC wireless interface). A STA can be a client station or an AP.
- *Basic Service Set (BSS):* The basic building block of an 802.11 wireless network, a BSS is composed of at least one station that has initiated a service set and possibly

more stations that have joined the service set. A BSS is usually initiated by an AP and then joined by client stations.

- *Basic Service Area (BSA):* The area containing the members of a basic service set (BSS). It may contain members of other BSSs.
- *Basic Service Set Identifier (BSSID):* The 6-octet (12 hex characters) MAC address representation that identifies a BSS. A single AP's radio can support multiple BSSs, using a unique BSSID for each one.
- *Independent Basic Service Set (IBSS):* A basic service set (BSS) that forms a self-contained network, and in which no access to a distribution system (DS) is available. IBSS networks also lack a central coordination point, such as an AP. An IBSS is often called an Ad Hoc or Peer-to-Peer network.
- *Extended Service Set (ESS):* A set of one of more interconnected basic service sets.
- *Distribution System (DS):* A system used to connect LANs and BSSs to create an ESS.
- *Distribution System Medium (DSM):* The medium used to communicate between APs and portals of an ESS.
- *Service Set Identifier (SSID):* The network name of a BSS or ESS, as known and identified by users.
- *Portal:* The logical point at which the integration service (translation from one format to another) is provided.

802.11 Communications

The first step required to communicate on an 802.11 WLAN is BSS location. The STA must locate an AP to which it desires to connect. This can be performed with active or passive scanning. The 802.11 MAC layer provides the following functions:

- *Scanning*—Before a station can participate in a Basic Service Set, it must be able to find the APs that provide access to that service set. Scanning is the process used to discover Basic Service Sets or to discover APs within a known Basic Service Set. It can be either passive (Beacon management frames) or active (Probe Request and Probe Response frames).
- *Synchronization*—Some 802.11 features require all stations to have the same time. Stations can update their clocks based on the timestamp value in Beacon frames.
- *Frame Transmission*—Stations must abide by the frame transmission rules of the Basic Service Set to which they are associated. These rules are the Distributed Coordination Function in all known systems at this time with enhancements provided for QoS in 802.11e and WMM.
- *Authentication*—Authentication is performed before a station can be associated with a Basic Service Set. This will be covered in more detail later in this section.

- *Association*—Once authentication is complete, the station can become associated with the Basic Service Set. This includes discovery of capability information in both directions—from the station to the AP, and from the AP to the station. Association is covered in more detail later in this section.
- *Reassociation*—When users roam throughout a service area, they may reach a point where one AP within an Extended Service Set will provide a stronger signal than the currently associated AP. When this occurs, the station will reassociate with the new AP.
- *Data Protection*—Data encryption may be employed to assist in preventing crackers from accessing the data that is transmitted on the wireless medium (WM).
- *Power Management*—Since the transmitters/receivers (transceivers) in wireless client devices consume a noteworthy amount of power, power management features are provided that assist in extending battery life by causing the transceiver to sleep for discreet specified intervals.
- *Fragmentation*—In certain scenarios it is beneficial to fragment frames before they are transmitted onto the WM. This type of scenario most often occurs due to intermittent interference. Fragmentation is covered in more detail later in this section.
- *RTS/CTS*—Request to Send/Clear-to-Send is a feature of IEEE 802.11 that will help prevent hidden node problems and allow for more centralized control of access to the WM. RTS/CTS is covered in more detail later in this section.

Beacon Frames

The beacon management frame is a special type of frame used in 802.11 networks. This frame is often referred to as the beacon since this is the frame subtype specified in 802.11 as amended. Table 2.3 lists the more important information provided in the beacon frame. More details of important frames are provided in Chapter 3.

Information	Description
Timestamp	Used for synchronization.
Beacon Interval	Used to specify the amount of time between beacon transmissions.
Capability Information	Used to communicate capability information such as security requirements, whether the service set is an ESS or an IBSS, and other capabilities as specified in the 802.11 standard as amended.

SSID	The ID or name of the network identified by the Beacon.
FH Parameter Set	Element is present within Beacon frames generated by stations using FH PHYs. Provides information for hop patterns, dwell time, and other parameters needed for FH PHYs.
DSSS Parameter Set	Element is present within Beacon frames generated by stations using DSSS PHYs. Provides information for channel specification.
CF Parameter Set	Element is only present within Beacon frames generated by APs supporting Point Coordination Function (PCF). Parameters provided are used to manage PCF. Unused and not implemented in vendor hardware.
IBSS Parameter Set	Element is present within Beacon frames generated by STAs in an IBSS. Contains the ATIM Window information for power saving operations in an ad-hoc wireless network (IBSS).
TIM	Element is present within Beacon frames sent by APs. This is the Traffic Indication Map. Used by STAs employing power save modes.
Supported Rates	Specifies up to eight data rates.
Extended Supported Rates	Specifies any other data rates not specified in supported rates.
ERP Information	Contains information that allows Clause 19 (ERP PHY) devices to coexist with Clause 15 (DSSS PHY) or Clause 18 (HR/DSSS PHY) devices.
RSN	The Robust Security Network (RSN) element is present when CCMP/AES or TKIP/RC4 is in use.
HT Capabilities	Defines 802.11n capabilities including maximum MPDU length, short GI, beamforming options, and supported spatial streams and MCSs.
HT Operation	Defines 802.11n channels and frequencies and protection modes.

VHT Capabilities	Defines 802.11ac capabilities including maximum MPDU length, short GI, beamforming options, and supported spatial streams and MCSs.
VHT Operation	Defines 802.11ac channels and frequencies.

Table 2.3: Beacon Frame Body Information

In an Ad Hoc wireless network (IBSS), all the stations take turns broadcasting the beacon frame. This is because there is no AP in an Independent Basic Service Set (IBSS).

Beacon frames can be used by client stations seeking a wireless network to join, or these client stations may use other frames known as probe request and probe response frames. Both methods will be covered in the following sub-sections *Active Scanning* and *Passive Scanning*.

Active Scanning with Probe Request and Probe Response Frames

Active scanning uses probe request and probe response frames instead of the beacon frame to find a WLAN to join. Two general methods can be used by a client station to find the WLAN. The first is to specify the SSID of the network being sought, and the second is to seek any BSS that may be able to hear and respond to the probe request.

If the SSID is specified in the probe request frame transmitted by the requesting station, all APs that are configured with a matching SSID should respond, assuming they receive the probe request frame. It is certainly possible that a set of APs using the same SSID could cover an area large enough that all of the APs will not receive the probe request transmitted from a specific location in that area. The response from the APs that hear the probe request is a probe response frame. The probe response frame contains the same basic information that the beacon frame contains with the exception of the Traffic Indication Map.

In an Ad Hoc wireless network, which is a network without an AP, the station that last transmitted the beacon frame will respond to probe requests. There are also times when no station will respond to a probe request. This happens when vendors provide a feature to disable probe responses, even though the 802.11 standard requires that all APs respond with a probe response when a probe request is received matching the AP’s configured SSID or when the probe request contains a wildcard SSID (an SSID of zero length, formerly called the broadcast SSID). The vendors often allow their APs to be configured so that they ignore wildcard SSIDs. While this is a non-standard configuration, as long as the WLAN administrator has configured all valid clients to specify the SSID, it should not cause problems within the WLAN for these clients.

Recall from CWSP that disabling the SSID broadcast in the beacon frames is sometimes thought to provide a more secure WLAN environment; however, it is important to remember that the association frames have the SSID in them by default. Unless this SSID broadcasting is turned off, those wishing to penetrate your network can easily discover the SSID with WLAN analysis software and then configure their clients with the appropriate

settings. Even if you disable both the response to wildcard SSID probe requests and the broadcasting of your SSID in the Beacon frames, the intruders can patiently wait until a frame is transmitted onto the WM that contains the SSID and then use this information to configure their client stations. Ultimately, the SSID should not be considered a factor in security management unless you are only concerned with casual Wi-Fi war drivers who lack any WLAN technical skills. You are not likely to take your wireless security so lightly in any business setting, and I do not recommend you take it that lightly in a home setting either.

If a probe request is transmitted onto the WM having a wildcard SSID (a null value for the SSID), all APs that receive the probe request will respond with a probe response containing their SSIDs. This is the standard behavior. Any devices that do not respond in this way are operating in a non-standard way as mentioned previously. Figure 2.3 illustrates the process of active scanning. The top half illustrates the probe request being transmitted and the bottom half illustrates the probe response coming from the APs.

The exact details of the active scanning process are a bit more complex than the simple overview presented up to now. In fact, active scanning involves channel switching and scanning each channel in a station’s channel list. If only one channel were scanned, the client STA would frequently be out of range of a usable AP. To ensure all available APs are located, the client STA will send probe requests on all channels, or on all channels for which it is configured to do so.

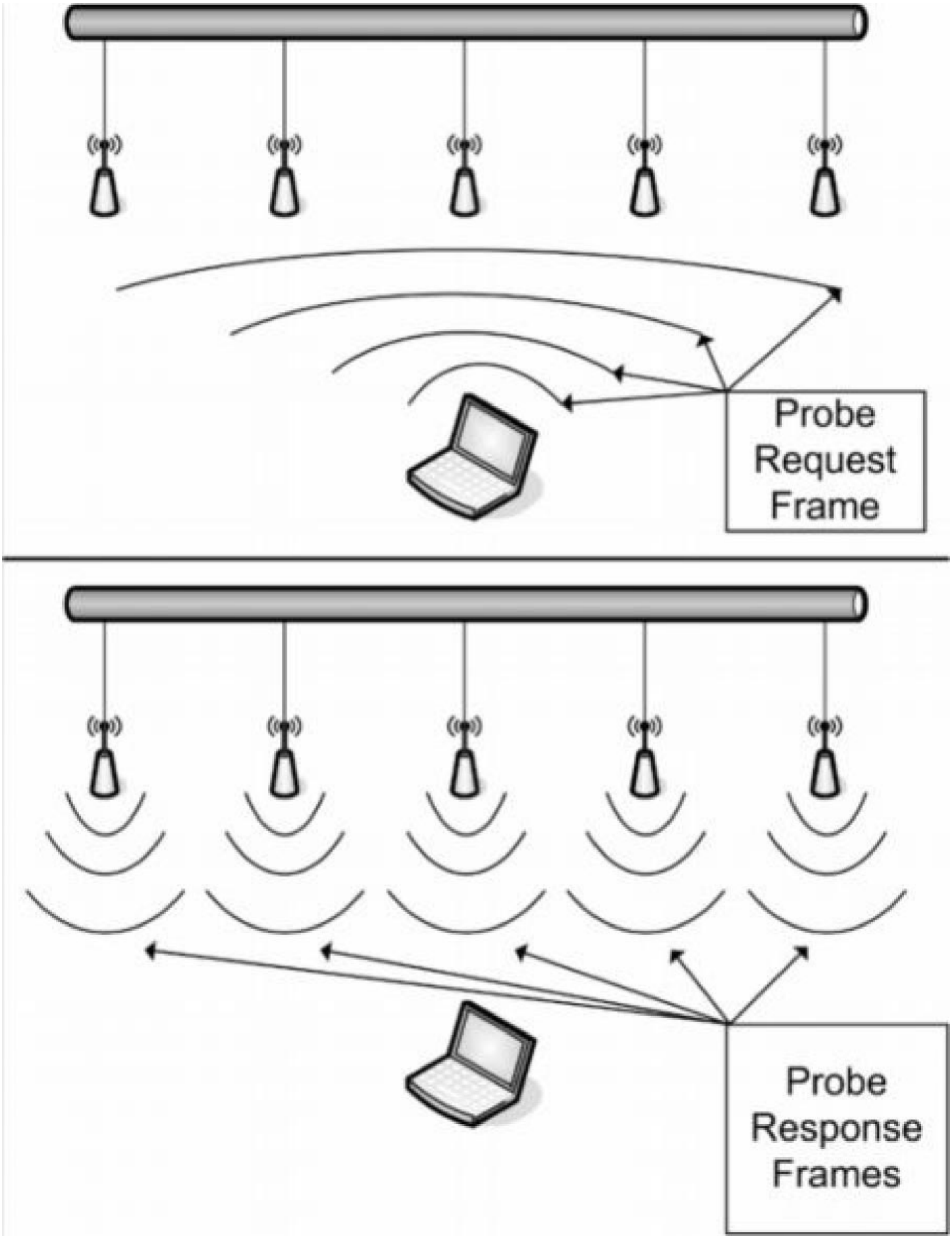


Figure 2-3: Active Scanning Process

The basic process is outlined here:

1. Switch to a channel.

2. Wait for an incoming frame or for the ProbeDelay timer to expire.
3. If the ProbeDelay timer expires, use DCF for access to the WM and send a probe request frame.
4. Wait for the MinChannelTime to pass.
    a. If the WM was never busy, there is no WLAN on this channel. Move to the next channel.
    b. If the WM was busy, wait until MaxChannelTime has expired and then process any probe response frames.

EXAM MOMENT: The specific channels that the client radio will scan are proprietary. Particularly in the 5 GHz band, many channels are simply not supported by many client devices. This is a common issue that must be considered in WLAN design, but it is also important for the analyst who must troubleshooting connection problems and dead spots in the WLAN.

Passive Scanning with Beacon Frames

Passive scanning is a much different process. Instead of transmitting to find the APs, the client station listens (receives) in order to find the APs. This is done by receiving Beacon frames and using them to find the AP for the Basic Service Set to be joined. When multiple APs transmit Beacon frames that are received by the passive scanning station, the station will determine the AP with the best signal (as determined by RSSI) and attempt to authenticate and associate with that AP.

802.11 State Machine

As you have learned in your CWNA studies, the state machine of the 802.11 standard can be in one of three states:

- Unauthenticated/Unassociated
- Authenticated/Unassociated
- Authenticated/Associated

In the initial state a client station is completely disconnected from the WLAN. It cannot pass frames of any type through the APs to other stations on the WLAN or the wired infrastructure. Authentication frames can be sent to the APs. These frames are not sent through the APs, with the exception of a split MAC implementation where a WLAN controller performs the authentication, but are sent to the AP. The distinction is important. Frames must be transmitted to the AP in order to eventually reach the authenticated and associated stage; however, until the final stage is reached, only authentication and association request frames will be processed by the AP.

APs, or WLAN controllers, keep a list known as the association table. Vendors report the stage of the station’s state machine differently. Some vendors may report that a client that has not completed the authentication process is unauthenticated and other vendors may simply not show the client in the association table view.

The second state of the state machine is the *authenticated and unassociated state*. To move from the first state to the second, the client station must perform some kind of valid authentication. This is accomplished with authentication frames. Once this second state is reached, the client station can issue association request frames to be processed by the AP; however, other 802.11 frame types are not allowed. In most APs the association table will now show “authenticated” for the client station. Since the interval between reaching the authenticated and unassociated stage and moving on to the authenticated and associated stage is very small (usually a matter of milliseconds), you will not see client stations in this state very often. In most cases you will either see “unauthenticated” or nothing for the first state and associated for the third state.

The only exception to this is what is sometimes called “pre-authentication” during enhanced roaming situations. A station can authenticate with any number of APs, but it can only be associated with one AP at a time. The AP to which the station is associated must be a single entity in order for other devices on the network to be able to reach that station. In some systems, the station is capable of authenticating with multiple APs so that it can roam more quickly when the need arises.

The third and final state is the *authenticated and associated* state. In order for a station to be in this state, it must have first been authenticated and then associated. The process of moving from state two (authenticated and unassociated) to this state is a simple four frame transaction. The client station first sends an association request frame to an AP to which it has been authenticated. Second, the AP responds with an acknowledgement frame. Next, the AP sends an association response frame either allowing or disallowing the association. The client sends an acknowledgement frame as the fourth and final step. If the third step resulted in an approval of the association request, the client station has now reached the authenticated and associated state and may communicate on the WLAN or through the WLAN to the wired network if encryption keys match and 802.1X is not enabled.

The association response frame includes a status code element. If the status code is equal to 0, the association request is approved or successful. Three other status codes that may apply include: 12, 17, and 18. A status code of 12 indicates that the association was rejected for some reason outside of the scope of the 802.11 standard. A status code of 17 indicates that the AP is already serving the maximum number of client stations that it can support. Finally, a status code of 18 indicates that the client station does not support all of the basic data rates required to join the BSS.

> **EXAM MOMENT:** The status codes can help the analyst troubleshoot connection problems when client STAs are being rejected in the initial association process. Be sure to remember the meaning of status codes 0, 12, 17, and 18.

The key point is to realize that you cannot transmit data frames for processing until you have been associated, and you cannot transmit association frames for processing until you have been authenticated. Additionally, when 802.1X/EAP is used, you cannot transmit user data until 802.1X/EAP authentication is successful. Before 802.1X/EAP success only authentication communications are allowed through the AP to the wired network. This provides for port-based security in a WLAN. Now that you have reviewed the three states in which a station can reside, let us explore the details of how the station can become authenticated and then associated.

Authentication

Based on the three possible states of a wireless station, you know that the second step to joining a WLAN after discovery through scanning is authentication. By now you know that the 802.11 standard specifies two methods of authentication: Open System authentication and Shared Key authentication. The first seems it would be used in less secure environments, while the second seems it would be used in more secure environments; however, we will review why the opposite is true.

Open System Authentication

Open System authentication is essentially a null algorithm. No true authentication (verification of identity) occurs. Additionally, Open System authentication is specified as the default authentication mechanism in the IEEE 802.11 standard. Table 2.4 provides a step-by-step sequence of events that transpire in the Open System authentication process.

You will notice that the four steps in Table 2.4 do not include any actual authentication of identity. APs configured to use Open System authentication will always respond with a positive authentication to any authentication request, unless they have some proprietary feature like band steering or load balancing enabled, and are choosing not to respond for this reason.

Step	Station Acting	Action Taken	Results
1	Client	Transmits an authentication frame with the code indicating that Open System authentication should be used.	Authentication Frame Transmitted
2	AP	Receives the authentication frame and responds with an Ack frame.	Authentication Frame Received
3	AP	Transmits an authentication frame to the client indicating a positive authentication.	Authentication Approved
4	Client	Receives the positive authentication frame and response with an Ack frame to the AP.	Approved Authentication Acknowledged

Table 2.4: Open System Authentication Process

Be careful not to confuse authentication with confidentiality. Data privacy or

confidentiality is about protecting transmitted data from interception. Authentication is about verifying identities of senders and receivers on the network. The point is that WEP was used in authentication (Shared Key), and it can also be used for confidentiality (data encryption). You could use WEP with both Open System authentication and Shared Key authentication for data confidentiality.

Note: **WEP is deprecated and no longer supported in modern secure WLANs. If a device is still in use with WEP, it should be replaced as soon as possible. See CWSP materials for more information.**

Before you move away from Open System authentication with an assumption that it provides no use, keep the following realities in mind:

- Open System authentication is preferred at hot spots where you want to provide unauthenticated access to the Internet or to use a captive portal for authentication.
- More secure authentication technologies, such as 802.1X, rely on Open System authentication. Open System authentication leaves the AP open to other layers of security beyond the pre-IEEE 802.11i authentication standards.

Shared Key Authentication

Shared Key authentication utilizes the wired equivalent privacy (WEP) key for authentication. WEP can also provide encryption of the MSDU, but the 802.11 standard defines this algorithm as providing protection from casual eavesdropping and should be understood as not providing protection from structured attacks. Due to the weaknesses discovered in the WEP algorithm, very few networks should implement and use Shared Key authentication or WEP encryption today and it is a deprecated protocol. Certainly, the networks that do utilize these algorithms are insecure and should be upgraded as soon as possible. In fact, the 802.11-2012 standard references WEP as a past tense solution when it says:

WEP-40 was defined as a means of protecting (using a 40-bit key) the confidentiality of data exchanged among authorized users of a WLAN from casual eavesdropping.

Notice the use of the past tense. The 802.11-2012 standard further states:

Except for Open System authentication, all pre-RSNA security mechanisms have been deprecated, as they fail to meet their security goals. New implementations should support pre-RSNA methods only to aid migration to RSNA methods.

Finally, the 802.11-2012 standard also states:

Shared Key authentication is deprecated and should not be implemented except for backward compatibility with pre-RSNA devices.

When Shared Key authentication is used, the client station and the AP must both use the same WEP key. APs can store multiple WEP keys so that some stations can communicate using one WEP key and other stations can communicate using another. The fact that both stations (the client and the AP) share the same key gives rise to the name Shared Key. The

Shared Key authentication process is documented in Table 2.5 as a sequence of steps with descriptions of the activities that occur in each step.

WARNING: Do not allow the greater complexity of the authentication process in Table 2.5 to mislead you. Even though Shared Key authentication performs real authentication, it is not more secure than using Open System authentication followed by EAP, WPA, or WPA2. These more secure technologies (WPA2 preferred) should always be used.

Note: **Interestingly, the 802.11-2012 standard states that, "The use of WEP for confidentiality, authentication, or access control is deprecated. The WEP algorithm is unsuitable for the purposes of this standard." Then, it says as well of TKIP, "The use of TKIP is deprecated. The TKIP algorithm is unsuitable for the purposes of this standard." Modern networks should use CCMP/AES as all other commonly implemented security solutions have been deprecated.**

Deauthentication

Deauthentication frames are known as advisory frames. This is because they are advising the network of something and the network cannot prevent that thing from occurring. A standard 802.11-based AP cannot deny a deauthentication frame. This frame would be transmitted to the AP (or other members of the IBSS in an ad-hoc network) and the receiving device would simply acknowledge the deauthentication. This would also result in a lowering of the state machine's state in the AP's association table.

A deauthentication frame will include the address of the station being deauthenticated and the address of the station with which the deauthenticating station is currently authenticated. The deauthentication frame will have a reason code of 3, which indicates the reason being that the deauthenticating station is either leaving or has left the Basic or Extended Service Set. Remember that authentication must happen before association can take place; for this reason, a deauthentication frame effectively disassociates and deauthenticates the transmitting client station from the AP.

Association, Reassociation, and Disassociation

After authentication comes association. As was stated earlier, a station can be authenticated with multiple APs, but it can be associated with only one. There are three frames related to association: association frames, reassociation frames, and disassociation frames.

Association

The process of association is very simple. Four frames are transmitted between the client station and the AP station. The first frame is an association request frame, which is followed by an acknowledgement frame from the AP. The third frame is an association response frame, which is followed by an acknowledgement frame from the client station. It is extremely rare for a client station to successfully authenticate and then fail to associate. This is because the client station can usually determine if it is compatible with

the Basic Service Set by inspecting the Beacon frames or probe response frames sent from the APs.

Step	Station Acting	Action Taken	Results
1	Client	Transmits an authentication frame with the code indicating that Shared Key authentication should be used.	Authentication Frame Transmitted
2	Access Point	Receives the authentication frame and transmits an Ack frame to the client.	Authentication Frame Received
3	Access Point	Generates challenge text (randomly generated plain text), and transmits it to the client station in an authentication frame.	Authentication Challenge Transmitted
4	Client	Receives the authentication challenge frame and transmits an Ack frame to the AP.	Authentication Challenge Received
5	Client	Places the challenge text in another frame while encrypting it with the WEP key, and transmits the challenge response to the AP in another authentication frame.	Authentication Challenge Response Transmitted
6	Access Point	Receives the challenge response authentication frame from the client, and transmits an Ack frame to the client.	Authentication Challenge Response Received
7	Access Point	Decrypts the encrypted text in the authentication challenge response frame, and if it matches the original text, authenticates the client by transmitting a positive authentication frame to the client. If it does not match the original text, a negative authentication frame is sent to the client.	Authentication Challenge Response Processed
8	Client	Client station received the results and transmits an Ack frame to the AP.	Authentication Process Complete

Table 2.5: Shared Key Authentication Process

Reassociation

Reassociation occurs when a client station roams from one AP to another within an Extended Service Set. Because reassociation is part of the roaming process, it will be covered in more detail in the next chapter. An immobile station may also reassociate with its AP in order to change its Robust Security Network Association (RSNA).

Service	Station Type
Authentication	All Stations
Deauthentication	All Stations
Association	Distribution System Service
Disassociation	Distribution System Service
Reassociation	Distribution System Service
Distribution	Distribution System Service
Integration	Distribution System Service
MSDU Delivery	All Stations
Data Confidentiality	All Stations
DFS	All Stations
TPC	All Stations
Higher-layer timer synchronization	All Stations
QoS traffic scheduling (optional)	All Stations and DSS

Table 2.6: MAC Sublayer Services and Associated Station Types

Disassociation

Like the deauthentication frame, a disassociation frame is an advisory frame in that the AP

cannot deny the disassociation. The disassociation service is the component of the MAC layer that is responsible for processing a disassociation. This is one of the thirteen architectural services of the 802.11 MAC layer. The full list of services is provided in Table 2.6 with link to the station type that contains the service.

Table 2.6 is inclusive of all station types including APs, client devices, and any other station that communicates on the 802.11 WM. The Distribution System Service (DSS) is provided by the Distribution System (DS), and may be in an AP or it may be fully or partially contained in a WLAN controller device when using a split MAC architecture. Besides managing station association and message forwarding within an infrastructure BSS, the DS is used to interconnect a set of Basic Service Sets to form an Extended Service Set.

Channel Access using CSMA/CA and DCF

After being authenticated and associated, a STA may contend for access to the medium. All STAs, including APs, must contend for the medium or for channel access. The Distributed Coordination Function (DCF) is the CSMA/CA method implemented in the 802.11 standard. All 802.11 devices support DCF and QoS STAs also support additional quality methods.

On a shared medium collisions may occur. These collisions must be handled in some fashion and wireless networks introduced new challenges to collision management. This section explains how collisions are handles in 802.11 networks.

Ethernet networks (IEEE 802.3) use a form of collision management known as collision detection (CD). Wireless networks use a different form of collision management known as collision avoidance (CA). The full name of the physical media access management used in wireless networks is carrier-sense multiple access/collision avoidance or CSMA/CA.

The essence of CSMA/CA is that collisions can happen in many places on the medium at any time during a transmission, and likely cannot be detected by the transmitter at its location. Listening for evidence of a collision while transmitting is thus worthless and not a part of the protocol. Transmissions cannot be aborted early. Collisions are only inferred as one possible explanation for failure to receive an immediate ACK (a frame used to “ACKnowledge” receipt of a frame) after transmitting a frame in its entirety. The frame must be retransmitted completely. Under these circumstances there is much value in collision avoidance, and therefore is much used in the 802.11 protocols.

If you have ever had a conversation with another person on the telephone you have probably experienced a communications collision. When you both started speaking at the same time, neither of you could hear the other effectively. Usually, you will both stop speaking for some amount of time, and then one of you will start speaking again. Since the time that both of you choose to wait is slightly different, there is a good chance that one of you will be able to communicate the next time. This example would be similar to collision detection as opposed to collision avoidance.

The “carrier sense” in CSMA means that the devices attempt to sense whether the physical medium is available before communicating. The “multiple access” indicates that more

than one device is accessing the physical medium. In a CD implementation of CSMA, when a collision is detected both devices go silent for a pseudo-random period of time. Since the time period is different for each device, they are not likely to try communicating at the same time again. This process helps recover from collisions and to avoid another collision. In a CSMA/CD implementation collisions occur because devices can begin communicating at the same time even though they both listened for “silence” on the physical medium. Silence was indeed detected, but both devices broke the silence at the same moment.

CSMA/CA is used in wireless networks, and it was also used in early Apple LocalTalk networks that were wired networks common to Apple devices. Collision avoidance is achieved by signaling to the other devices that one device is about to communicate. This functionality would be like saying, “Be quiet, for the next few minutes, because I will be talking.” in a telephone conversation. You are avoiding the collision by announcing that you are going to be communicating for some time interval. CSMA/CA is not perfect due to hidden node problems, but it provides a more efficient usage of a medium like RF than would CSMA/CD.

Carrier Sense

Carrier sense is the process of checking to see if the medium is in use or busy. If you have multiple telephones in your house and a single line that is shared by all of these telephones, you use a manual form of carrier sense every time you use one of the phones to make a call. When you pick up the phone, you listen to see if someone else is already using the phone. If someone is on the line, you may choose to hang up the phone and wait until it becomes available. If you have ever been on the phone when someone else begins dialing without first checking to see if anyone is using the line, you have experienced a form of collision as the tones penetrated your ears and overcame your conversation with noise.

In 802.11 WLANs two kinds of carrier sense are performed: virtual carrier sense and physical carrier sense.

Physical carrier sense uses clear channel assessment (CCA) to determine if the physical medium is in use, and is provided by the PHY and not the MAC. CCA is accomplished by monitoring the medium to determine if the amount of RF energy detected exceeds a particular threshold. Due to the nature of WLAN architectures, there is no requirement for all stations to be able to hear all other stations existing in the same Basic Service Set. This is because the wireless AP forms a kind of hub for the Basic Service Set. A station may be able to hear the AP and the AP may be able to hear the other station, but the two stations may not be able to hear each other. This results in what is commonly known as the hidden node problem, as you likely remember from CWNA studies. For this reason wireless networks must use other forms of carrier sense in addition to CCA to deal with medium access control.

The other form is virtual carrier sense, which uses a network allocation vector (NAV), and is provided by the MAC and not the PHY. The NAV is a timer in each station that is used to determine if the station can utilize the medium. If the NAV has a value of 0, the station may contend for the medium. If the NAV has a value greater than 0, the station must wait

until the timer counts down to 0 to contend for the medium. Stations configure their NAV timers based on Duration fields in other frames using the medium. For example, if a station detects a frame with a specific duration set in the Duration field, it will set the NAV timer to this duration and will wait until that time has expired before contending for access.

To be clear, both the physical carrier sense and the virtual carrier sense must show that the medium is available before the station can contend for access. If the NAV timer reaches 0 and the station uses CCA to detect activity on the medium only to find there is such activity, the station still cannot transmit. In this case, another frame may be pulled from the medium and used to set a new NAV timer value for countdown. While it may seem that this would prevent a station from ever communicating, the rate of frame transfer is so high that all of these actions usually take place in far less than one second.

Note: **An additional form of carrier sense that is not often written about is what you might call phantom frame sensing. In this scenario, the PHY reads an incoming PLCP header length value and loses the incoming signal completely. However, since the header length was read, the device can still defer to the rest of the phantom frame.**

Interframe Spacing

After the station has determined that the medium is available using carrier sensing techniques, it still cannot communicate immediately. Instead, it must observe interframe space (IFS) policies. IFS is a time interval in which frames cannot be transmitted by stations within a Basic Service Set. This space between frames ensures that frames do not overlap each other. The time interval differs depending on the frame type and the applicable IFS type for that frame.

While the IFS implementation in IEEE 802.11 systems can result in the appearance of Quality of Service (QoS), it should not be confused with 802.11e or any Layer 3 or higher QoS solution. IFS is an 802.11 feature that allows for dependent frames to be processed in a timely manner. For example, a standard 802.11 data frame is transmitted using the DIFS interval, and the Acknowledgement (ACK) to this data frame is sent back using the SIFS interval. Because the ACK uses a SIFS interval, the ACK frame will take priority over any other data frames that are waiting to be transmitted. This way, the original station that transmitted the data frame will receive the ACK frame and not attempt to resend the data frame. The frame to IFS interval relationships that are specified in the 802.11 standard ensure that frames will be processed in their proper sequence.

I have mentioned some of the IFS types defined by the 802.11 standard already. These IFS types include the following types and will now be covered in more detail:

- SIFS and RIFS
- PIFS
- DIFS

- EIFS
- AIFS

The Short Interframe Space (SIFS) is the shortest of the available IFS parameters in 802.11 devices preceding 802.11n. The new RIFS (reduced IFS) IFS is even shorter still, and it was introduced in 802.11n but it was deprecated in 802.11ac for 5 GHz PHYs; however, it is still in used with the Directional Multi-Gigabit (DMG) PHY of 802.11ad (though the standard indicates that it may be removed from there as well in a future revision). Frames that are specified to use SIFS will take priority over frames that are specified to use PIFS, AIFS, DIFS, or EIFS. This priority function is simply a result of the IFS length. Since the SIFS is shorter than AIFS, PIFS, and DIFS, stations that are waiting to send a frame that is specified to use a SIFS interval will have a shorter wait time and will therefore have access to the WM before other stations with frames specified for longer IFS types.

SIFS is used for many different frames including:

- ACK frames immediately following the receipt of a data frame
- CTS frames sent as a response to RTS frames
- Data frames that immediately follow CTS frames
- With the exception of first exchange and error conditions, all frame exchanges made in PCF mode
- With the exception of the first fragment, all fragment frames that are part of a fragment burst

As technically defined by the IEEE 802.11 standard as amended, the SIFS time interval is to be the time from the end of the last symbol of the previous frame to the beginning of the first symbol of the preamble of the subsequent frame as seen at the air interface. The accuracy level required is +/-10% of the slot time for the PHY in use. For example, the actual SIFS time interval must be within 2 µs of the specified time interval for the DSSS PHY. Slot times for the various PHYs are listed on the next page.

The SIFS times for the various PHYs are listed here:

- FHSS – 28 µs
- DSSS – 10 µs
- OFDM (including HT and VHT) – 16 µs
- HR/DSSS – 10 µs
- ERP – 10 µs

The Reduced IFS (RIFS) is only 2 µs in length and can be used in place of the SIFS in 802.11n networks that do not allow legacy devices. If the 802.11n HT PHY is operating in Greenfield mode, the RIFS may be used. Since this greatly reduces the time between burst frames as well as between data frames and acknowledgement frames, the overall throughput of the network is improved. However, practically no Greenfield mode HT networks have been implemented because either another nearby network or a single non-

HT client in the range of the cell makes it impossible. 802.11ac does not use the RIFS, and it is likely to be completely removed in a later update to the standard.

The Point (Coordination Function) Interframe Space (PIFS) is neither the shortest nor longest interval, resulting in a priority greater than DIFS, but less than SIFS. When an AP needs to switch the network from Distributed Coordination Function mode to Point Coordination Function mode, it will use PIFS frames. Point Coordination Function is an optional part of IEEE 802.11 and has not been implemented in any market devices. The PIFS duration interval is equal to the SIFS interval for the PHY and one slot time duration for the PHY. For example, DSSS has a 20 µs slot time and a 10 µs SIFS interval resulting in a PIFS interval in a DSSS PHY of 30 µs. For another example, the OFDM PHY has a 9 µs slot time and a 16 µs SIFS interval, resulting in a PIFS interval in an OFDM PHY of 25 µs.

The following are the slot times for the 802.11 PHYs operating in 2.4 and 5 GHz:

- DSSS – 20 µs
- HR/DSSS – 20 µs
- ERP – 20 µs (long); 9 µs (short)
- OFDM – 9 µs
- HT – 20 µs (Long in 2.4 GHz); 9 µs (short in 2.4 GHz and always used in 5 GHz)
- VHT – 9 µs

The Distributed (Coordination Function) Interframe Space (DIFS) is the longest of the three IFS types covered so far. It is used by standard data frames. The greater delay interval ensures that frames specified for SIFS and PIFS intervals are able to transmit before DIFS data frames. The DIFS interval is calculated as the PHYs SIFS interval plus two times the PHYs slot time. Based on the same numbers used in the previous paragraphs for the PIFS interval calculations and this new algorithm for calculating the DIFS interval, the DSSS PHY has a DIFS interval of 50 µs and the OFDM PHY has a DIFS interval of 34 µs.

The Arbitration IFS (AIFS) is used in quality of service (QoS) stations. AIFS is used for the transmission of all data frames, management frames, and select control frames by a QoS station. The control frames using AIFS include:

- PS-POLL
- RTS
- CTS (when not responding to an RTS)
- BlockAckReq
- BlockAck

The Extended Interframe Space (EIFS) is used when a frame reception begins, but the received frame is incomplete or is corrupted based on the Frame Check Sequence (FCS) value. When the last frame the station received was corrupted, the station uses EIFS for the next frame that it transmits. The EIFS interval is the longest of the IFS intervals, and is

calculated based on the following more complex algorithm:

```
EIFS = SIFS + (8 X ACKsize) + Preamble Length + PLCP
Header Length + DIFS
```

The time calculation is the amount of time in microseconds that it takes to transfer the 8 ACKs, preamble, and PLCP header. As you can see, the EIFS is more than the DIFS and SIFS combined.

> **EXAM MOMENT:** For the exam, you should remember which IFS is shortest and which is longest. From shortest to longest they are RIFS, SIFS, PIFS, DIFS, AIFS, and EIFS.

Contention Window

The IFS delay interval is not the end of the wait for devices that are seeking time on the wireless medium (WM). After the IFS delay interval has passed, the device must then initiate a random backoff algorithm, and then contend for the WM if the Distributed Coordination Function is in effect—and it almost always is in today's wireless networks. This random backoff algorithm is processed and applied using the contention window.

Note: **The phrase contention window has caused much confusion, but it is the phrase in use in the 802.11 standard. This "window" is actually a range of integers from which one is chosen at random to become the backoff timer for the immediate frame queued for transmission. Think of it like a contention range instead of a contention window and it will be a little easier for you.**

All stations having a frame to transmit choose a random time period within the range specified as the contention window. Next the predefined algorithm multiplies the randomly-chosen integer by a slot time. The slot time is a fixed-length time interval that is defined for each PHY such as DSSS, FHSS, or OFDM. For example, FHSS uses a slot time of 50 µs, and DSSS uses a slot time of 20 µs.

As you can see, there are definite variations among the different PHYs supported in the IEEE 802.11 standard as amended. The 802.11n amendment used the standard 9 µs slot time used in existing PHYs that support OFDM.

Now that you have most of the pieces to the media contention puzzle, you can begin to put them together in order to understand how a wireless station decides when it should try to communicate on the WM. In order to understand this, imagine that a station has a data frame that it needs to transmit on the WM. This data frame will be required to use the DIFS IFS since it is a standard data frame. Furthermore, imagine that the station uses carrier sense to determine that a frame is currently being transmitted. For discussion's sake, let us assume that the station detected that the frame being transmitted had a Duration/ID field value of 20 µs. The station sets its NAV to count down the 20 µs and waits. The NAV reaches 0, and the station uses carrier sense and detects that the WM is silent. At this time the station must wait for the DIFS interval to expire, and since the

station is using the DSSS PHY, it waits for 50 µs. Next, the station waits for the random backoff time period to expire, and when it does the station uses carrier sense and detects that the WM is silent. The station begins transmitting the data frame. All of this assumes the network is using the Distributed Coordination Function, which is the primary contention management functionality that has been implemented in widespread hardware at this time.

Collision Avoidance

Ultimately, the carrier sense, IFS, and random backoff times are used in order to decrease the likelihood that any two stations will try to transmit at the same time on the WM. The IFS parameters are also used in order to provide priority to the more time sensitive frames such as ACK and CTS frames. The CCA (PHY and MAC), IFS, variable contention window, and random backoff times, together, form the core of the Distributed Coordination Function.

Even with all of these efforts, a collision can still occur. In order to deal with these scenarios, acknowledgement frames or ACK frames are used. An ACK frame is a short frame that uses the SIFS IFS to let the sending device know that the receiving device has indeed received the frame. If the sending device does not receive an ACK frame, it will attempt to retransmit the frame. Since the retransmitted frame will be transmitted using the rules and guidelines we have talked about so far, chances are the next frame—or one of the next few—will make it through without collisions.

The processes documented here are illustrated in the 802.11-2012 standard with the image in Figure 2.4.

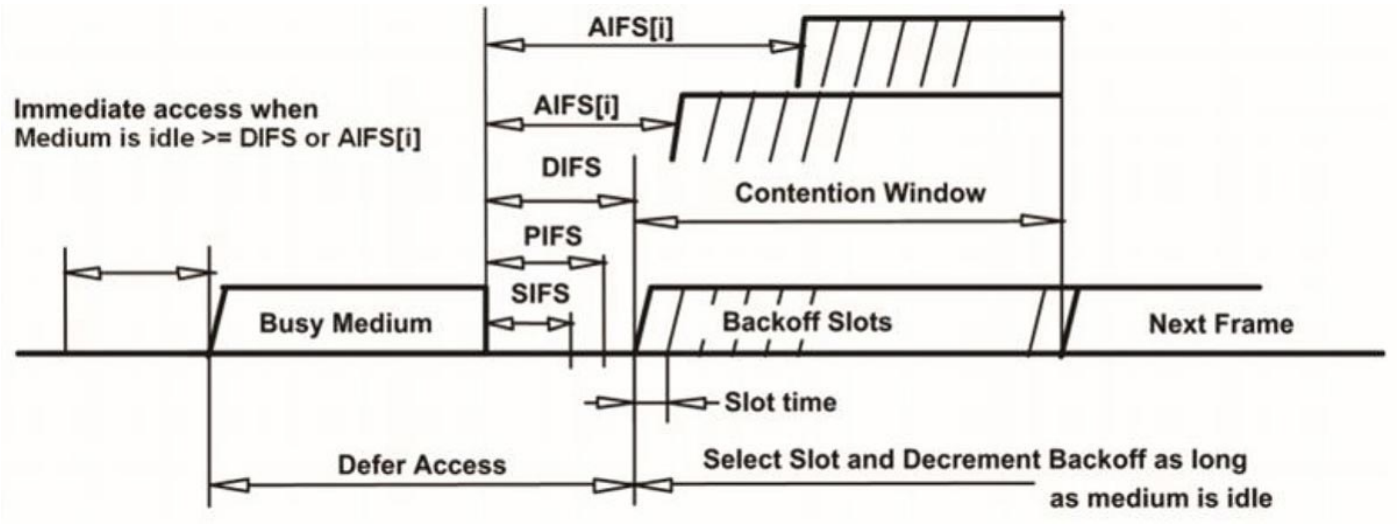


Figure 2.4: The DCF Operation Overview

802.11e and WMM

Many networking technologies require very low latency. In fact, latency issues have even been a problem in some wired networks. The holy grail of networking today is convergence: voice and data (and even video) on the same medium. Convergence has brought latency to the forefront in network design and troubleshooting. One way to provide lower latency is to dedicate a medium to a single pair of devices; however, this is cost prohibitive. The alternative is to somehow identify the higher priority information,

and to make sure that priority information gets preferential access to the medium. This is the heart of Quality of Service (QoS).

PCF was an early contender as a solution to the QoS puzzle in WLANs. However, there was one great limitation: PCF can only prioritize a given device (or MAC address) and not different applications coming from that device. Along with this limitation there are no PCF APs that could be installed today anyway, given that PCF was never really accepted. Since the IEEE has released a solution to the QoS problem in the form of the IEEE 802.11e amendment, it is unlikely that PCF in its original construct will be implemented in the future.

IEEE 802.11e specifies the use of EDCAF (Enhanced Distributed Coordination Access Function) and HCF (Hybrid Coordination Function). 802.11e was ratified on September 22, 2005, and was a 211 page document describing the prioritization mechanisms that have become the standard for QoS in 802.11. 802.11e has been rolled into 802.11-2007 and is included in the latest version of the .11 standard—802.11-2012. The purpose of the document is stated as defining MAC procedures to support LAN applications with QoS requirements like voice, audio, and video.

Two new station types are introduced by IEEE 802.11e: QoS access points (QoS APs) and QoS stations (QoS STA). A QoS AP is an AP that can support the QoS facility. A QoS STA is a station that supports the QoS facility and can act as a standard station when associated with a non-QoS AP. The QoS facility is inclusive of the following components that distinguish a QoS STA from a non-QoS STA:

- QoS Functions
- Channel Access Rules
- Frame Formats and Frame Exchanges
- Managed Objects

EDCAF is the 802.11e enhancement to DCF. Eight traffic categories, or priority levels, are defined by EDCAF. The traffic having the higher priority level will gain access to the WM before traffic having a lower priority level. Ultimately, EDCAF does not provide a guarantee of access to the WM; however, it does increase the probability over DCF that a higher priority frame will be transmitted before a lower priority frame.

These eight traffic categories are defined by the User Priority (UP) value. This value can be from 0 to 7. The UP values are identical to those used in 802.1D. The IEEE 802.11e amendment further explains these UP values and their interpretation.

HCF provides a preemptive capability to the QAP that was not available to an AP with PCF. A PCF AP, if it were available, would have the ability to preempt other stations in the BSS during the contention-free period; however, it could not preempt other stations during the contention period. HCF adds this capability. This preemption should not be thought of as interrupting a station’s frame transmittal, but rather that the QAP can ensure that it will be able to transmit on the WM next.

While 802.11e was being developed, the Wi-Fi alliance released their Wireless Multimedia (WMM) extensions certification. This certification is based on the draft IEEE

802.11e standard and was released to provide QoS for voice over WLAN. The WMM certification will continue to be updated and redefined to mean the latest interoperable QoS featured available from multiple chip vendors.

RTS/CTS

DCF provides a CSMA/CA implementation for WLANs using distributed coordination. PCF could have provided CSMA/CA through centralized or point coordination. Sometimes, you need something different than what is offered by either DCF or PCF alone. Instead of the AP polling the stations to see which station needs to communicate, the stations can tell the AP that they need to communicate and then wait for the AP to give them the go ahead. This method is called Request to Send/Clear to Send (RTS/CTS).

When you are traveling on business or holiday, you have two basic ways of determining where you will sleep at night, assuming you plan to stay in a hotel. You can call ahead and make reservations, or you can just stop at a hotel when you get tired and ask if they have a vacancy. I remember going on trips with my father that were like the latter. We would stop at hotel after hotel only to be rejected many times before finally finding one with a vacancy. However, there was also the chance that the first hotel would indeed have a vacancy. If it did have a vacancy, this would take less time than calling ahead to make the reservation. (Remember, we didn’t have cell phones back then so calling to make the reservation would have taken extra time.)

A similar scenario can happen on a WLAN when the hidden-node problem occurs. In this situation there are two or more clients that can hear the AP and that can also each be heard by the AP, but for a number of potential reasons cannot hear each other. Therefore, when a frame is sent from one of the client stations (STA1) to the AP, the other client station (STA2) might not be able to sense that it is transmitting using physical sensing. This results in STA2 transmitting a frame at the same time, causing corruption or cancellation of the other station’s frame. It is like the frames reached the AP and were told, “no vacancy.”

RTS/CTS is like calling ahead and making reservations. And like the process of calling ahead, RTS/CTS requires extra overhead every time. If you stop at a hotel and check for a vacancy and find that 99% of the time or more there is one, calling ahead to make a reservation would not pay off in the end. However, it you find that a large percentage of the time there are no vacancies, calling ahead would pay off quickly. RTS/CTS is like this, too. If you are having problems like hidden node or other issues that cause retries or BSS congestion, enabling RTS/CTS can help resolve them. If you are not, the “calling ahead” will only add unnecessary overhead to your WLAN.

RTS/CTS works according to the following process:

1. A station wishing to transmit using RTS/CTS sends a request to send frames to the AP.
2. When the AP receives the RTS request, it sends a clear-to-send frame to the WLAN as a broadcast.
3. The stations in the vicinity all hear either the duration in the request to send frame

or the clear-to-send frame and know to stay silent.

4. The original requesting station transmits its frame and receives acknowledgement during this quiet window.

RTS/CTS can function in an Infrastructure Basic Service Set (BSS) or an Independent Basic Service Set (IBSS). In the BSS, the RTS/CTS exchange is between the client stations that wish to send or receive data and the AP, and either may initiate the exchange. In the IBSS the RTS/CTS exchange is between the two communicating client stations. The non-involved stations hear the exchange and set their NAV timers to cooperate with the RTS/CTS process. The RTS/CTS function is enabled by setting an RTS/CTS threshold (specific frame size), that enables RTS/CTS to operate when frame sizes are equal to or greater than the threshold.

An additional implementation of clear to send is found in the IEEE 802.11g amendment for the ERP PHY and still used in later MAC/PHY implementations. This implementation provides for a CTS-to-self. Essentially, the station using this option can communicate using OFDM and faster data rates than older stations such as those using the HR/DSSS PHY. In order for these stations to coexist, the station with the newer PHY will transmit a CTS frame that was not preceded by an RTS frame. This frame will be transmitted using modulation (and therefore data rates) that can be understood by the stations with the older PHYs. Those stations will go silent as they honor the duration value in the CTS frame. During this silent period, the ERP-based station will transmit its OFDM modulated signal without further concern for the non-ERP PHYs.

Data-Rate Factors

Dynamic rate selection, dynamic rate switching, automatic rate shifting, and dynamic rate shifting all refer to 802.11-2012 Section 9.7 Multirate support. But whatever you call it, it is the process of reducing or increasing the data rate to the next supported data rate as the quality of the RF signal changes.

Remember that signal strength attenuates over distance. This results in a weaker signal at a longer distance than is available at a shorter distance. Other factors, such as absorption into materials in the service area, can also result in a weaker signal at a point equidistant from the AP as another point with a stronger signal. Whatever the reason for reduced signal quality, the data rate is lowered to provide more effective use of the WM.

Consider that modulation schemes used in the DSSS PHY, for example, change fewer attributes of the RF signal fewer times in order to modulate data onto the signal than do the modulation schemes used in the OFDM or ERP PHYs. As the quality of the signal degrades, it becomes more and more difficult to demodulate the more complex modulation schemes. By slowing down the data rate by reducing the sophistication of modulation, it becomes easier to demodulate the data.

A standards-based device will only change its data rate to one supported by the standard. For example, a HR/DSSS PHY will shift from 11 to 5.5 Mbps but will not shift from 11 to 6 Mbps because 6 Mbps is not supported by the HR/DSSS PHY. In the same way, an ERP

PHY will shift from 48 to 54 Mbps, but it will never shift from 48 to 51 Mbps since 51 Mbps is not a supported data rate according to the standard.

The actual data rate changes are controlled by proprietary, vendor-specific functions. Some clients will shift from higher rates to lower rates before others. Only testing of actual client behavior can reveal how the data rates change

Data rates are impacted by several factors, but it ultimately comes down to the signal-to-noise ratio (SNR). Additionally, interference must be considered. Noise is a general reference to the noise floor; however, additional sporadic or permanent RF generators can impact the data rate, as well. For example, in an environment where the noise floor is typically -93 dB, the addition of an interferer (like a microwave oven) can lower the data rate, as well.

The data rate is determined by the ability of the receiver to demodulate the signal. Higher data rates require more separation between the actual 802.11 signal and the other RF activity in the environment. This separation is referred to as the SNR. Therefore, to achieve higher data rates the client STA must be close enough to the AP to have a high SNR. This is a reference to closeness as it relates to signal strength and not necessarily physical proximity. For example, one STA may be in the same large room as the AP at a distance of fifty feet with a very different SNR (likely better) than another station only thirty feet away but behind two walls. For this reason, the more important factor than physical distance is RF signal strength. It is all about the SNR and interference sources in the environment when it comes to radio communications of all sorts.

The Shannon-Hartley theorem defines the bandwidth capabilities of a channel. The formula is:

$$C = B \log_2 (1 + S/N)$$

C is the channel's capacity in bits per second (bps). *B* is the channel's bandwidth in kilohertz (kHz). *S* is the received signal strength and *N* is the noise in the environment. While the details of this formula are beyond the scope of the CWAP exam, it is important to remember that the channel capacity is dictated by three primary factors: bandwidth, signal strength, and noise or interference. For example, the bandwidth of a traditional 802.11 channel is 20 MHz or 20,000 kHz.

It is important to remember that the Shannon-Hartley theorem defines the maximum rate at which a channel can be used. It also reveals that the SNR is a controlling factor regardless of the channel bandwidth. To get the highest data rates, the SNR must be high (25–40 dB). Other than improving the SNR, the only option to increase the data rate is to increase the bandwidth.

Why does the SNR matter? It matters because a high SNR makes it easier for the receiver to process a signal with complex modulation and coding schemes. Modulation is the way bits are communicated with varying wave forms. Coding is the way error correction or redundancy is built into the communication.

For example, the 802.11ac amendment to 802.11-2012 specifies modulation and coding tables that also include the number of spatial streams and other factors that impact the data rate. Each stream is modulated with a specified modulation technique, such as BPSK or

QAM, and uses a coding technique that either uses more or fewer bits for recovery. If the coding rate is 5/6 (the best rate available), then five bits are useful and 1 is for recovery. Therefore, the highest data rate for three spatial streams is 288.9 Mbps with a 20 MHz channel. Table 2.7 shows the 802.11ac data rates available with three spatial streams in a 20 MHz channel.

Modulation	Coding	Short-Guard Interval	Long-Guard Interval
BPSK	1/2	21.7	19.5
QPSK	1/2	43.4	39
QPSK	3/4	65	58.5
16-QAM	1/2	86.7	78
16-QAM	3/4	130	117
64-QAM	2/3	173.3	156
64-QAM	3/4	195	175.5
64-QAM	5/6	216.7	195
256-QAM	3/4	260	234
256-QAM	5/6	288.9	260

Table 2.7: 802.11ac 20 MHz Data Rates with Three Spatial Streams in Mbps

The guard interval is the space between symbols (not frames) used to prevent inter-symbol interference. Most environments work well with a short-guard interval (SGI) of 400 ms. Some highly reflective environments may require the older pre-802.11n long-guard interval of 800 ms. This setting alone has a significant impact on the data rate.

Notice particularly in the table that the only difference between 288.9 and 260 Mbps with an SGI is the coding. Both of the last two modulation and coding schemes (MCSs) use 256-QAM. The highest data rates use more bits for useful data than the lower data rates.

As a WLAN analyst, it is important to understand what causes a client STA to select a given data rate. It is also important to know that the AP may send to the client using one data rate and the client may send to the AP using another. This is because the frame must be understood at the receiver. While the AP may receive a frame from the client at a higher data rate successfully, the client may not be able to receive at that same data rate due to localized RF activity. In such cases, retries may cause the AP to select a lower data rate.

In the standard these data rates are referenced in MCS tables as MCS0-9. Some combinations do not support MCS9 (for example, 1, 2, 4, 5, 7, and 8 spatial streams cannot use MCS9, but 3 and 6 spatial streams can in a 20 MHz channel). The full details of the MCS tables are in the 802.11ac amendment. Additionally, 802.11-2012 provides MCS tables for 802.11n and data rate specifications for early PHYs, such as OFDM, ERP and HR/DSSS.

WLAN Architectures

In the popular WLAN PtMP model, which is used for most indoor wireless networks, two primary implementation methodologies exist: the single MAC model and the split MAC model. The single MAC model is sometimes called an edge or intelligent edge model, and the split MAC model is sometimes called a centralized model. For CWAP duties knowledge of both is important.

Single MAC Model (Edge, Autonomous, or Standalone)

When a single MAC model is used it means that the APs contain all of the logic within them to perform MAC layer operations. With this model all 802.11 services reside within the AP with the possible exception of security services when WPA-Enterprise or WPA2-Enterprise is implemented. The single MAC model is the oldest and is still very popular in small and medium-sized WLANs. Both the costs and the benefits of the single MAC model must be considered.

Single MAC model costs:

- Decentralized administration may require more ongoing support effort.
- APs may be more expensive since they have more powerful hardware.
- Each AP may be able to handle fewer client stations.

Single MAC model benefits:

- No single point of failure. If one AP goes down, the others continue to function.
- Less wired network traffic required to manage the wireless stations.
- More features within the APs themselves.

Split MAC Model (Centralized)

The split MAC model is called such because portions of the MAC layer operations are offset to centralized controllers, while other portions remain in the AP. These types of APs are often called thin APs since they do not perform as many functions as the traditional APs (fat APs). The split MAC model is very popular in large networks today and is used in many smaller networks, as well. Most vendors refer to the split MAC model as a controller-based architecture. Again, the costs and benefits associated with the split MAC model must be considered.

Split MAC model costs:

- Possible single point of failure at the WLAN controller; however, enterprise level implementations will include a backup controller to prevent such a failure.
- Increased wired network traffic required to manage the wireless stations.

- Fewer features within the APs themselves when using truly thin APs.

Split MAC model benefits:

- Centralized administration may reduce ongoing support efforts.
- APs may be less expensive since they can have less memory and processing power.
- Each AP may be able to handle more client stations since the AP does not have to handle management processing overhead.

You may have noticed that, in a large way, the benefits of the split MAC model are the costs of the single MAC model and the benefits of the single MAC model are the costs of the split MAC model. While there are certainly more details involved than this, it is important to understand that you will be giving up something regardless of the model you choose. The key is to determine what is best for the organizational and technical needs of the organization in which you are implementing the WLAN.

Note: **The split MAC model is more commonly referred to as the controller-based model today. Both terms may be seen on the CWAP exam.**

Wireless Mesh

Another wireless networking model to understand is the wireless mesh architecture. In the database world you have a one-to-one relationship model, which is like the PtP model in WLANs. You also have a one-to-many relationship model, which is like the PtMP model in WLANs. However, database theory also presents a many-to-many relationship model, which is much like the mesh networking model in WLANs. Therefore, you could say that mesh networking is like a multipoint-to-multipoint (MPtMP) model.

In a mesh network, all APs may connect to all other APs that are turned on and within the range of each other. Additionally, data travels through each node so that every node is both a router/repeater and an end node at the same time. The benefits of a mesh networking model include:

- Communications within areas that would normally have many LOS obstructions.
- Data routing redundancy.
- Mesh networks that are used to implement networks that cannot support Ethernet cable runs to distant APs required by traditional WLAN topologies.

The first benefit is seen because mesh nodes are placed close enough to each other that a path will always be available around obstructions that would normally prevent wireless links. Figure 2.5 illustrates this benefit. Notice that data can travel from node A to node B, then to node C, and finally to node D. If this were not a mesh network, there would be no clear path from node A to node D.

The second benefit is also seen in Figure 2.5. If the route mentioned previously (A to B to C to D) was to become unavailable, data routing redundancy exists in that the route from A to H to E to D could be utilized. Alternate routes also exist, for example A to C to D or A to G to E to D. Mesh infrastructures may provide redundancy for better availability; however, they may also reduce the overall throughput of the wireless network since each AP must be both a client station and an AP station.

The IEEE 802.11s amendment specified a standard for wireless mesh networking that is incorporated into 802.11-2012. You learned that the normal DS (distribution system) for a WLAN is an Ethernet LAN. However, the IEEE standard leaves the specification open so that a wireless distribution system (WDS) could also be used. The 802.11s amendment is aimed at detailing just such a WDS. This means that our future could see networks that are entirely wireless without a single Ethernet cable (or other wired standard) anywhere, assuming the network does not require connections to a traditional infrastructure. Using wireless Internet access, the network could indeed provide Internet connectivity even though no Ethernet wires exist in the meshed network infrastructure.

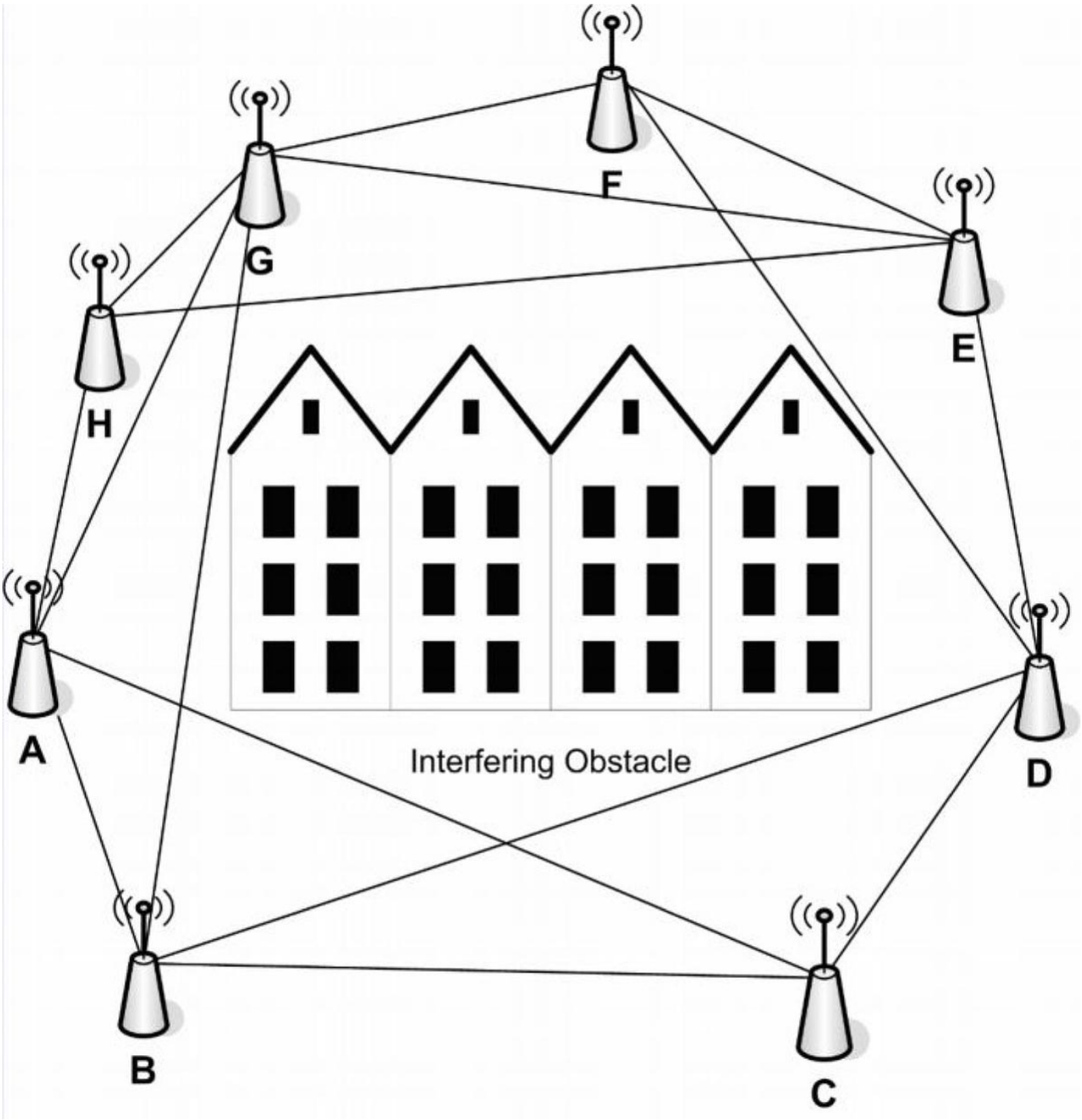


Figure 2.5: Solving LoS Problems with Mesh Links

Right now it seems that the more wireless we implement, the more Ethernet cables we install; this could change with evolving modulation schemes, frequency distribution, and powerful processors at lower prices. This evolution will be aided by both the 802.11n/ac amendments for a MIMO PHY and the 802.11s amendment for a mesh-based WDS, but there is still plenty of work to do and plenty of uses for those wires. While we are years from an entirely wireless infrastructure the potential is exciting.

Consider Table 2.8 in order to fully understand the key differences between mesh wireless access layers and traditional (intelligent edge) wireless. You will notice that mesh wireless access layers provide fast deployment. Deployment is usually faster because the mesh network is self-building and self-healing. The self-healing feature provides fault tolerance. Mesh access layers often have dynamic backhauls that can adjust to individual mesh AP

failures. (The path to the needed network resources is often called the backhaul.) Traditional WLANs have a single route out of the APs and onto the wired network.

Mesh	Traditional
Fast deployment	Medium to slow deployment
Less planning	More planning
Dynamic backhaul	Fixed backhaul
Fault-tolerant	Non-fault-tolerant
Greater cost (more APs are required)	Lower cost

Table 2.8: Mesh Wireless versus Traditional Wireless

While considering a mesh access layer, it is also important to remember the potential negative aspects:

- Mesh devices use routing protocols that are usually proprietary in today's implementations.
- Over-engineering (needing more APs than a traditional deployment) may be required. Most implementations will not require over-engineering, but some scenarios may demand it to implement true mesh with redundant routes.
- Network delays may increase if too many mesh hops exist between the client and the wired network.
- The backhaul and the access traffic share the same wireless medium. Additionally, scenarios may exist where one AP provides the only link available for two or more other APs. This scenario reduces the true throughput for the APs passing through the single AP within the mesh. However, a dual-radio mesh node can solve this problem.

Common Wireless Architectures

To put the pieces together, this section will present the WLAN models that have evolved over time. I will start with the first model that was implemented using 802.11 technology, and then progress through the evolutionary stages of WLAN design models. While the models did not necessarily evolve in a precisely sequential order as presented here, the adoption of the differing models does seem to have followed a path much like this. Additionally, it is important to note that anything beyond the common intelligent edge model is beyond the scope of the IEEE standard. These more advanced models may still

utilize the standard for communications, but they implement the standard in a way not explicitly declared within the standard. The result is simple: anytime you use vendor hardware that implements 802.11 in a way other than the intelligent edge model, you will usually be locking yourself into that vendor's hardware for the infrastructure devices. However, any standards-based client should still be able to connect.

Note: **When working with the various wireless architectures, it is important to remember that the client devices will have a large impact on the performance of the network. The 802.11 standards specify how the AP and WDS work and the frames that can be passed between the clients and the AP, but the internal working of the client supplicant is up to the vendor. These variations can result in significant performance differences.**

Intelligent Edge or Distributed

The first devices to be released to the market were the standard autonomous "fat" or "thick" APs that are still used heavily today (sometimes also called controller-less APs). This kind of AP contains the entire logic system needed to implement, manage, and secure (according to the original 802.11 specification) a WLAN. The benefit of this type of WLAN is that implementation is very quick when you are only implementing a single AP or even a few. Conversely, a drawback to this type of WLAN is that implementation is very slow when you are implementing dozens or hundreds of APs. Many networks around the world have more than a thousand APs so scalability is important. Another drawback is that since autonomous APs are individually configured, errors are frequently introduced during the implementation and maintenance processes.

You can imagine the time involved if you have to set up each AP individually. At stage one, the intelligent edge, this was your only choice, though eventually WLAN network management (WNMS) solutions were introduced to ease the burden

The process for implementing an intelligent edge architecture looks like this:

1. Configure the AP according to your needs and security policies.
2. Bring the AP onto the live or production network.
3. Repeat until all APs are configured.

Yes, you can cheat and save the configuration from one AP and then load it onto another, but this methodology would be the only trick up your sleeve when it comes to automation before the introduction of WNMS solutions. One common solution was to use scripting tools to automate the configuration management, but the modern centralized management architectures are much more efficient and stable.

WLAN Network Management System or Centralized Management with Distributed Processing

When we arrive at stage two in the evolution of WLAN management, we encounter centralized configuration management with distributed intelligence. The devices and

software that provide this functionality comprise the WNMS. This stage provided much faster implementations of traditional fat or autonomous APs, and worked using SNMP or other proprietary communication protocols to configure and manage the APs across the network. The WNMSs usually supported the rollout of firmware so that the APs could be updated without having to visit each one individually. You would still need to touch every single AP to provide the initial configuration (i.e., change the SNMP from default communities or SNMPv3 with username/password) so that the APs could be managed by WNMS.

This model provided scalability, but did not reduce the cost of the APs and did not offset any processing from the APs so that they could handle more stations at each AP. In this model, autonomous APs are still used. Some cloud-based systems today are very similar to the older WNMS model. They may provide more monitoring and better management systems, but if the APs are still autonomous, it is basically a WNMS in the cloud.

Centralized WLAN Architecture or Split MAC

That brings us to stage three: centralized WLAN architecture. This networking model utilizes lightweight or thin APs (also called dumb APs) and depends on a wired network connection to the WLAN switches or controllers. The WLAN controller contains all the logic for processing and managing the WLAN. This configuration allows the APs to handle more client stations and provides for less complex implementation. For example, most of these systems allow you to connect the lightweight AP (sometimes called an access port to differentiate it from an AP) to the network that provides a connection to the WLAN controller and the AP and controller will automatically synchronize without any intervention from the engineer. Of course, there is still the requirement of initial setup and configuration of the controller, but moving forward it can be automatic. The items that are automatically configured may include the channel used by the AP, the encryption methods used, the SSID, and more. Profiles are created on the controller to pass down in configuration settings to the APs.

> **EXAM MOMENT:** Controller-based APs often use DHCP option 43 to locate a WLAN controller. They may also use DNS to locate the controller, if the vendor supports it. Additionally, they can use cached information from previous controller connections to locate the desired controller.

Hybrid WLAN Architecture

The hybrid WLAN architecture uses a WLAN controller like the centralized architecture and represents stage four in WLAN evolution. The difference is that hybrid APs are used instead of lightweight APs. A hybrid AP is an AP that can perform some or all of the functions needed within a BSS, and can also allow for some or all of these functions to be managed by the central controller. This is the model often used to enable distributed forwarding, which means that data traffic is sent directly to the destination instead of passing through the controller. Centralized forwarding requires that the traffic be passed to the controller, and the controller is responsible for sending it on to the destination address.

Unified WLAN Architecture

The unified WLAN architecture is where the wireless controlling functions are simply integrated into the standard wired switches used within our network cores. These

integrated switches may be deployed in an access or distribution role, but they are the same switches used for standard Ethernet communications. Add-on cards provide the capabilities needed for WLAN management.

Here, the switches that provide wired network functionality to wired clients also have the capability to serve the needs of wireless APs so that specialty wireless switches/controllers are no longer needed as separate devices. Today's centralized and hybrid solutions usually depend on a connection from the wireless controller to a wired switch that actually has connections to the APs. The future may see more development of multiport switches that have wireless controller functionality built in, reducing the need for an extra wired switch; however, this model has not caught on as the predominant model to this point.

Cloud-based Architecture

The cloud-based model simply places the management and/or control of the APs in the cloud. Instead of hosting a local controller on the network, the logic is placed in a vendor's resources in the cloud. Some cloud-based systems have all traffic passed through them for Internet access, and others distribute the forwarding of all data frames directly through the local APs to the network or Internet. Aerohive® and Meraki (Cisco) are examples of vendors that implement cloud-based architectures.

Multiple Channel Architecture (MCA)

The traditional WLAN architecture is the multiple-channel (multichannel) architecture (MCA). A multichannel architecture is built with careful planning that is maintained over time, though many modern vendors recommend using radio resource management (RRM) to implement MCA. The 802.11 PHYs that operate in the 2.4 GHz band provide three non-overlapping channels. In the United States, the non-overlapping channels are 1, 6, and 11. The 5 GHz bands offer many more non-overlapping channels with 802.11a/n/ac. I'll focus on the 2.4 GHz band here to make the explanations simpler. Strategically configuring APs to use channels 1, 6, and 11 and then staggering the channel usage throughout a coverage area allows complete coverage of larger areas.

As an example, consider the simple floor plan in Figure 2.6. Assuming this entire single-floor building needs coverage, multiple APs will be needed. In order to provide the highest data rates to all users, APs will be installed and power levels will be adjusted accordingly.

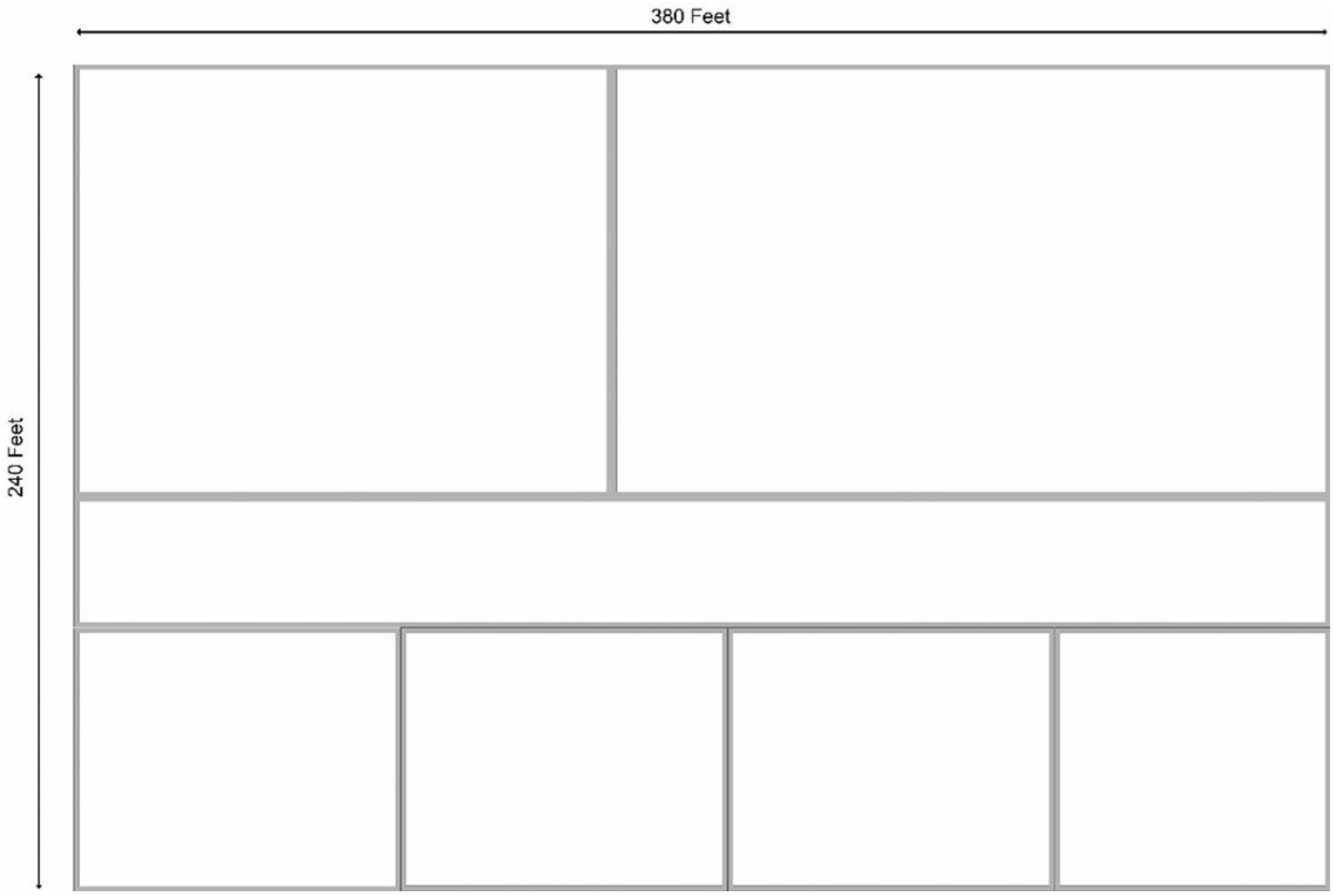


Figure 2.6: Floor Plan of Intended Coverage Area

MCA plans are often depicted with hexagons to represent the coverage of each omnidirectional antenna and AP pair. In the real world, antennas do not ever propagate the signals in a perfect hexagonal shape; however, the hexagon shape is useful as an early planning tool. Figure 2.7 shows a potential plan for covering the floor represented in Figure 2.6.

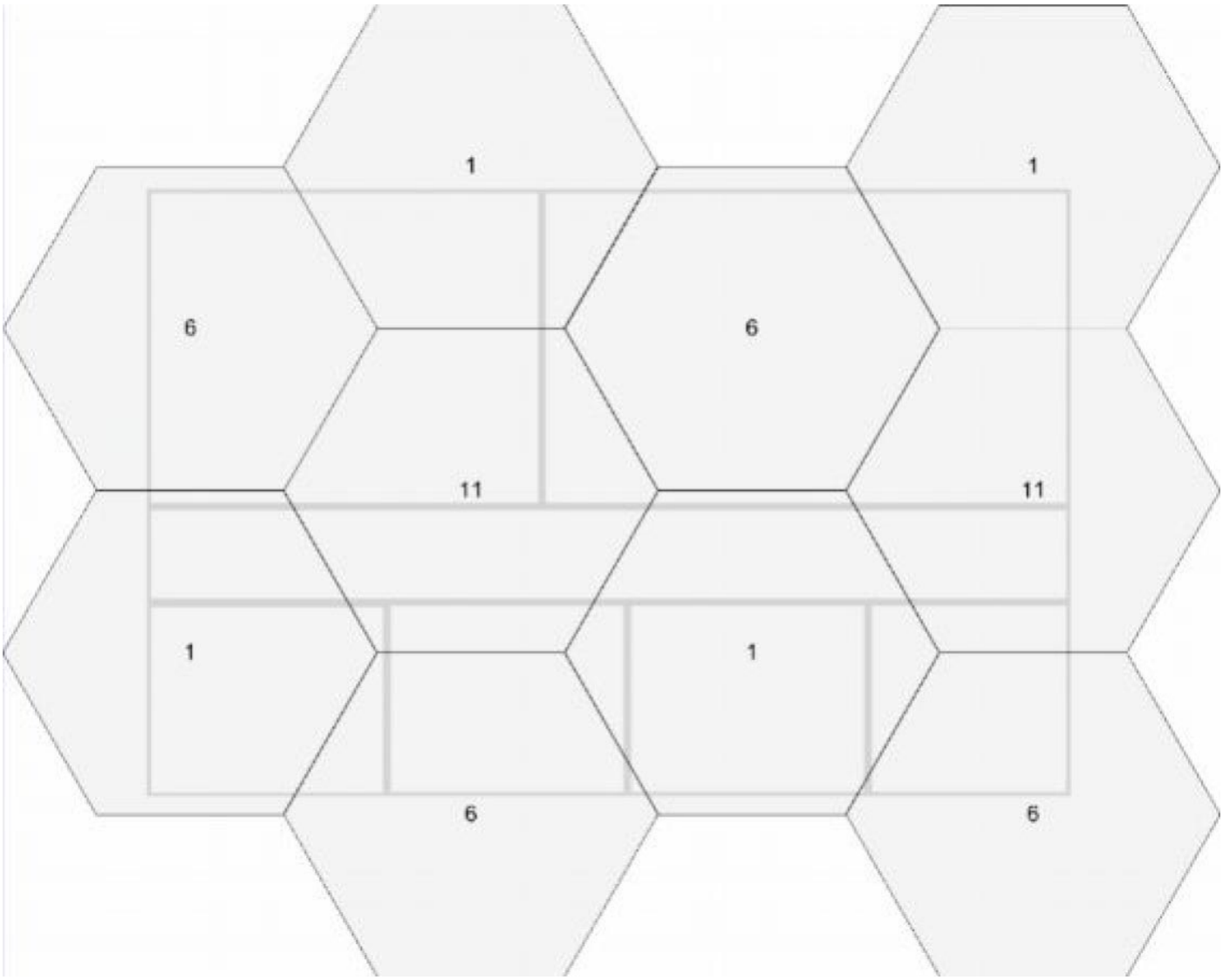


Figure 2.7: Hexagon Coverage Plan

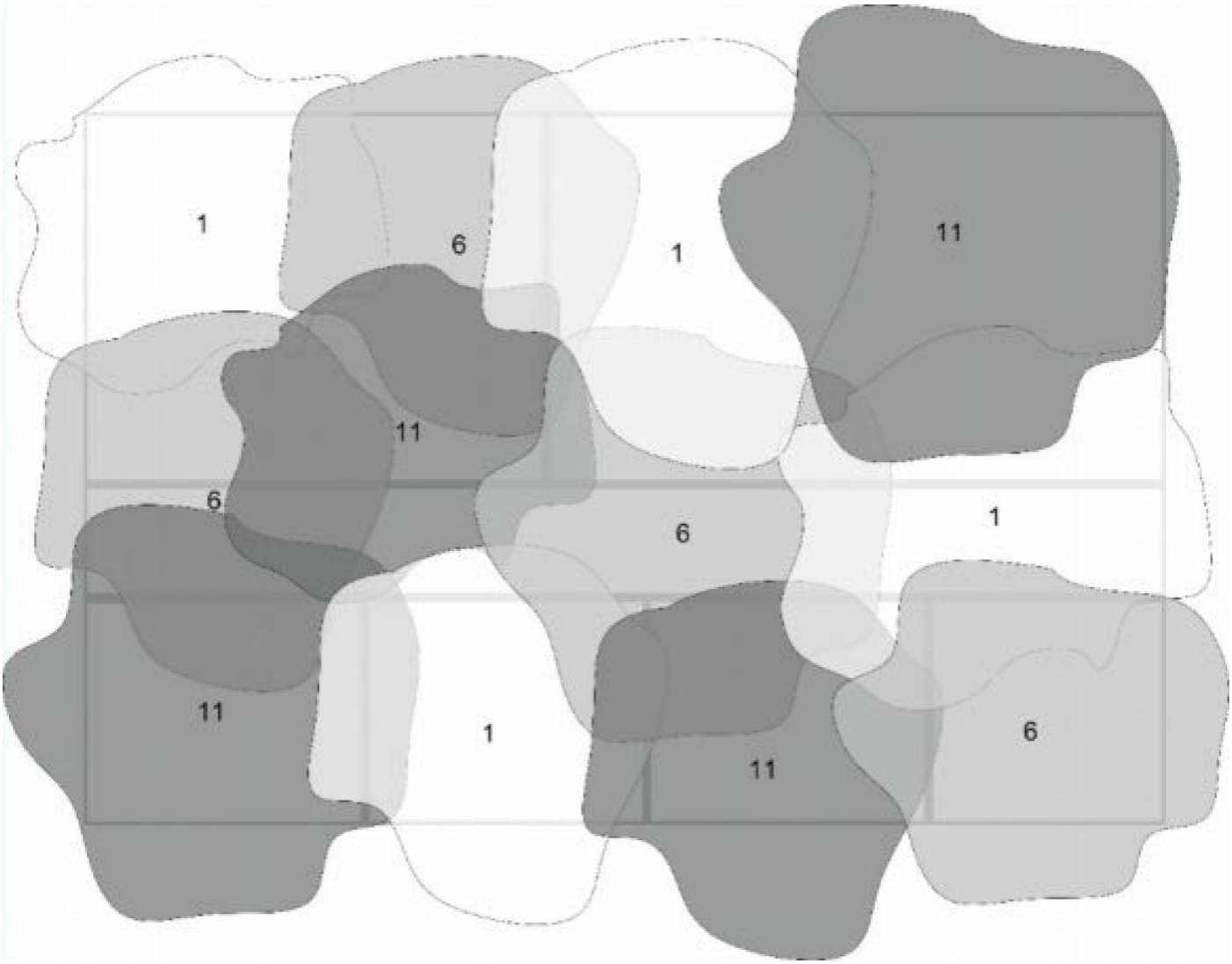


Figure 2.8: Realistic Coverage Plan

As painful as it is to look at, Figure 2.8 shows a more realistic view of an implementation pattern using MCA plans. As you can see, the coverage area (cell) created by each antenna/AP pair is not a nice, clean hexagon matching up perfectly with another cell. Instead, they form an ugly overlapping pattern that gets the job done while being influenced by real-world conditions.

Several problems are introduced with the MCA solution:

- Output power settings may vary at each AP, and this causes site surveys to be more difficult and time consuming.
- Adjacent-channel interference (interference among channels 1 and 6 or channels 6 and 11 or channels 1 and 4, as examples) is common, and measures must be taken to reduce it.
- It is more difficult to implement high client volume areas (such as conference and meeting rooms) within the context of a larger WLAN.
- Over time, WLANs require manual or automated adjustments as the environment changes.

One of these bullets, implementing high-client volume areas, demands further explanation.

Referring back to Figure 2.6, consider this: What if you need to provide coverage for 32

client stations in that room in the lower-left corner of the floor plan? To do this, you will usually need to install more than one AP in the area and, as you can see in Figure 2.8, channels 1 and 6 are already heavily represented in the area and channel 11 would certainly have some ghosting into the space, as well. You could provide a separate 802.11a/n/ac network using the 5 GHz band in that room, but this decision would prevent single-band client users from roaming in and out of the room. If roaming is not required, the issue is solved. If roaming is required, you will have to perform very careful adjustments to output power settings and AP locations to provide the needed connection bandwidth in the room, or you will have to upgrade all clients to support dual-band radios. Many newer clients already support dual-band radios, but the odds are very high that a laptop purchased in 2010 or earlier will have a 2.4 GHz band radio only. Some brand new clients sold in 2015 were also still 2.4 GHz only. High density is much easier in 5 GHz, but 2.4 GHz support is still required in most WLANs.

Single-Channel Architecture

Single-channel architecture (SCA) goes by many names, depending on the vendor, including Air Traffic Control (Meru, now Fortinet) and Channel Blanketing (Extricom) among others. The basic concept of SCA is simple: forget about cell planning; just implement multiple APs using the same channel and then control which APs are used to communicate at any moment with a centralized switch. The end result is zero cell-sized planning, zero initial configuration, and the ability to dedicate each SCA WLAN to a specific technology. For example, Figure 2.9 shows the same floor plan represented in Figure 2.6 being covered with SCA. Channel 1 could be used to traditional data. Channel 6 could be used for voice data, and channel 11 could be used for location services or any other need.

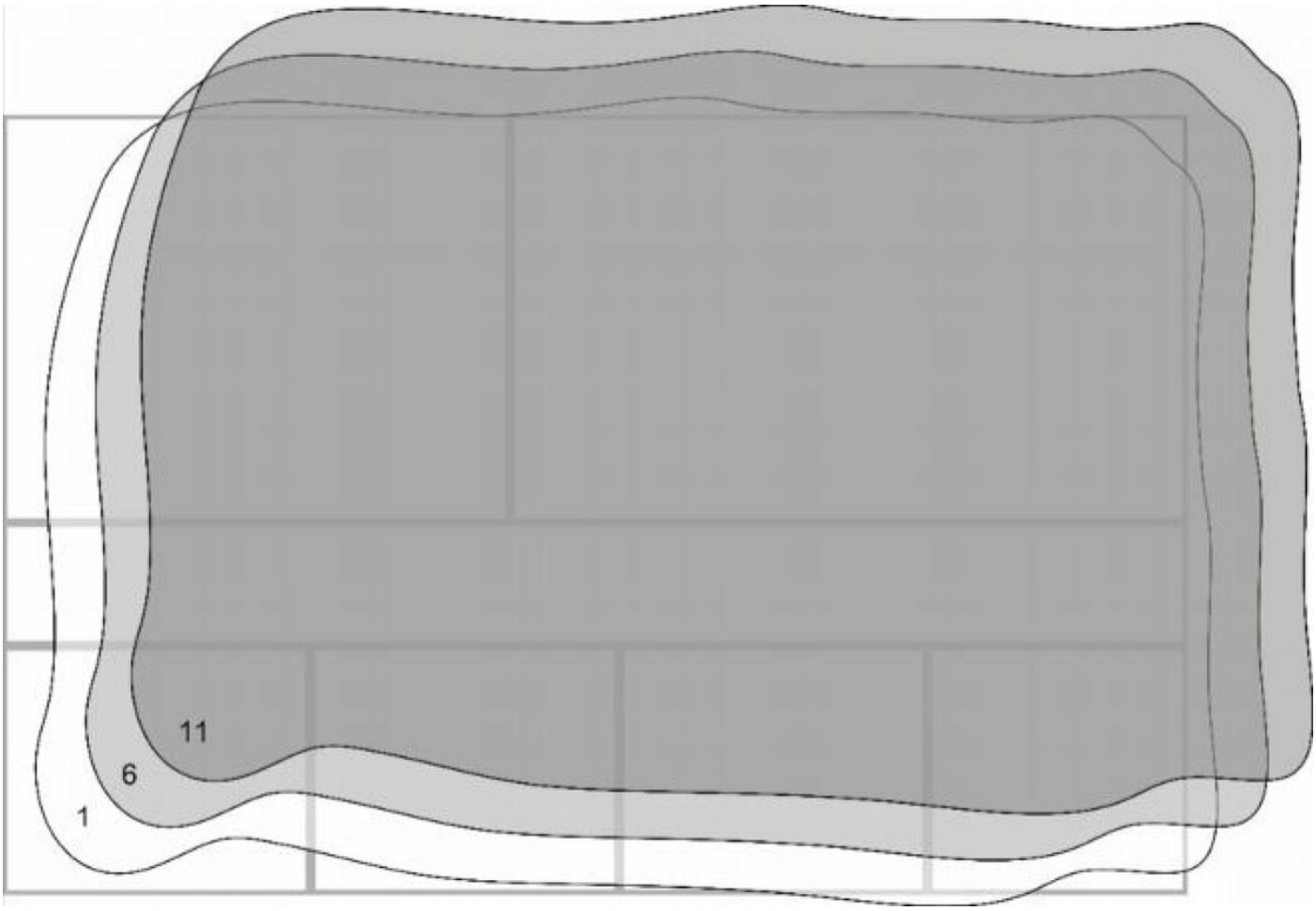


Figure 2.9: Single-channel Architecture Representation

One of the most important benefits of SCA is that roaming decisions are taken away from the clients and controlled by the WLAN switch. This means that roaming is fast, seamless, and secure. Questions remain about the scalability of this solution, but in smaller implementations, there is no argument about the simplicity of roaming management in the SCA plan.

However, just like MCA, SCA has potential drawbacks:

- Co-channel interference is only eliminated through the reduction of total bandwidth available in a given space.
- Centralized roaming decisions require more powerful WLAN switches and may not scale well.
- Adjacent-channel interference may become a bigger issue and decrease overall throughput, though this will not likely be a significant factor.
- The SCA network will cause more interference with neighboring MCA networks because of the “all channel” saturation is employs.

I think it’s important to talk about the first bullet point in more detail. SCA vendors usually state that co-channel interference is removed with their solutions. Co-channel interference occurs when two wireless stations communicate on the same channel in order to participate in different BSSs. Many engineers mistakenly assume that co-channel interference only occurs among APs; however, client stations can also (and are more likely to) cause co-channel interference. (You may recall studying this in CWDP, if you’ve

studied for that exam.) The SCA vendors suggest that co-channel interference is removed because of the centralized algorithms that determine which APs should communicate at any given time. However, these algorithms result in a potential reduction in overall throughput available on the WLAN. With SCA plans, frames will not be transmitted at the same time if the centralized controller determines that the transmitting APs would interfere with each other. This protects against co-channel interference on the downlink, but it does not help when the client stations communicate with the APs. Thankfully, many more frames are sent from the AP to the client in most WLANs, but the client transmissions are still a factor. For example, clients must acknowledge all those downlink frames with an uplink ACK frame.

With the MCA plans, frames may get through even though co-channel interference is high. Stated differently, two APs sufficiently separated can transmit a frame at the same time. A protocol analyzer located at either AP may be able to detect the other AP's communications, proving co-channel interference, but the frames may still get through. In the end, MCA plans that are configured for proper channel separation may result in greater throughput than SCA plans. Of course, as the SCA algorithms improve, this may become less of an issue.

The differences between MCA and SCA are important and must be considered carefully when choosing a WLAN vendor. Table 2.9 provides a comparison of the positive and negative trade-offs between these two potential solutions. As you can see, both solutions have pros and cons. Now you have more information to help you make an informed decision.

> **EXAM MOMENT:** SCA solutions usually use the APs as simple radios, and the 802.11 MAC layer operations are handled entirely in the central switch or controller.

Cooperative Control

Another WLAN architecture illustrates the creativity of wireless vendors. It is called Cooperative Control. As with all nonstandard implementations, the wireless technology professional should be cautious when selecting such solutions. If the vendor should go out of business, the entire infrastructure may have to be replaced for future upgrades or repairs. I will present a high-level overview of this architecture here, in order to expose you to a variety of options.

MCA	SCA
Positive: More control for the engineer	Negative: Less control for the engineer
Negative: More work for the engineer	Positive: Less work for the engineer
Positive: Results in less over-engineering	Negative: May result in more over-engineering
Negative: Implementation time is longer	Positive: Implementation time is shorter
Positive: The network can be completely based on standards	Negative: Some proprietary code must be used, at least in the infrastructure
Negative: Bigger networks require more intensive site surveys	Positive: The size of the network is irrelevant, but the model may not scale

Table 2.9: MCA versus SCA

Aerohive Networks developed the Cooperative Control Access Point (CC-AP) to address the limits of standard WLAN deployments.

CC-APs are a combination of a standard AP and specialized cooperative control protocols that provide similar functionality to that offered on WLANs that uses a centralized controller or switch. The CC-AP is called a HiveAP, and these APs exist in Hives that share information for fast and secure roaming, radio channel and power management, security, mesh networking capabilities, and Quality of Service (QoS).

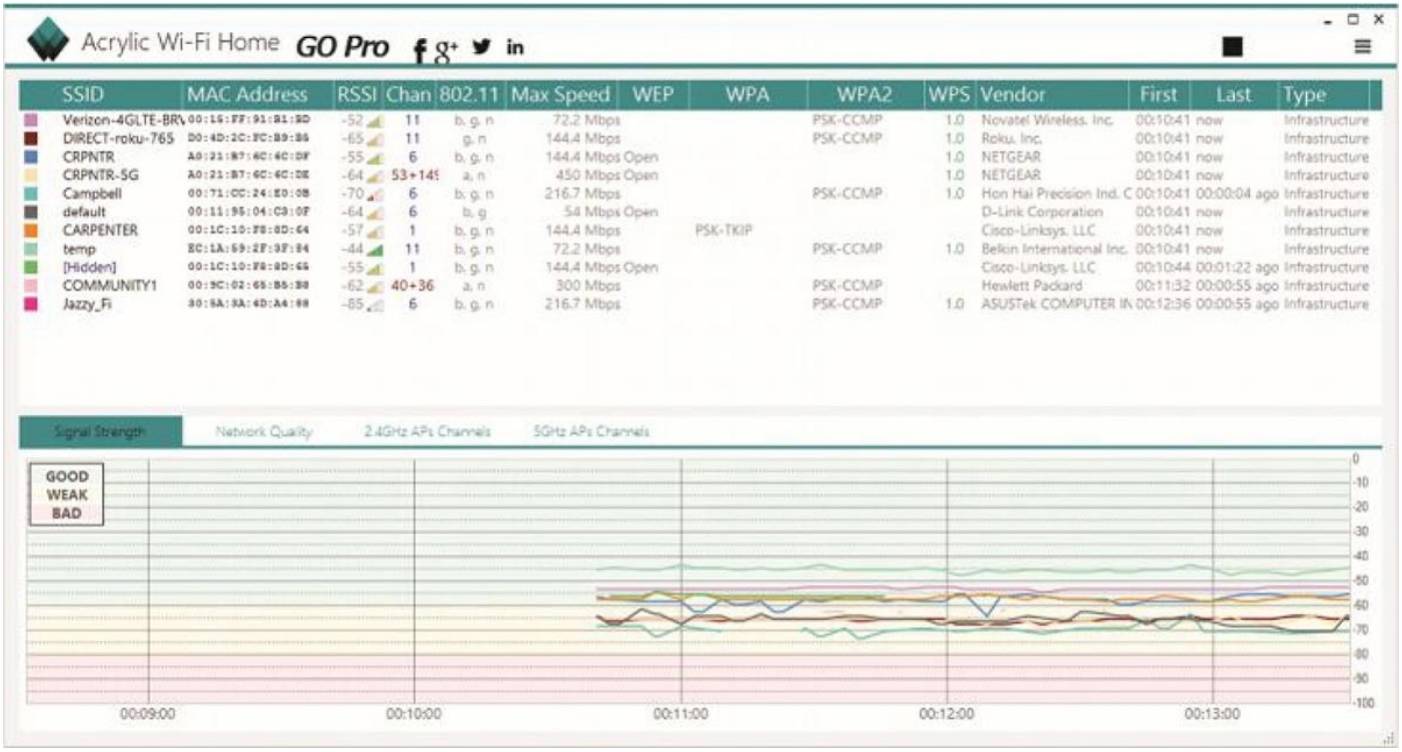
Two types of components work together to provide the cooperative control in a Hive: HiveAPs and a HiveManager. The HiveAPs are actual APs, and the HiveManager is software running on a system that centrally configures the HiveAPs, provides firmware updates, and supports monitoring and troubleshooting options. This cooperative control model is also cloud-based; however, the option for an on premise HiveManager is also available. The HiveManager software runs on a specialized appliance server.

The most important thing to remember about Hives is this: Hives are more proprietary than they are standard. You can connect any standard client to the Hive-based network, but you cannot connect any standard AP to the Hive. To learn more about this architecture, visit www.Aerohive.com.

Exercise 2

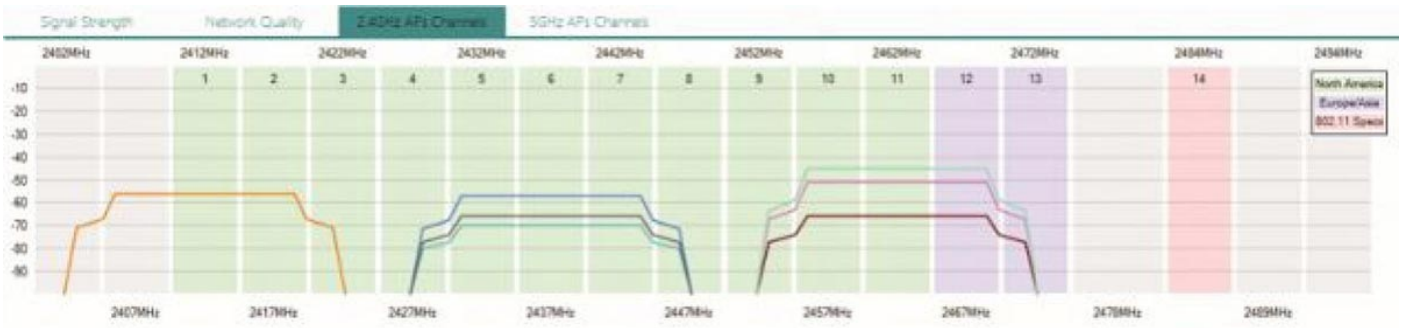
In this exercise, you will use the free Wi-Fi scanner Acrylic Wi-Fi Home to see the WLANs in your vicinity and explore the common features of such tools. Tools like this are used by even the most skilled WLAN engineers to quickly discover active networks in an area. This is an example tool and many tools provide similar information. This tool discovers the same information available to STAs during active or passive scanning.

1. Download the free version of Acrylic Wi-Fi home at: www.acrylicwifi.com
2. Install the software on your Windows computer equipped with a dual-band client (supporting both 2.4 GHz and 5 GHz.
3. Run the software.
4. Note the detected WLANs as in Graphic 2.1



Graphic 2.1: Acrylic Wi-Fi Home Showing Wlans on the Default Screen

5. Select the 2.4 GHz APs Channels tab to view only the 2.4 GHz networks discovered as in Graphic 2.2.



Graphic 2.2: Viewing the 2.4 GHz Networks

6. Notice the detected APs on each channel. Particularly note the channels with

multiple APs at better than -70 dB, such as channel 11 in Graphic 2.2.

7. Select the 5 GHz APs Channels tab to view only the 5 GHz networks discovered as in Graphic 2.3.

Graphic 2.3: Viewing the 5 GHz Networks

8. Finally, select the Network Quality tab and click on the different networks to view channel quality. Note that the overall network quality is a reference, in this application, to channel quality, signal quality, signal-to-noise, network security, transmission speeds and 802.11 standards as in Graphic 2.4.

Graphic 2.4: Viewing Network Quality Data

9. Close the application.

Chapter Summary

In this chapter, you studied the communications that take place in an 802.11 WLAN. First,

you reviewed the terminology used and then explored the CSMA/CA procedures defined in DCF. Enhancements to DCF providing QoS will be covered in more detail in Chapter 9. You also explored the various WLAN architectures used and the impact the have on performance and operations.

Review Questions

1. At Layer 3 of the OSI model, what is the data called?
    a. Frame
    b. Segment
    c. Packet
    d. MSDU
2. By what name is the MPDU referenced in the Physical Layer of the OSI model?
    a. MSDU
    b. MPDU
    c. PSDU
    d. PPDU
3. Which one of the following factors has the greatest impact on the data rate usable by a WLAN STA?
    a. Whether Block ACKs are used or not
    b. Duration of the frame
    c. Cable length
    d. SNR
4. In addition to the NAV being 0 and the Backoff Timer being 0, what must be true for a WLAN radio to begin transmitting a frame?
    a. The Length field in the PLCP header must be 0.
    b. The IP packet must be included in the frame.
    c. The CCA must return an idle state.
    d. Nothing else is required.
5. In the DCF arbitration process, where is the interframe space utilized?
    a. Before the backoff timer begins
    b. After the backoff timer ends
    c. After the CCA reports an idle state
    d. Between symbols
6. What IFS is used by a STA immediately after a data frame is received to send an ACK frame?
    a. AIFS
    b. DIFS

c. SIFS

d. PIFS

7. What maximum number of MCS values is available for a given scenario including the number of spatial streams and the channel width?

a. 72

b. 10

c. 9

d. 11

8. Which interframe space is the shortest among those listed?

a. DIFS

b. SIFS

c. RIFS

d. PIFS

9. From what source is the NAV timer set in standard 802.11 operations?

a. PLCP header

b. DurationID field

c. NTP server

d. Local clock

10. Between what does the short-guard interval provide space?

a. Symbols

b. Segments

c. Frames

d. Data Frames and ACK Frames

11. What DHCP option is often used by lightweight APs to locate a WLAN controller?

a. 54

b. 43

c. 90

d. 18

12. When configuring an AP for optimal operations in the 2.4 GHz band, what channel should be avoided?

a. 1

b. 3

c. 6

d. 11

13. As the WLAN analyst for your organization, you must locate all wireless networks detectable within the facility. What utility can be used to perform this operation without complicated training classes or long learning curves?

    a. Wi-Fi scanner

    b. A spectrum analyzer

    c. A protocol analyzer

    d. WLAN controller interfaces

14. What WLAN architecture utilizes a centralized device through which all WLAN traffic passes?

    a. Coordinated Control

    b. Controller-based

    c. Intelligent Edge

    d. WNMS

15. What model is defined as including all logic and processing within the AP for MAC and PHY operations?

    a. Split MAC

    b. Single MAC

    c. Controller-based

    d. Switch-based

16. If DHCP does not provide the location of a WLAN controller, what other option may be used by an AP?

    a. DNS

    b. The Controller field in the MAC header

    c. The Management field in the PLCP header

    d. WINS

17. What follows the SFD field of the PLCP preamble?

    a. MAC header

    b. MSDU

    c. MPDU

    d. PLCP header

18. What theorem defines the maximum bandwidth capabilities of a channel?

    a. Nyquist

    b. Shannon-Hartley

c. Polyhedron

d. Binomial

19. What standard defines the channels that will be actively scanned with probe requests for 802.11 WLANs?

    a. IEEE 802.11

    b. There is not a standard; it is vendor-proprietary.

    c. IEEE 802.2

    d. ISO 9000

20. What is the SIFS time for the 802.11ac PHY?

    a. 16 microseconds

    b. 9 microseconds

    c. 20 microseconds

    d. 50 microseconds

21. When is EIFS used?

    a. Only in 802.11ac networks

    b. When a frame is being received but is corrupted or not fully received

    c. Only in 802.11n networks

    d. Only in FHSS networks

22. What is the slot time for the OFDM PHY?

    a. 20 microseconds

    b. 9 microseconds

    c. 16 microseconds

    d. The OFDM PHY uses no slot times

23. What level of guarantee is given by EDCAF to WLAN traffic?

    a. Certainty of priority

    b. Level 0

    c. Probabilistic priority

    d. Level 5

24. Which PHY has the higher priority access to the medium based on slot times?

    a. HR/DSSS

    b. FHSS

    c. OFDM

    d. DSSS

25. What 802.11 amendment defined a mesh BSS?

a. 802.11a

b. 802.11k

c. 802.11r

d. 802.11s

Review Question Answers

1. **C** is correct. IP packets are created at Layer 3 or the Network Layer. The IP packets include an IP header and footer surrounding the TCP segment or UDP datagram.
2. **C** is correct. When a layer receives a PDU from the layer above, it becomes an SDU; therefore, the PHY references the MPDU as a PSDU and uses it to create the PPDU, which will include the PLCP header for transmission.
3. **D** is correct. SNR is the most important factor in determining the data rate a client or AP can use to receive a frame. Data rates will be shifted to lower rates based on retries in order to accomplish a rate at which the other STA may effectively receive.
4. **C** is correct. At all times, the CCA must return idle or a frame cannot be transmitted. This is true regardless of any other parameters in the DCF operation.
5. **A** is correct. The IFS is used before the backoff timer starts. This allows for STAs needing to send important frames, like ACK frames, to begin contention before STAs with less important frames, like data frames.
6. **C** is correct. The short interframe space (SIFS) is used so that the acknowledgement (ACK) frame can accomplish greater likelihood of access the medium before any other STAs frame.
7. **A** is correct. MCS values of 0-9 are available in the appropriate configurations. Not all configurations support all MCS values, but 10 is the maximum number available for a given configuration, for example, 3 spatial streams and a 20 MHz channel.
8. **C** is correct. The reduced interframe space (RIFS) is the shortest and is only used in limited 802.11n scenarios. It is removed from 802.11ac and may be completely removed in the future.
9. **B** is correct. The Duration or DurationID field is used to set the network allocation vector (NAV) timer that is used in the DCF arbitration process.
10. **A** is correct. Guard intervals are used between symbols to prevent intersymbol interference.
11. **B** is correct. DHCP option 43 is the common parameter used to provide the location of the WLAN controller via its IP address.
12. **B** is correct. Channels 1, 6 and 11 should be used for optimal performance in regions supporting only channels 1-11. Channel 3 should not be used in any practical scenario.
13. **A** is correct. A Wi-Fi scanner is a simple tool used to locate and display all WLANs and information regarding them.
14. **B** is correct. A controller-based architecture is also called a centralized architecture. Newer controller-based WLANs support both centralized and

distributed data forwarding, however.

15. **B** is correct. The single MAC model includes all required 802.11 processing in the APs.
16. **A** is correct. APs can use DHSP option 43, DNS, broadcasts, and the internal cache to locate a WLAN controller.
17. **D** is correct. The PLCP header follows the preamble and the start-of-frame delimiter (SFD) is the final portion of the preamble.
18. **B** is correct. The Shannon-Hartley theorem defines the channel capacity as a factor of bandwidth, signal and noise.
19. **B** is correct. The standards do not define supported channels for STAs. The supported channels are defined by the chipset and/or drivers used or created by the vendors.
20. **A** is correct. The SIFS time for the 802.11ac PHY is 16 microseconds, which is true for all 5 GHz OFDM PHYs.
21. **B** is correct. When a frame is being sent and it is lost in the middle of reception, EIFS is used to ensure that a frame sent from the STA that lost the frame does not interfere with other communications.
22. **B** is correct. The slot time for the OFDM (802.11a) PHY is 9 microseconds.
23. **C** is correct. Probabilistic priority is made available through EDCAF. The higher priority frames have a greater likelihood of being transmitted first, but they do not have a guarantee of being transmitted first.
24. **C** is correct. Because the OFDM PHY has a small 9 microsecond slot time, it has higher priority access than the other listed PHYs.
25. **B** is correct. An MBSS (mess BSS) is defined in 802.11s and, having been ratified, is now part of 802.11-2012.

Chapter 3:

802.11 Frames

Objectives

2.3 Understand and explain the 802.11 frames including general frame format, management frames, control frames, data frames, and how they apply to WLAN analysis.

2.4 Understand and explain the 802.11 PHY header and preamble and the indications for WLAN performance and operations.

Wired and wireless local area networks (LANs) use MAC layer frames for communicati between Data Link Layer network peers. These peers might include a wired computer communicating with a switch or another server on the same switch or broadcast domain. In Wi-Fi, these peers typically include wireless client STAs communicating with APs and vice versa. This chapter will provide detailed information on frames and frame formats. The information provided will help you better understand both 802.11 communications and the use of protocol analyzers, which are covered in Chapter 5.

Framing Review

In the previous chapter, you learned that frames are a collection of organized or meaningful bits. Both devices (the sender and receiver of the frame) must understand the meaning of the bits. This mutual understanding is what we mean by the term protocol. In computer networking, a protocol is a standardized set of bits and communication procedures used to transfer information between two devices. The bits may be standardized by an industry organization like the IEEE or IETF, or they may be standardized in a proprietary manner by a vendor. Either way, they are meaningfully standardized and can be used for communications.

A frame in computer networking shares similarities with a frame in a window. The window is the glass, and the window frame is the wood or metal around the glass. The purpose for the frame is to provide for handling of the glass. That is, the glass is what you want for functionality, and the frame allows you to install it. In a similar way, many frames are simply carriers of desired information on the network. The frame is sent in order to transfer the body of the frame (when considering data frames). The point of sending a data frame is not to send the frame itself, but the data contained in the frame. However, some organized method of sending that data must exist, hence we have frames.

I find it helpful to begin with a simple example of a fictitious frame. Imagine that you want to have a way to send words between two devices. Words like “horse,” “cat,” and others. However, you have to define the target device and the source device to do so. In this simple example, we’ll assume that’s primarily what you have to do. Furthermore, assume that in this simple example, no more than four devices can exist on the network. Therefore, we need only two bits for the source and two bits for the destination based on the fact that two bits (for example, 01 or 10) can represent up to four values (0, 1, 2 and 3) and therefore four devices. Our frame header and data would look like this (showing the actual word as text instead of bits for simplicity at this point):

```
SRC      DST      DATA
 ##  |   ##  |   word
```

Where SRC is the source address consisting of two bits and DST is the destination address consisting of two bits. Now, assume the following devices are on this simple network:

- Computer1 – 00
- Computer2 – 11

- Computer3 – 01
- Computer4 – 10

If Computer1 desired to send the word “horse” to Computer4, the frame would look like this (showing the actual word as text instead of bits for simplicity):

```
0010horse
```

At the Physical Layer, the network adapter would need to generate the signal for 0 twice, then the signal for 1 once and then the signal for 0 again, followed by the signals for the bits representing the word horse. The receiving devices would all be listening for bits three and four in the frame to see if it is for them. Computer4 would see that bits three and four are equal to its own address (10) and then receive the rest of the data, in this case, the word “horse.” Computer2 and Computer3 would see that bits three and four are neither 11 nor 01 and know that they can ignore the rest of the data.

The benefit of knowing the source device is that the receiving device could respond with an acknowledgement frame to indicate that the transmitted frame was received as expected. That is, Computer4 could send back a standard acknowledgement message to Computer1. In our simple example, let us say that an acknowledgement is simply a set of four ones after the SRC and DST bits. Computer4 would send the following frame:

```
10001111
```

To take it one step further, if the word received was not recognized, the receiver may assume corruption has occurred and respond with a frame indicating such. Let us say that a corrupt data notification is simply a set of four zeros. Computer4, in this case, would send the following frame:

```
10000000
```

Note: **This binary concept reminds me of my favorite T-shirt that reads, “Binary is as easy as 01, 10, 11!” and another favorite that reads, “There are 10 kinds of people: those who understand binary and those who don’t!” The point here, is that, if you don’t know basic binary, you can’t understand computer math and communications. This chapter and the preceding one should help with that.**

This simple example illustrates the concept of a protocol—a standard way to communicate on the network. While this scenario is not as complicated or capable as protocols used in either Ethernet (802.3) or Wi-Fi (802.11), it illustrates the true simplicity behind frames and their use on the network. With this basic understanding, you can go further and easily understand the more detailed frame formats in Ethernet and Wi-Fi. In the rest of this section, I will provide a brief overview of Ethernet frame formats, as they are also helpful in fully understanding Wi-Fi frame formats. First, a few terms should be understood as they are often used when discussing frames and packets and the meaning of the bits used.

- **Most significant bit (MSB):** The bit having the highest value in binary notation. Also called the left-most bit as it is usually the bit in the left position in binary

notation (though this is not always true in the standards that define communication bits). The MSB is also called the high order bit. For example, in the 802.11 standard, the subtype field for frame type identification is specified with “the most significant bit (MSB) of the Subtype field, b7, is defined as the QoS subfield.” This simply means that bit b7 (the identifier of the bit based on position) is equal to 1 for all QoS subtypes, and it is equal to 0 for all non-QoS subtypes in data frames or, stated differently, this bit determines if it is a QoS data frame or not. For example, all data frames are defined with a Type field value of 10, but the subtype field value of 0000 is standard data and the subtype field value of 1000 is QoS data.

- **Least significant bit (LSB):** The bit having the lowest value, and the one that determines even or odd value when converted to decimal. Also called the right-most bit as it is usually the bit in the right position in binary notation.
- **Most significant bit first (MSBF):** Indicates that, when receiving bits, the MSB is received first and the LSB is received last. Both 802.3 and 802.11 transmit the least significant bit first instead. The opposite is LSB first (LSBF)

Here is an important example of these terms from the IEEE 802.11-2012 standard:

In control frames of subtype PS-Poll, the Duration/ID field carries the association identifier (AID) of the STA that transmitted the frame in the 14 least significant bits (LSB), and the 2 most significant bits (MSB) both set to 1. The value of the AID is in the range 1–2007.

This statement means that the two MSBs of the DurationID field determine if the field represents a duration or an AID. If it represents an AID, the two bits (remember, the MSBs) are set to 11. If it carries the duration of the frame, the bit (in this case the single MSB) is set to 0. Further study of the standard reveals that the two MSBs can be set to 01 to represent PCF, but this will never be seen in production networks as PCF is not used (as you may recall from CWNA and CWSP). Interestingly, the MSBs are bits 14 and 15 with bits 0-13 being the LSBs in this case; therefore, the MSBs are the right-most bits and not the left-most bits. However, 802 standards typically define bits from LSB to MSB and state that the LSB is transmitted first and the MSB is transmitted last, such as in 802.3-2012 Ethernet, clause 3.3. For more information in this specific scenario related to the DurationID field, see the 802.11-2012 standard clause 8.2.4.2.

Ethernet Frames

In this section, we will explore the Ethernet (802.1-2012) frame format. It is far simpler than 802.11 frames because it does not have to provide as much logical management of the medium (wires for Ethernet and RF for Wi-Fi). Additionally, as a WLAN analyst, you will find many situations where you must perform analysis on the Ethernet side to troubleshoot wired issues as discussed in Chapter 7.

The first thing to explore is the 802.3-2012 diagram of the Ethernet communications process, as it links back to our discussion of MSBs and LSBs and brings it into the real world. Figure 3.2 shows the diagram as presented in the standard.

Note: **This section discusses the basic Ethernet frame and does not include discussion of expanded frame options like 802.1Q VLAN and QoS (using priority code point (PCP) tags) tagging and Jumbo frames. These topics are beyond the scope of discussion at this point. However, they will be addressed briefly in Chapter 7 in the discussions of wired networking issues that impact WLAN operations.**

To read the Ethernet communications model diagram accurately, consider that the information that appears to be in layers could also be presented side-by-side from left to right instead of from top to bottom, which is a more common way to display a frame. However, the IEEE chose to represent the model in this way within the standard and it does provide a more compact viewing arrangement. Also, remember that the term octet is the accurate term for an 8-bit byte to differentiate it from any other byte length that may be used.

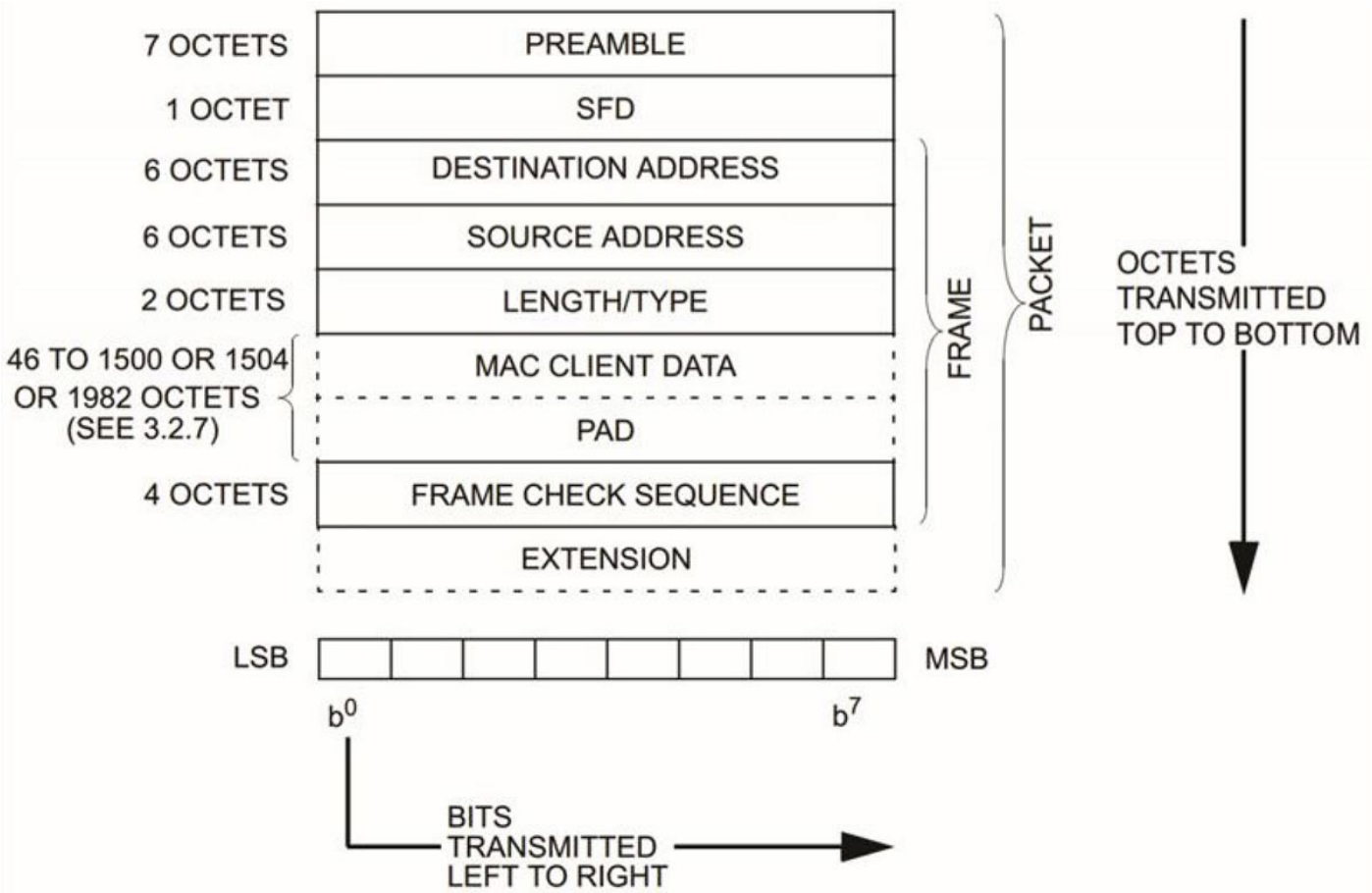


Figure 3.1: Ethernet Communications Model

Preamble

Like with 802.11 PHY frames, 802.3 frames are sent with a preamble and start-of-frame delimiter (SFD) prepended to the MAC frame. The preamble is 7 octets (56 bytes) and is used to allow the physical signaling sublayer (PLC) circuitry to enter steady state synchronization so that its timing is aligned with the incoming frame on receipt. It is like a wakeup call to the receiving network interface adapter (NIC). The Ethernet preamble is simply:

```
10101010 10101010 10101010 10101010 10101010 10101010
10101010
```

The preamble bits are sent LSBF with the bits sent as presented here from left to right; or with the left-most bit first.

SFD

Next is the SFD. It is the simple sequence of bits `10101011`. Note that the preamble ends with a `0`, but the SFD ends with a `1`. This change in pattern tells the receiver that the MAC frame begins immediately thereafter. As you can see the PHY header for Ethernet is very simple. You will see that the PHY header and the preamble and SFD all combined are more complex for 802.11 communications in the later sections titled 802.11 PHY Preamble and 802.11 PHY (PLCP) Header.

DA and SA Fields

The actual Ethernet MAC frame consists of four basic fields, with possible extensions:

- Destination Address (DA)
- Source Address (SA)
- Length/Type
- Frame Check Sequence (FCS)

The DA is the MAC address of the receiver and the SA is the MAC address of the transmitter. The DA and SA fields use the format shown in Figure 3.2. The first bit of the field identifies whether the address is targeted at an individual or a group. If equal to 0, it is targeted at an individual address. If equal to 1, it is targeted to a group address. The second bit of the field identifies whether the address is globally or locally administered. A globally administered address is set to 0 and a locally administered address is set to 1. Given that a MAC address is 46-bits (the actual address), the extra two bits for I/G and U/L bring the total field size to 48 bits or six octets (bytes). MAC addresses are typically said to be 48 bits or six octets long; however, in reality the Ethernet standard simply uses the normal format for a MAC address for the DA and SA fields, which is to have the first two bits (or the first and second LSBs) identify the address type and the 46 MSBs to identify an actual unique address for the devices.

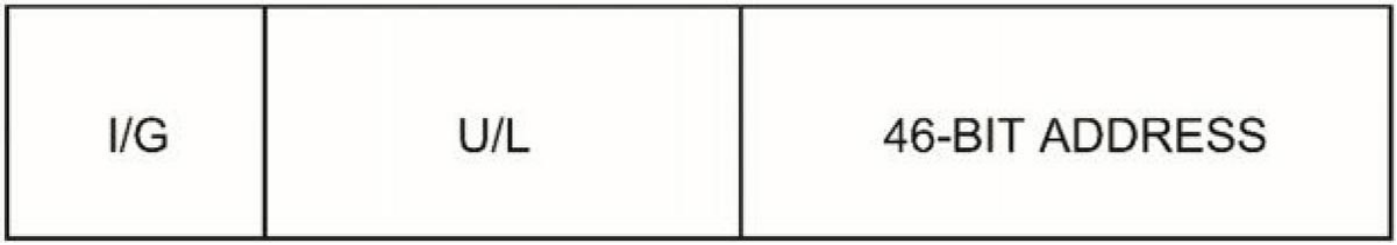


Figure 3.2: The DA and SA Field Format

Group addresses, when the I/G bit is set to 1, can include multicast and broadcast addresses. Multicast addresses are associated based on a higher-level protocol, and the addresses are somehow logically related in a method outside of the direct Ethernet specification. The broadcast address is simply 46 ones (or all ones) in the 46-Bit Address subfield of the DA or SA field.

A locally-administered address (indicated by a 1 in the U/L subfield) is an address assigned by the administrator instead of using the burned in address (BIA). The BIA is a globally administered address.

Length/Type Field

The next field in the Ethernet frame is the Length/Type field. This field either specifies the length of the MAC Client Data or it specifies the Ethertype of the client protocol. Table 3.1 provides examples of the Length/Type field being used to identify the Ethertype.

Protocol	Length/Type Value in Hex	Length/Type Value in Binary
IPv4	0x800	0000 1000 0000 0000
ARP	0x806	0000 1000 0000 0110
LLDP	0x88CD	1000 1000 1100 1101
EAP over LAN	0x888E	1000 1000 1000 1110

Table 3.1: Ethertype Values Commonly Used in the Length/Type Field

The Length/Type field is often simply called the Type field in modern documentation as it is mostly used for this purpose today.

Data Field

The data field contains the actual payload from the upper layers (Network through Application). Ethernet implementations support a standard frame size of 1518 bytes, with 18 bytes consumed by the DA (6 bytes), SA (6 bytes), Length/Type (2 bytes) and FCS fields (4 bytes). Therefore, the payload can be up to 1500 bytes. However, payloads of larger sizes are supported by many complex variations including Jumbo frames. For our purposes here, the standard size of 1500 bytes is sufficient.

When the data field is not as long as the minFrameSize value, it must be “padded” to equal that size. The padding is appended to the MAC client data (the upper layer payload). This padding is required for proper CSMA/CD operation, and the actual padding bits are not defined in the standard. The minimum frame size (minFrameSize) is defined as 512 bits or 64 octets for all Ethernet PHYs from 10 Mbps through to 100 gigabits per second (Gbps).

FCS

The FCS field contains bits that are used to validate the integrity of the frame. The FCS field provides integrity for the DA, SA, Length/Type and Data fields (including padding if it is required as mentioned in the Data Field section previously). The FCS field contains a cyclic redundancy check (CRC) value. It is 4 octets long or 32-bits. The CRC bits are placed into the FCS field in reverse so that the MSB is received first even though Ethernet

frames in entirety are said to be transmitted as LSB to MSB.

Extension

The Extension field is used when the frame would be less than a slot time in the applicable Ethernet PHY. The field ensures that a frame consumes a slot time. The calculation of the extension field is as follows:

```
slotTime - minFrameSize
```

Figure 3.3 shows a capture of an Ethernet frame in Wireshark (an open source protocol analyzer). Notice the Type field is set to 0x800 as in Table 3.1 and has been decoded (converted to explanatory output) by Wireshark as IPv4.

802.11 General Frame Format

Now that you understand framing concepts in general and have explored a real-world framing implementation that is much simpler than 802.11, you can better understand 802.11 frames. This section explores the general frame format used in 802.11 framing. The next sections, 802.11 Frame Types and Important 802.11 Frames, go into the specific frames used for significant actions on the WLAN link.

Figures 3.4 through Figure 3.7 show the general frame format as it has evolved from 802.11-prime (1997) through 802.11-2007, then through 802.11-2012, and finally as presented in 802.11ac. The following pages explain the purpose of the various fields described in the figures. Just as with Ethernet, the 802.11 Wi-Fi frame surrounds and carries the MSDU, but 802.11 frames are also used without upper layer payloads for management purposes. This important point will become clear throughout this chapter.

Figure 3.4 shows the original 802.11-1997 (or 802.11 prime) general frame format. At this point the frame is as simple as it gets for 802.11, and greater complexity is added as new capabilities are introduced. Figure 3.5 shows the general frame format as it appeared in 802.11-1999, which included the addition of the 802.11a and 802.11b PHYs. As you can see, no changes were introduced to the general frame format with the introduction of these PHYs. The first significant change to the general frame format came with the introduction of 802.11e in 2005, which introduced QoS to the standard. To be clear, in 2004, the 802.11i amendment introduced some changes in subfields, such as the renaming of the WEP field of the Frame Control Subfield to Protected Frame instead. This allowed the field to indicate that encryption was used, but did not require that the encryption be the then-proven weak Wired Equivalent Privacy (WEP) algorithm.

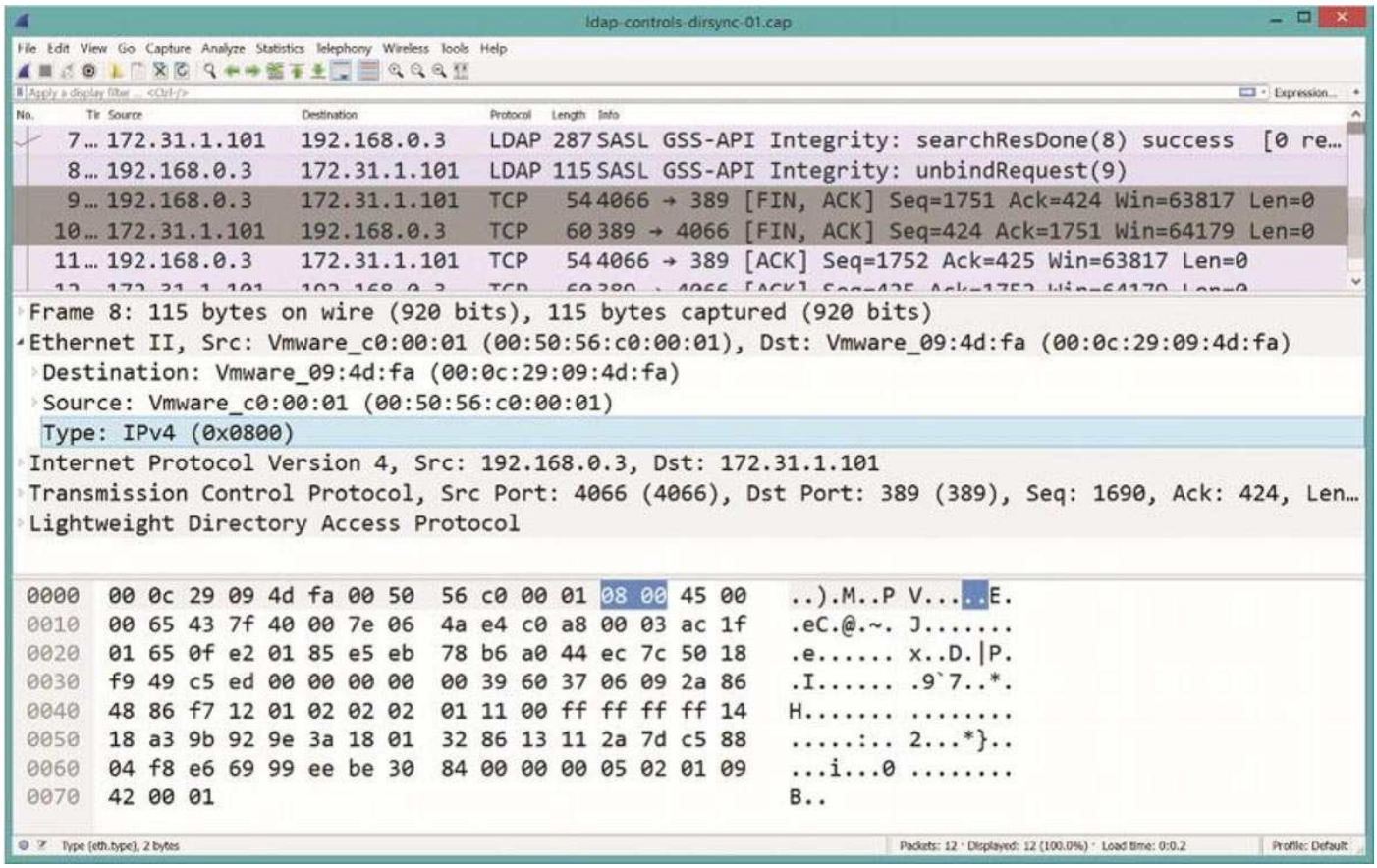


Figure 3.3: An Ethernet Frame (LDAP) in Wireshark

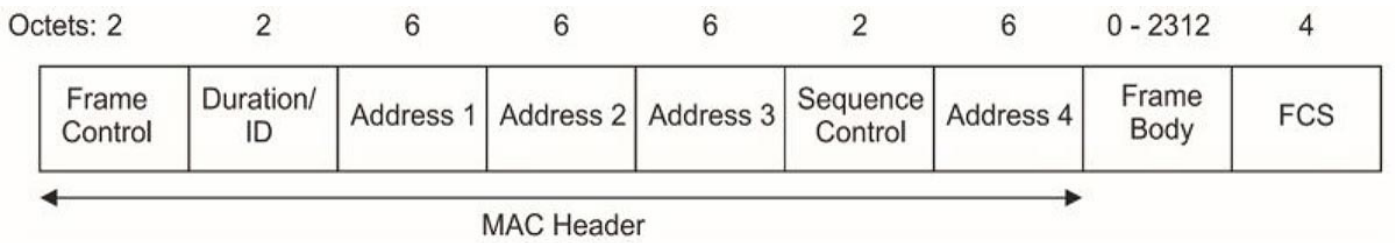


Figure 3.4: 802.11 General Frame Format from 802.11-1997

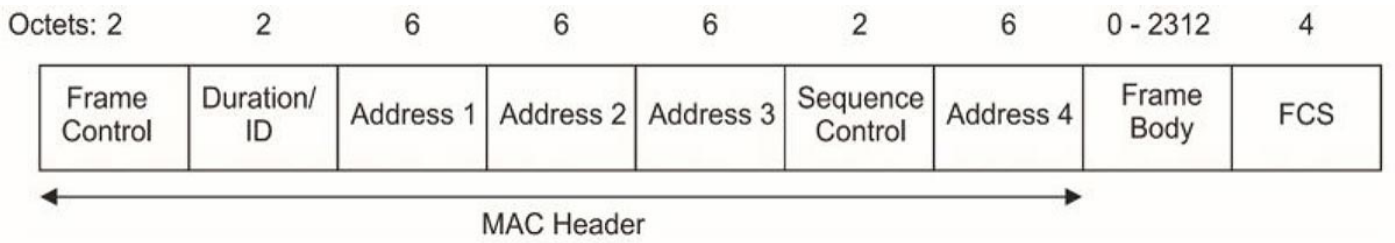


Figure 3.5: 802.11 General Frame Format from 802.11-1999

The frame changes made in 802.11e were incorporated into 802.11-2007 and are shown in Figure 3.6. Notice that the Frame Body field is no longer specified as 0 – 2312, but instead as 0–2304. This change was actually made in 802.11e and rolled into 802.11-2007. The typing mistake shown in figure 3.6 is from the actual standard. It should read 0-2304 and not 0-2324.

Because 802.11e was all about QoS, it also added the QoS Control field used to pass QoS information and define queue operations in the STAs.

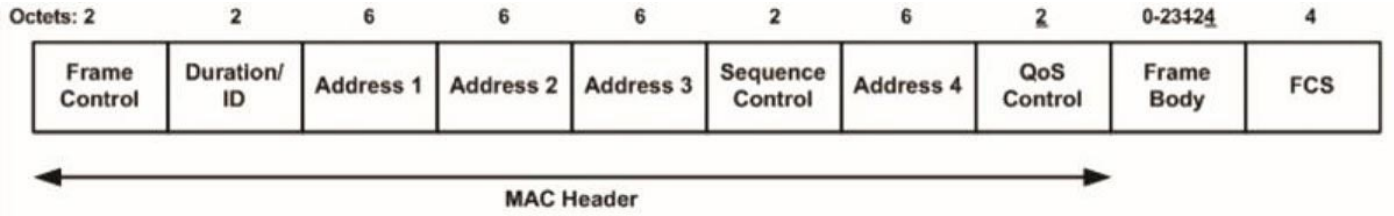


Figure 3.6: 802.11 General Frame Format from 802.11-2007

The next big change to the general frame format came with the ratification of 802.11n in 2009, and was incorporated into 802.11-2012 in the rollup of the standard. Figure 3.7 shows this change allowing for a longer frame body when aggregated MSDU (A-MSDU) frames are constructed (the size limit is still 2304 when non-A-MSDU frames are constructed). Additionally, you can see that 802.11n introduced the HT Control field, which contains information related to transmit beamforming and antenna selection (ASEL), among other items.

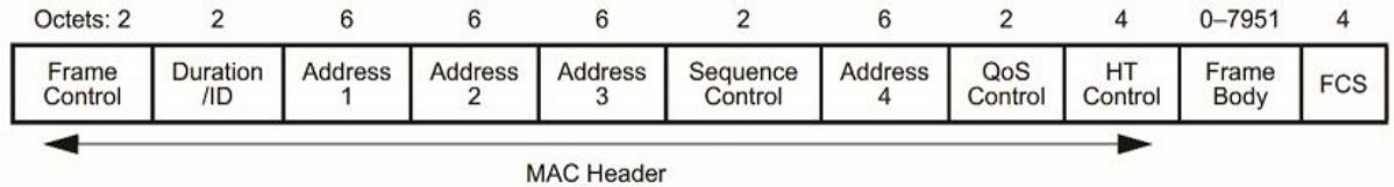


Figure 3.7: 802.11 General Frame Format from 802.11-2012

The final general frame format in this book is the 802.11ac frame format. Only a slight change in appearance is made, but it is significant in implementation. Figure 3.8 shows the new 802.11ac general frame format. Notice that the Frame Body field now says only "variable" for the length. The standard simply states that the Frame Body field is of variable size and is constrained with a minimum length of 0 octets and a maximum length based on the maximum MMPDU (mesh MPDU), MSDU, A-MSDU, and MPDU sizes of the recipients for the PPDU format in use. Additionally, when fields such as QoS Control, Address 4 and HT Control are included, they can impact the available length of the Frame Body field. Finally, security (Temporal Key Integrity protocol (TKIP), Counter Mode with Cipher Block Chaining-Message Authentication Code Protocol (CCMP), GCM with Galois Counter Mode Protocol (GCMP) and the Michael Integrity Check (MIC) parameters) can impact the available length of the Frame Body.

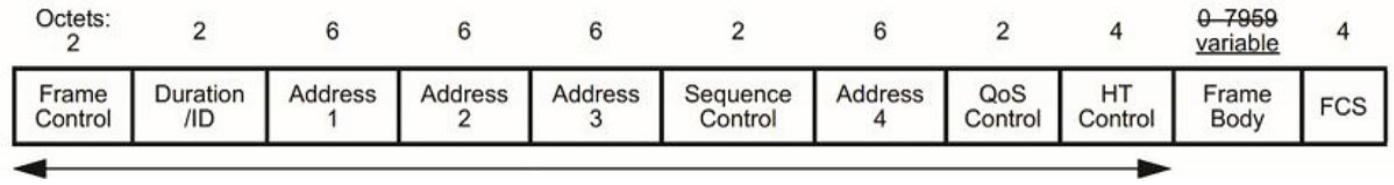


Figure 3.8: 802.11 General Frame Format from 802.11ac-2013

Additionally, the HT Control field has an HT variant and a VHT variant for the High Throughput PHY and Very High Throughput PHY respectively. Within the HT Control field is a HT Control Middle field, which varies for 802.11n and 802.11ac.

The preceding information shows the way in which the 802.11 standard has evolved over time. Part of the job of a WLAN analyst is to possess and maintain knowledge related to these changes. Such knowledge maintenance can be achieved by acquiring the new amendments and browsing them for significant changes, reading blogs such as those at CWNP.com, watching webinars like those in the CWNPTV channel on YouTube, and

taking new training classes made available by CWNP. Additionally, as CWNP certifications are revised, new and updated knowledge from the 802.11 standard and various vendor implementations is included.

The remainder of this section will provide a brief description for each of the fields in the 802.11 general frame as it is in 802.11ac. The QoS Control field, Frame Control field, and HT Control field will have the lengthiest descriptions as they include more meaningful data for the WLAN analyst than most of the others, or the data they contain is more complex.

Frame Control

The Frame Control fields set important parameters for the frame. These parameters include the frame type and subtype as well as the direction of the frame in a BSS. Figure 3.9 shows the bits in the Frame Control field and their purposes.

	B0 B1	B2 B3	B4 B7	B8	B9	B10	B11	B12	B13	B14	B15
	Protocol Version	Type	Subtype	To DS	Fro m DS	More Frag-ments	Re-try	Power Manage-ment	More Data	Protect-ed Frame	Or-der
Bits:	2	2	4	1	1	1	1	1	1	1	1

Figure 3.9: The Frame Control Field as Defined in 802.11-2012

The Protocol Version bits are always set to 00 at this point indicating that no incompatible version has been developed. If, in the future, an incompatible version is released, these bits can be used for that notification.

Type	Bits	Subtype	Bits
Management	00	Beacon	1000
Management	00	Association Request	0000
Management	00	Association Response	0001
Management	00	Authentication	1011
Management	00	Deauthentication	1100
Management	00	Action	1101
Management	00	Action No Ack	1110
Control	01	Control Wrapper	0111
Control	01	Block Ack Request (BlockAckReq)	1000
Control	01	Block Ack (BlockAck)	1001
Control	01	PS-Poll	1010
Control	01	RTS	1011
Control	01	CTS	1100
Control	01	Acknowledgement (ACK)	1101
Data	10	Standard Data Frame	0000
Data	10	Null Data Frame	0100
Data	10	QoS Data	1000
Data	10	QoS Null Data Frame	1110

Table 3.2: Frame Types and Subtypes from 802.11-2012

The Type and Subtype fields define the frame type (management, control or data) and the subtype. Table 3.2 lists the important valid values for these bits.

802.11-compatible protocol analyzers decode the frame type and subtype bits (subfields) and display the most appropriate of the three types and many subtypes in the decode view. As a WLAN analyst, you should know the different frame subtypes and their meaning or description. This information is provided in the later section of this chapter called *802.11 Frame Types*.

The next subfields are the To DS and From DS bits. One bit each, they determine whether a frame is transmitted from a STA to the AP, from the AP to a STA, from one STA to another in an IBSS or using the four-address MAC header format. The four-address format is used, per the standard, in a mesh BSS. Figure 3.10 shows the To DS and From DS values appropriate as defined in the 802.11 standard. While the direction of a frame can be defined by the source and destination address (MAC addresses), if you know the AP MAC address, the From DS subfield can be useful as a quick reference. If it is set to 1 and the

four-address format is not in use, you know that the frame is traveling from the AP to a client STA.

Additionally, anytime you see a frame with both the To DS and From DS bits set to 0, you know it is a frame operating in an ad-hoc or IBSS network. This is useful in troubleshooting network problems. For example, an IBSS operating on the same channel as a nearby BSS can cause excess CCI. Filtering a protocol capture on the To DS and From DS fields can quickly reveal any IBSS traffic, which can then be addressed from a management/administrative perspective.

To DS and From DS values	Meaning
To DS = 0 From DS = 0	A data frame direct from one STA to another STA within the same IBSS, a data frame direct from one non-AP STA to another non-AP STA within the same BSS, or a data frame outside the context of a BSS, as well as all management and control frames.
To DS = 1 From DS = 0	A data frame destined for the DS or being sent by a STA associated with an AP to the Port Access Entity in that AP.
To DS = 0 From DS = 1	A data frame exiting the DS or being sent by the Port Access Entity in an AP, or a group addressed Mesh Data frame with Mesh Control field present using the three-address MAC header format.
To DS = 1 From DS = 1	A data frame using the four-address MAC header format. This standard defines procedures for using this combination of field values only in a mesh BSS.

Figure 3.10: Explanation of the To DS and From DS Subfields as Defined in 802.11-2012

The More Fragments subfield is used to indicate whether the current frame is part of a fragmented frame or not. Fragmentation occurs based on the fragmentation threshold setting in the AP or client device. Fragmentation is used to increase the probability that a transmitted frame will get through in a high contention with hidden node issues or interference laden environment. Sending a smaller frame results in a greater likelihood of the frame getting through before interference occurs. The fragmentation threshold defaults to 2346 to accommodate the maximum frame size without fragmentation. Interfaces allowing adjustment of this value provide the option to set it between 256 and 2346 per the standard. It should only be enabled in high retry environments. You know fragmentation is being used when you see the More Fragments bit set to 1 in some frames.

The Retry field is useful in tracking frame transmission errors. If a frame is transmitted and the transmitter does not receive an ACK frame in response, the transmitting station will resend the frame using contention processes. When retransmitting, the frame will include the Retry field set to 1. This bit is used by the receiving STA to eliminate duplicate frames, but it can also be useful for tracking retries on the network to see if they are causing performance issues. Most WLAN protocol analyzers designed specifically for WLAN analysis will provide reports on the retry rate or the percent of frames sent as retransmissions.

The Power Management field is a 1 bit field indicating whether power management is used by the STA. The value of this field determines the mode in which the STA will operate after the completion of frame transmission. The Power Management field is always set to 0 by an AP with its transmissions as it does not enter power save mode. It is also set to 0 in management frames that cannot be buffered, and in frames sent to an AP by

a STA before it is associated. All other frames may use the bit, set to 1, to indicate the intention to enter power save mode so that the AP knows to buffer frames for that STA until it wakes.

The More Data field is used by the AP (or another STA in an IBSS) to indicate that more frames are buffered for that STA, so that it will not enter sleep mode. When set to 1 it indicates that the AP or STA is holding more frames for the STA to which the current frame is targeted. Additionally, when a STA sends a frame to the AP and that frame includes the More Data Ack subfield of the QoS capability element (discussed more later) set to 1, and the AP has frames buffered for the STA with Automatic Power Save Delivery (APSD) enabled, the AP will set the More Data field to 1 in the ACK frame that it sends back to that STA so that the STA knows the AP has frames buffered for it.

The Protected Frame field, which replaces the older WEP field, indicates that the MSDU is encrypted in the frame if it is set to 1. When set to 0, no encryption is used at the 802.11 MAC sublayer.

The final field is the Order field. It is used for two purposes:

- It is set to 1 in a non-QoS data frame to indicate that it contains an MSDU.
- It is set to 1 in a QoS data or management frame to indicate that the frame contains an HT Control field. This allows processing by HT devices that are aware of the decoding of the HT Control field.

Figure 3.11 shows a protocol analyzer decode of the Frame Control field with explanatory information included. Most protocol analyzers provide such explanatory information so that you are not required to look up bits in tables to recall the meaning of those bits. In this particular capture, it is a QoS data frame that is encrypted and being transmitted from the AP to a STA.

Duration/ID

The Duration/ID field is used for two purposes. First, it may contain the duration of the frame. Second, it may contain the association identifier (AID) of the STA that transmitted the frame. When a PS-Poll frame is transmitted by a STA, the Duration/ID field contains the AID of the STA so that the AP knows that it is awake and can send buffered frames. In both non-QoS and QoS data frames, it contains the duration of the frame. Additionally, in control frames, in contains the duration of the frame exchange. When containing the duration, it is used to set the NAV timer for the CSMA/CA operations.

```
802.11 MAC Header
    Version:                0 [0 Mask 0x03]
    Type:                   %10  Data [0 Mask 0x0C]
    Subtype:                %1000  QoS Data [0 Mask 0xF0]
    Frame Control Flags:    %01000010 [1]
                               0... .... Non-strict order
                               .1.. .... Protected Frame
                               ..0. .... No More Data
                               ...0 .... Power Management - active mode
                               .... 0... This is not a Re-Transmission
                               .... .0.. Last or Unfragmented Frame
                               .... ..1. Exit from the Distribution System
                               .... ...0 Not to the Distribution System
```

Figure 3.11: Protocol Analyzer Decode of the Frame Control Field

Address 1, 2, 3, and 4

The 802.11 general frame format specifies four address fields. Table 3.3 provides an overview of the use of these fields. In the table, RA is the receiver address, DA is the destination address, TA is the transmitting STA address, and SA is the source address. In an IBSS the transmitting STA or source STA may not define the BSSID, so it is specified separately with Address 3. When an AP is communicating to a STA, the BSSID may be used in Address 2 and the source address may be in Address 3 as they may be different. An AP can implement multiple SSIDs and, therefore, the BSSID is not always the MAC address of the AP. When a STA sends to the AP, the BSSID may be used in Address 1 and the destination address is used in Address 3 as the target AP MAC address may not match the AP’s BSSID for the particular SSID. Finally, only a mesh transmission uses all four addresses as there may be intermediary devices involved in the transmission before it reaches the final wireless destination. The DA address field may contain an individual or group intended as the target, and the RA address may, as well. The difference between the RA address and the DA address is that the RA address is always the immediate recipient of the frame, and the DA address is the ultimate target of the frame (for example, in a mesh BSS). The SA address is always the original source of the frame, and the TA address is the address of the STA that transmitted the frame onto the medium. That is, the TA address may be one or more in-between STAs in a mesh BSS moving the frame forward from the SA to the DA.

Mode	Address 1	Address 2	Address 3	Address 4
IBSS	RA/DA	TA/SA	BSSID	Not used
AP to STA	RA/DA	TA/BSSID	SA	Not used
STA to AP	RA/BSSID	TA/SA	DA	not used
Mesh	RA	TA	DA	SA

Table 3.3: Four Address Fields and Utilization

Sequence Control

The 16-bit sequence control field is used with fragmentation and for the removal of duplicate frames should they occur. It is divided into a 4-bit fragment number and a 12-bit sequence number. When an MSDU is fragmented, all fragments have the same sequence number and the fragment number is incremented by 1 (while starting at 0) for each frame until all fragments are delivered. The sequence number starts at 0 and is incremented for each new frame or set of frames with fragmentation until it reaches 4095, at which point it simply resets to 0 and beings again. The primary use of this in analysis is the detection of fragmented frames and the analysis of in or out of sequence frame delivery.

QoS Control

The QoS Control field is a 16-bit field that identifies the category to which the frame belongs for queuing purposes. It has additional QoS-related bits, and also bits related to A-MSDU and mesh (in a mesh BSS) operations. The most important factor in this field for most analysis scenarios is the user priority (UP) information for the frame. In the standard, this is referenced as the traffic identifier (TID) subfield. Given that EDCA is implemented in QoS WLANs based on the wireless multi-media (WMM) certification by the Wi-Fi Alliance, the bits 0-3 in the QoS Control field are mapped with possible values from 0 to 7. Table 3.4 lists the mapping of WMM access categories (ACs) to 802.1d tags.

Access Category	802.1d	Description
WMM Voice (AC_VO)	7,6	Highest Priority – Intended for VoIP
WMM Video (AC_VI)	5,4	Next highest priority – Intended for video streaming
WMM Best Effort (AC_BE)	0,3	Standard data traffic
WMM Background (AC_BK)	2,1	Lowest priority – may be used for file transfer or print operations

Table 3.4: Wi-Fi Alliance WMM ACs Mapped to 802.1d Tags

WMM operates based on queues created for the various ACs. For example, a STA will have a queue for AC_VO, another for AC_VI, and so on. The highest priority queue gets to take advantage of a transmit opportunity (TxOP) before the lower priority queues.

The key to understanding the probabilistic priorities provided by WMM is the contention window (CW) you studied in Chapter 2. Without WMM (or EDCA), the CW has a minimum value (aCWmin) of 0 and a maximum value (aCWmax) of 1023. This changes with WMM. Table 3.5 lists the default EDCA or WMM CW parameters.

Access Category	aCWmin	aCWmax
AC_VO	3	7
AC_VI	7	15
AC_BE	15	1023
AC_BK	15	1023

Table 3.5: ACs and CW Parameters

Table 3.5 makes it clear that the random selection of a backoff timer from the CW will be a higher value more often than not for AC_BE and AC_BK frames than for AC_VO and AC_VI frames. These are default settings and may be tweaked in many APs to optimize even further, though changes to these category CW settings can only be realized on performance improvements in busy environments (BSSs). In low traffic BSSs, very little

impact is made by adjusting CWs.

HT Control

The next field is the HT Control field. It is used to specify various parameters related to the HT operations and VHT operations. There is an HT variant and a VHT variant of the HT Control field. This field provides an excellent case study of the importance of reserved bits. Figure 3.12 shows the HT Control Field in the 802.11-2012 standard before 802.11ac was ratified. Figure 3.13 shows the Link Adaptation Control subfield details from 802.11-2012.

	B0 B15	B16 B17	B18 B19	B20 B21	B22 B23	B24	B25 B29	B30	B31
	Link Adaptation Control	Calibration Position	Calibration Sequence	Reserved	CSI/ Steering	NDP Announce-ment	Reserved	AC Constraint	RDG/ More PPDU
Bits:	16	2	2	2	2	1	5	1	1

Figure 3.12: HT Control Field in 802.11-2012

	B0	B1	B2 B5	B6 B8	B9 B15
	Reserved	TRQ	MAI	MFSI	MFB/ASELC
Bits:	1	1	4	3	7

Figure 3.13: Link Adaptation Control Subfield in 802.11-2012

Note that in Figure 3.13, bit 0 is reserved. That is, of the 16 bits in the Link Adaptation Control field, only 15 are used and the first bit is reserved. This decision became very important with the ratification of 802.11ac. Notice in Figure 3.14, which shows the HT Control Field in 802.11ac, that the format seems to have changed entirely from Figure 3.12. However, the format has not changed nearly as much as it appears. The VHT subfield is simply utilizing the reserved bit 0 from the Link Adaptation Control subfield as it existed in 802.11-2012 to determine the format of the next 29 bits (now the HT Control Middle subfield) in the HT Control field.

	B0	B1 B29	B30	B31
	VHT	HT Control Middle	AC Constraint	RDG/More PPDU
Bits	1	29	1	1

Figure 3.14: HT Control Field in 802.11ac

	B1 B15	B16 B17	B18 B19	B20 B21	B22 B23	B24	B25 B28	B29
	Link Adaptation Control	Calibration Position	Calibration Sequence	Reserved	CSI/ Steering	HT NDP Announcement	Reserved	DEI
Bits:	15	2	2	2	2	1	4	1

Figure 3.15: HT Control Middle if VHT=0

B1	B2	B3 B5	B6 B8	B9 B23	B24 B26	B27	B28	B29
Reserved	MRQ	MSI/ STBC	MFSI/ GID-L	MFB	GID-H	Coding Type	FB Tx Type	Unsolicited MFB
Bits: 1	1	3	3	15	3	1	1	1

Figure 3.16: HT Control Middle if VHT=1

From these images, you can see that the VHT subfield now determines whether the HT Control Middle bits are formatted for HT communications (VHT=0) or VHT communications (VHT=1). This VHT subfield was simply a reserved field in previous editions of the 802.11 standard.

The HT Control field is used for communications related to antenna selection and beamforming.

Frame Body

The Frame Body field, as discussed earlier, contains the actual MSDU payload to be transmitted. It incurs overhead if encryption is used and may include extra information in a mesh BSS. When the mesh control field is included in the Frame Body, it is encrypted as part of the data. TKIP/RC4 incurs 20 bytes of overhead, and CCMP/AES incurs 16 bytes of overhead.

FCS

The final field is the Frame Check Sequence field, which is a 4 byte or 32-bit field. It is calculated against the MAC header and Frame Body and is used to detect errors in communication.

802.11 Frame Types

The frames used in WLANs are divided into three types or categories as defined in the type field. The Types are further divided into subtypes. The three types are management, control, and data frames. They are briefly described in this section.

Management Frames

Management frames are those used to manage access to the WLAN, announce information about it and perform certain actions. The following frames are defined as management frames and are used in production WLANs:

- Beacon: used to announce information about the BSS by the AP.
- Probe: used by clients to locate a BSS based on an SSID to which they may connect.
- Association: used to association with an AP and begin communicating through it.

- Disassociation: used to remove an association from an AP.
- Reassociation: used to associate to another AP in the same ESS when already associated with an AP in that ESS.
- Authentication: used to authenticate to an AP to prepare for association or roaming.
- Deauthentication: used to remove the AID and deauthenticate with an AP.
- Action: used for spectrum management, fast BSS transition and other actions taken within a BSA.

Management frames use the frame format shown in Figure 3.17 from 802.11-2012. The only change to this frame format in 802.11ac is the maximum size of 2320 has been changed, and the Frame Body is specified as simply a variable length. These frame elements have been sufficiently described in the preceding section of this chapter.

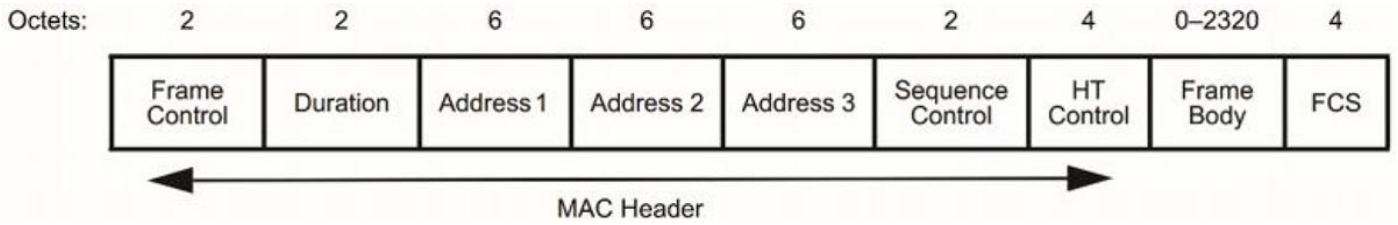


Figure 3.17: Management Frame Format

Control Frames

Control frames are used to control access to the medium for STAs that are connected to an AP or the WLAN. The following frames are defined as control frames and are used in production WLANs:

- *ACK:* acknowledgement frame used to signal receipt of a frame.
- *RTS:* request to send (RTS) frame used to request the target STA to send a CTS frame.
- *CTS:* clear to send (CTS) frame used to clear the medium for transmission of another frame.
- *BlockAckReq:* frame used to request block acknowledgement.
- *BlockAck:* block acknowledgement for multiple frames in a burst.
- *Control Wrapper:* used to carry other control frames while including an HT Control field.

Control frames have a limited 802.11 header followed by the information needed for the specific control frame. The Frame Control field is the same across control frames and is depicted in Figure 3.18.

Data Frames

Data frames carry data or may be used for control functions related to power management when the null data frame is used. Data frames use the general frame format discussed previously in this chapter. They include the full header for the specific MAC/PHY being used, and include an MSDU with the exception of the Null Data frame. The term null should be understood quite literally as there are 0 bytes in the Frame Body of a Null Data frame. Data frames come in two primary types:

1. Data: standard non-QoS data using standard DCF rules.
2. QoS Data: QoS data using EDCA rules.

	B0 B1	B2 B3	B4 B7	B8	B9	B10	B11	B12	B13	B13	B15
	Protocol Version	Type (Control)	Subtype	To DS (0)	From DS (0)	More Frag (0)	Retry (0)	Power Man-age-ment	More Data (0)	Protected Frame (0)	Order (0)
Bits:	2	2	4	1	1	1	1	1	1	1	1

Figure 3.18: Frame Control Field of the Control Frame

PCF Frames

Point Coordination Function (PCF) frames are documented in the standard but are not used in active WLANs as the PCF mode is not implemented in current vendor solutions. PCF frames are not tested on the CWAP exam. They include the CF-End+CF-Ack frame and the CF-End frame. The only significant exception to this rule is that 802.11n added the ability to use a CF-End frame to indicate that it has no more data to send even though it possesses a TxOP. This is used when STBC is implemented. If you know this, you know all you need for the exam and practical real-world troubleshooting related to the PCF frames.

Important 802.11 Frames

This section reviews the most important 802.11 frames the WLAN analyst should understand. With an understanding of these frames, you will be better prepared to perform protocol analysis and to troubleshoot WLAN issues. These important frames include:

- Beacon
- Probe Request
- Probe Response
- Authentication
- Deauthentication
- Association
- Disassociation
- Reassociation Request

- Reassociation Response
- Request-to-Send
- Clear-to-Send
- Null
- Power Save-Poll
- Acknowledgement

Beacon Frames

Beacon frames are used to announce the BSS for client STAs that wish to connect. They are transmitted by default by the AP every 100 time units (TUs), or at the same interval for STAs in an IBSS. The default TU is 1024 microseconds (µs). Therefore, the default beacon frame interval is 102.4 milliseconds (ms) and not the common 100 ms many reference; however, such references are typically rounding the beacon interval and are not concerned with absolute accuracy. The beacon interval can be adjusted, but very little benefit is achieved by lengthening it to more Tus, with the exception of high SSID count networks), and so it is seldom changes (despite being talked about as a potential “tuning” parameter on occasion).

Note: **When you have multiple SSIDs on each AP radio, the extra overhead required to transmit the beacon frames for each SSID can make the adjustment of the TU value justifiable. It can potentially reduce the overhead by several percentage points in situations with three or more SSIDs per AP.**

The beacon frame is a management frame so it uses the management frame format shown in Figure 3.17 earlier. The frame body, which is of variable size, carries the beacon specific information. Table 3.6 lists the frame body elements of the beacon frame from 802.11-2012 and amendments 802.11aa, 802.11ac, 802.11ad and 802.11ae.

Order	Information	Description
1	Timestamp	Time of the frame transmission.
2	Beacon interval	TUs used to count between beacon transmissions.
3	Capability	Specifies information about the capabilities of the AP, such as whether the STA is an AP or a STA in an IBSS, whether privacy (encryption) is supported or not, whether APSD is

		implemented or not, and whether the short preamble is allowed or not.
4	Service Set Identifier (SSID)	If dot11MeshActivated is true, the SSID element is the wildcard value as described in Clause 8.4.2.2 of 802.11-2012.
5	Supported rates	The rates supported in the lower rate set.
6	Frequency-Hopping (FH) Parameter Set	The FH Parameter Set element is present within Beacon frames generated by STAs using FH PHYs.
7	DSSS Parameter Set	The DSSS Parameter Set element is present within Beacon frames generated by STAs using Clause 16, Clause 17, and Clause 19 PHYs. The element is present within Beacon frames generated by STAs using a Clause 20 PHY in the 2.4 GHz band.
8	CF Parameter Set	The CF Parameter Set element is present only within Beacon frames generated by APs supporting a PCF. This element is not present if dot11HighThroughputOption Implemented is true and the Dual CTS Protection field of the HT Operation element is 1.
9	IBSS Parameter Set	The IBSS Parameter Set element is present only within Beacon frames generated by STAs in an IBSS.
10	Traffic indication map (TIM)	The TIM element is present only within Beacon frames generated by APs or mesh STAs.
11	Country	The Country element is present if dot11MultiDomainCapabilityActivated is true or dot11SpectrumManagementRequired is true or dot11RadioMeasurementActivated is true.
12	FH Parameters	FH Parameters as specified in 8.4.2.11 are optionally present

		if dot11MultiDomainCapabilityActivated is true.
13	FH Pattern Table	FH Pattern Table information as specified in 8.4.2.12 are optionally present if dot11MultiDomainCapabilityActivated is true.
14	Power Constraint	The Power Constraint element is present if dot11SpectrumManagementRequired is true and is optionally present if dot11RadioMeasurementActivated is true.
15	Channel Switch Announcement	Channel Switch Announcement element is optionally present if dot11SpectrumManagementRequired is true.
16	Quiet	The Quiet element is optionally present if dot11SpectrumManagementRequired is true or dot11RadioMeasurementActivated is true.
17	IBSS DFS	IBSS DFS element is present if dot11SpectrumManagementRequired is true in an IBSS.
18	TPC Report	The TPC Report element is present if dot11SpectrumManagementRequired is true or dot11RadioMeasurementActivated is true.
19	ERP	The ERP element is present within Beacon frames generated by STAs using extended rate PHYs (ERPs) defined in Clause 19 and is optionally present in other cases.
20	Extended Supported Rates	The Extended Supported Rates element is present if there are more than eight supported rates, and it is optional otherwise.
21	RSN	The RSNE is present within Beacon frames generated by STAs that have dot11RSNAActivated equal to true.
22	BSS Load	The BSS Load element is present if dot11QosOption Implemented and dot11QBSSLoadImplemented are both true.
		The EDCA Parameter Set element is present if

23	EDCA Parameter Set	dot11QosOptionImplemented is true, and dot11MeshActivated is false, and the QoS Capability element is not present.
24	QoS Capability	The QoS Capability element is present if dot11QosOption Implemented is true, and dot11MeshActivated is false, and EDCA Parameter Set element is not present.
25	AP Channel Report	If dot11RMAPChannelReportActivated is true, one AP Channel Report element is present for each operating class that has at least 1 channel to report.
26	BSS Average Access Delay	The BSS Average Access Delay element is present if dot11RMBSSAverageAccessDelayActivated is true and the value of the AP Average Access Delay field is not equal to 255 (measurement not available); otherwise, the BSS Average Access Delay element is optionally present if dot11RMBSSAverageAccessDelayActivated is true.
27	Antenna	The Antenna element is present if dot11RMAntennaInformationActivated is true and the value of the Antenna ID field is not equal to 0 (unknown antenna); otherwise, the Antenna element is optionally present if dot11RMAntennaInformationActivated is true.
28	BSS Available Admission Capacity	The BSS Available Admission Capacity element is present if dot11RMBSSAvailableAdmissionCapacityActivated is true with the following exceptions: 1) when Available Admission Capacity Bitmask equals 0 (Available Admission Capacity List contains no entries), or 2) when the BSS Load element is present, and the Available Admission Capacity Bitmask states that only AC_VO is present in the Available Admission Capacity List field.
29	BSS AC Access Delay	The BSS AC Access Delay element is present if dot11RMBSSAverageAccessDelayActivated is true and at least one field of the element is not equal to 255 (measurement not available); otherwise, the BSS AC Access Delay element is optionally present if dot11RMBSSAverageAccessDelayActivated is true.

30	Measurement Pilot Transmission	The Measurement Pilot Transmission element is present if dot11RMMeasurementPilotActivated is a value between 2 and 7.
31	Multiple BSSID	One or more Multiple BSSID elements are present if dot11RMMeasurementPilotActivated is a value between 2 and 7 and the AP is a member of a Multiple BSSID Set with two or more members, or if dot11MgmtOptionMultiBSSIDActivated is true, or if dot11InterworkingServiceActivated is true and the AP is a member of a Multiple BSSID Set with two or more members and at least one dot11GASAdvertisementID MIB attribute exists.
32	RM Enabled Capabilities	RM Enabled Capabilities element is present if dot11RadioMeasurementActivated is true.
33	Mobility Domain	The Mobility Domain element (MDE) is present if dot11FastBSSTransitionActivated is true.
34	DSE registered location	The DSE Registered Location element is present if dot11LCIDSERequired is true.
35	Extended Channel Switch Announcement	The Extended Channel Switch Announcement element is optionally present if dot11ExtendedChannelSwitchActivated is true.
36	Supported Operating Classes	The Supported Operating Classes element is present if dot11ExtendedChannelSwitchActivated is true.
37	HT Capabilities	The HT Capabilities element is present when dot11HighThroughputOptionImplemented attribute is true.
38	HT Operation	The HT Operation element is included by an AP and a mesh STA when dot11HighThroughputOptionImplemented attribute is true.
		The 20/40 BSS Coexistence element is optionally present

39	20/40 BSS Coexistence	when the dot112040BSSCoexistenceManagementSupport attribute is true.
40	Overlapping BSS Scan Parameters	The Overlapping BSS Scan Parameters element is optionally present if the dot11FortyMHzOptionImplemented attribute is true.
41	Extended Capabilities	The Extended Capabilities element is optionally present if any of the fields in this element are nonzero.
42	FMS Descriptor	The FMS Descriptor element is present if dot11MgmtOptionFMSActivated is true.
43	QoS Traffic Capability	The QoS Traffic Capability element is optionally present if dot11MgmtOptionACStationCountActivated is true.
44	Time Advertisement	The Time Advertisement element is present every dot11TimeAdvertisementIntervalDTIMs if dot11MgmtOptionUTCTSFOffsetActivated is true.
45	Interworking	The Interworking element is present if dot11InterworkingServiceActivated is true.
46	Advertisement Protocol	Advertisement Protocol element is present if dot11InterworkingServiceActivated is true and at least one dot11GASAdvertisementID MIB attribute exists.
47	Roaming Consortium	The Roaming Consortium element is present if dot11InterworkingServiceActivated is true and the dot11RoamingConsortiumTable has at least one entry.
48	Emergency Alert Identifier	One or more Emergency Alert Identifier elements are present if dot11EASActivated is true and there are one or more EAS message(s) active in the network.
49	Mesh ID	The Mesh ID element is present if dot11MeshActivated is true.
	Mesh	The Mesh Configuration element is present if

50	Configuration	dot11MeshActivated is true.
51	Mesh Awake Window	The Mesh Awake Window element is optionally present if dot11MeshActivated is true.
52	Beacon Timing	The Beacon Timing element is optionally present if both dot11MeshActivated and dot11MBCAActivated are true.
53	MCCAOP Advertisement Overview	The MCCAOP Advertisement Overview element is optionally present if both dot11MeshActivated and dot11MCCAActivated are true.
54	MCCAOP Advertisement	One or more MCCAOP Advertisement elements are optionally present if both dot11MeshActivated and dot11MCCAActivated are true.
55	Mesh Channel Switch Parameters	The Mesh Channel Switch Parameters element is present when dot11MeshActivated is true and either Channel Switch Announcement element or Extended Channel Switch Announcement element is present.
56	QMF Policy	Indicates the QMF policy parameters of the transmitting STA. The QMF Policy element is present when dot11QMFActivated is true, and is not present otherwise. The QMF Policy element is never present in Beacon frames in an IBSS.
57	QLoad Report	The QLoad Report element is present every dot11QLoadReportIntervalDTIM DTIMs if dot11QLoadReportActivated is true.
58	HCCA TXOP Update Count	The HCCA TXOP Update Count element is present if both dot11PublicHCCATXOPNegotiationActivated is true and an HC is collocated with the AP.
59	Multi-band	The Multi-band element is optionally present if dot11MultibandImplemented is true.
	VHT	The VHT Capabilities element is present when the

60	Capabilities	dot11VHTOptionImplemented is true.
61	VHT Operation	The VHT Operation element is present when the dot11VHTOptionImplemented is true; otherwise, it is not present.
62	VHT Transmit Power Envelope element	One VHT Transmit Power Envelope element is present for each distinct value of the Local Maximum Transmit Power Unit Interpretation subfield that is supported for the BSS if both of the following conditions are met: — dot11VHTOptionImplemented is true; — Either dot11SpectrumManagementRequired is true or dot11RadioMeasurementActivated is true. Otherwise, this parameter is not present.
63	Channel Switch Wrapper element	The Channel Switch Wrapper element is optionally present if dot11VHTOptionImplemented is true and at least one of a Channel Switch Announcement element or an Extended Channel Switch Announcement element is also present in the Beacon frame and the Channel Switch Wrapper element contains at least one subelement.
64	Extended BSS Load element	The Extended BSS Load element is optionally present if dot11QosOptionImplemented, dot11QBSSLoadImplemented and dot11VHTOptionImplemented are true.
65	Quiet Channel	Either one Quiet Channel element containing an AP Quiet Mode field equal to 0 or one or more Quiet Channel elements each containing an AP Quiet Mode field equal to 1 are optionally present if dot11VHTOptionImplemented is true, and either dot11SpectrumManagementRequired or dot11RadioMeasurementActivated is true.
66	Operating Mode Notification	The Operating Mode Notification element is optionally present if dot11OperatingModeNotificationImplemented is true.
Last	Vendor Specific	One or more vendor-specific elements are optionally present. These elements follow all other elements.

Table 3.6: Beacon Frame Body Options

As seen in Table 3.6, the amount of information contained in a beacon frame is quite extensive. Figure 3.19 shows a protocol capture and decode of the beacon frame revealing important information about the BSS. The highlighted areas show the SSID of the captured BSS beacon frame and an example of a vendor-specific field. Additional information shown includes the RSN Information element, which reveals the security methods used in the BSS.

```
▷ Frame 1: 398 bytes on wire (3184 bits), 398 bytes captured (3184 bits)
▷ Radiotap Header v0, Length 23
▷ 802.11 radio information
▷ IEEE 802.11 Beacon frame, Flags: ........
◢ IEEE 802.11 wireless LAN management frame
  ◢ Fixed parameters (12 bytes)
      Timestamp: 0x0000000000000000
      Beacon Interval: 0.102400 [Seconds]
    ▷ Capabilities Information: 0x0531
  ◢ Tagged parameters (339 bytes)
    ◢ Tag: SSID parameter set: Class-802.1X-4
        Tag Number: SSID parameter set (0)
        Tag length: 14
        SSID: Class-802.1X-4
    ▷ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]
    ▷ Tag: DS Parameter set: Current Channel: 6
    ▷ Tag: Traffic Indication Map (TIM): DTIM 2 of 0 bitmap
    ▷ Tag: Country Information: Country Code US, Environment Any
    ▷ Tag: Power Constraint: 0
    ▷ Tag: ERP Information
    ◢ Tag: RSN Information
        Tag Number: RSN Information (48)
        Tag length: 26
        RSN Version: 1
      ▷ Group Cipher Suite: 00-0f-ac TKIP
        Pairwise Cipher Suite Count: 2
      ▷ Pairwise Cipher Suite List 00-0f-ac AES (CCM) 00-0f-ac TKIP
        Auth Key Management (AKM) Suite Count: 1
      ▷ Auth Key Management (AKM) List 00-0f-ac WPA
      ▷ RSN Capabilities: 0x0000
        PMKID Count: 0
        PMKID List
    ▷ Tag: Vendor Specific: Microsof: WPA Information Element
    ▷ Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    ▷ Tag: Vendor Specific: Microsof: WMM/WME: Parameter Element
    ▷ Tag: Vendor Specific: Epigram: HT Capabilities (802.11n D1.10)
    ▷ Tag: HT Capabilities (802.11n D1.10)
    ▷ Tag: Vendor Specific: Epigram: HT Additional Capabilities (802.11n D1.00)
    ▷ Tag: HT Information (802.11n D1.10)
    ▷ Tag: Vendor Specific: AtherosC: Advanced Capability
    ▷ Tag: Vendor Specific: AtherosC: Unknown
    ▷ Tag: Vendor Specific: Aerohive
```

Figure 3.19: Beacon Frame Decode

Beacon frames serve many purposes, including:

- Announce the existence of a BSS.
- Provide information required by client STAs to determine ability to connect to the BSS.
- Provide power management information related to buffered frames.
- Indicate the security required to participate in the BSS.
- Provide signal strength information to the client STAs to select the best AP for connections.
- Allow the administrator or analyst to quickly identify the existing APs and the SSIDs they serve using a Wi-Fi scanner or protocol analyzer.

To filter on beacon frames in Wireshark, use the following filter:

```
wlan.fc.type_subtype == 0x08
```

To filter out beacon frames from the display in Wireshark, use the following filter:

```
wlan.fc.type_subtype != 0x08
```

More information on viewing captures in Wireshark and filtering for them is provided in Chapter 5.

Figure 3.20 shows a Wireshark capture displaying the Beacon frames based on a coloring rule. Note that beacons are seen from two APs in this capture. One is an Aerohive AP and the other an Extreme Networks AP. You will learn to colorize your captures in Wireshark in Chapter 5.

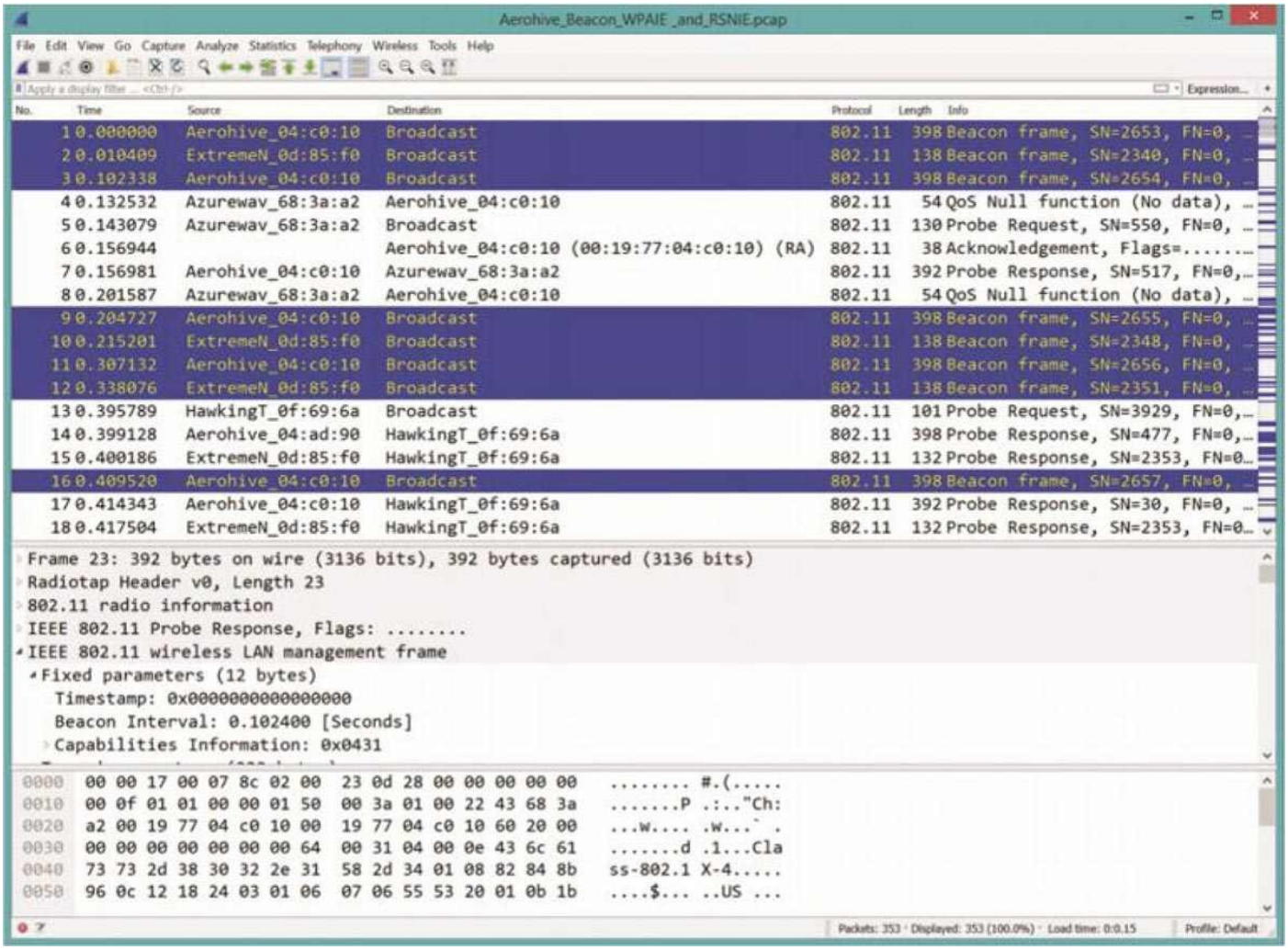


Figure 3.20: Colorized Capture with Beacon Frames

Probe Request and Probe Response Frames

Probe Request and Response frames are used for active scanning. The STA sends a Probe Request and the AP responds with a Probe Response. If the STA sends a Probe Request with a broadcast SSID, all APs respond with a Probe Response on the channel. This allows a STA to immediately request a listing of all APs available without waiting for Beacon frames. Figure 3.21 shows the Probe Request and Probe Response frames colorized in yellow and red, while the Beacon frames are colorized in blue. Figure 3.22

shows more details of the Probe Request decode, and Figure 3.23 shows details of the Probe Response decode.

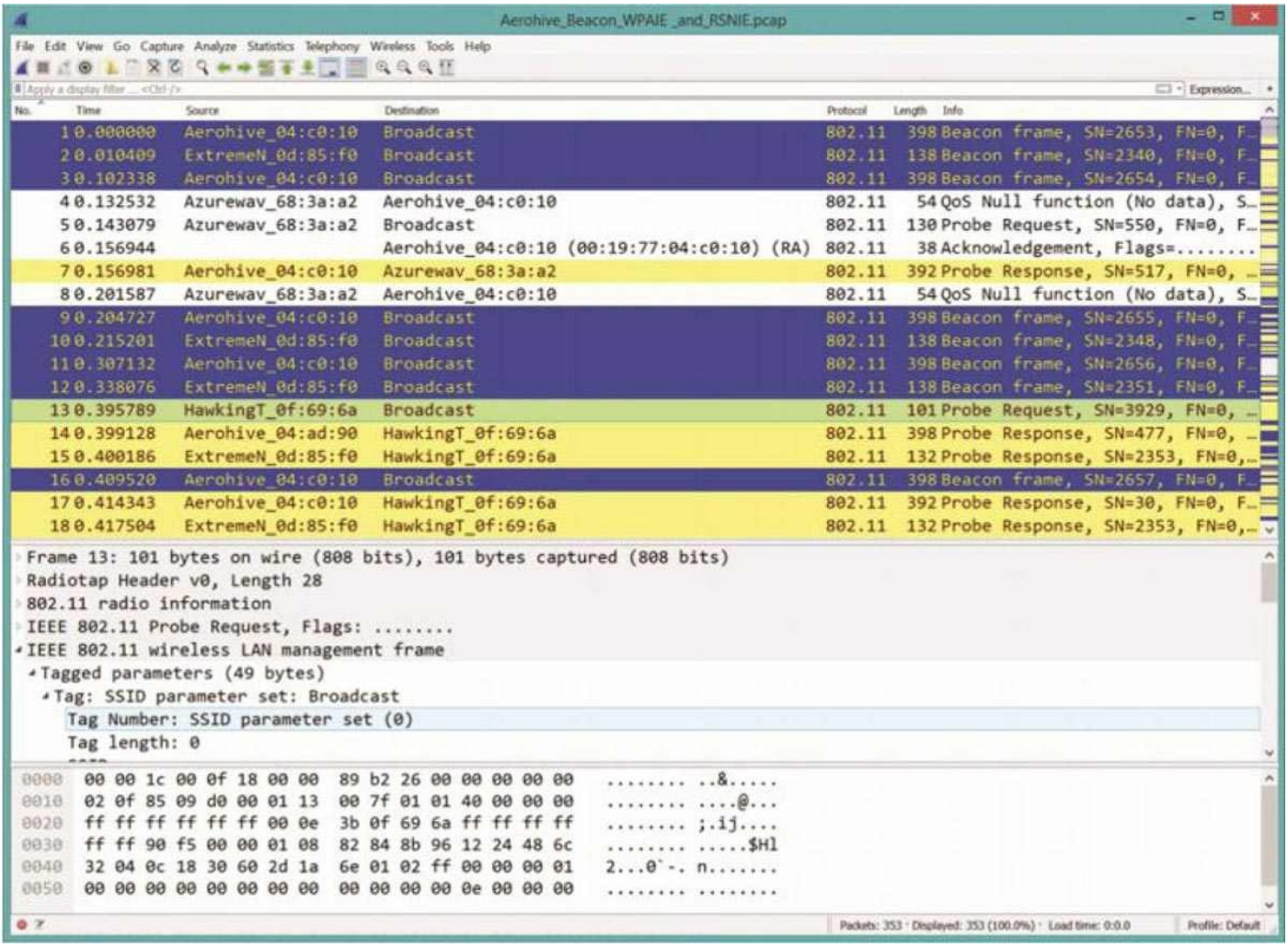


Figure 3.21: Colorized Capture with Probe Request and Response Frames

To filter on probe request and probe response frames, use the following Wireshark filter:

```
wlan.fc.type_subtype == 0x4 or wlan.fc.type_subtype == 0x5
```

To filter out probe request and probe response frames, use the following filter:

```
wlan.fc.type_subtype != 0x4 and wlan.fc.type_subtype != 0x5
```

It is often beneficial to evaluate probe requests and probe responses when troubleshooting performance issues on the WLAN. Some clients will continually probe other channels than the one to which they are connected. The amount of probing may be able to be reduced by adjusting the roaming aggressiveness on the client. While VoIP handsets and even tables should roam aggressively, in many scenarios laptops are used more like mobile devices and less like roaming devices. That is, they are used in one place, the screen is closed and they are taken to another place, and then they are used again. With such behaviors, continually probing for better APs while not moving only causes extra overhead on the network. At the same time, in many laptops, changing the roaming aggressiveness settings seems to have no significant impact. Therefore, the value of such changes must be considered on a device-by-device basis.

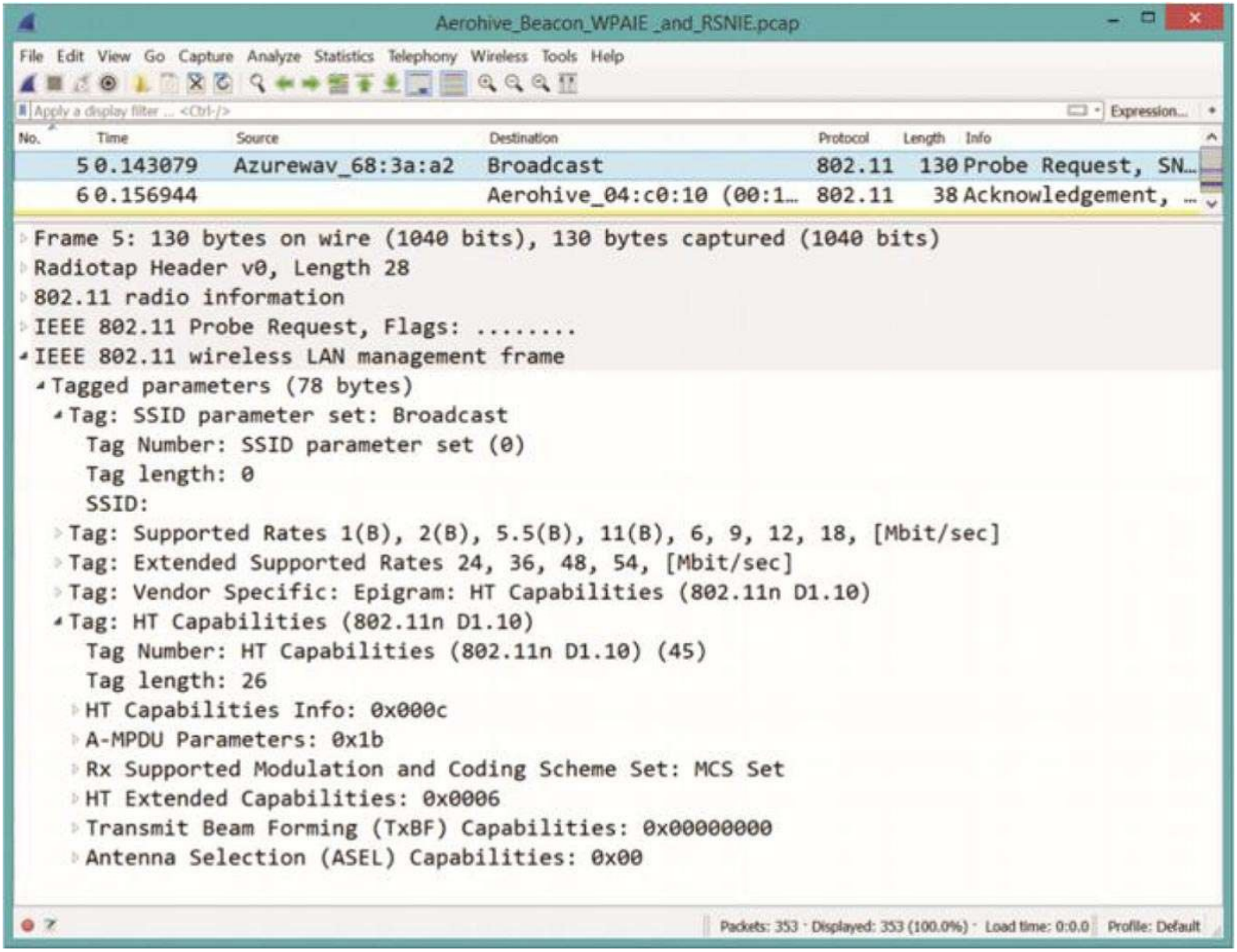


Figure 3.22: Probe Request Decode

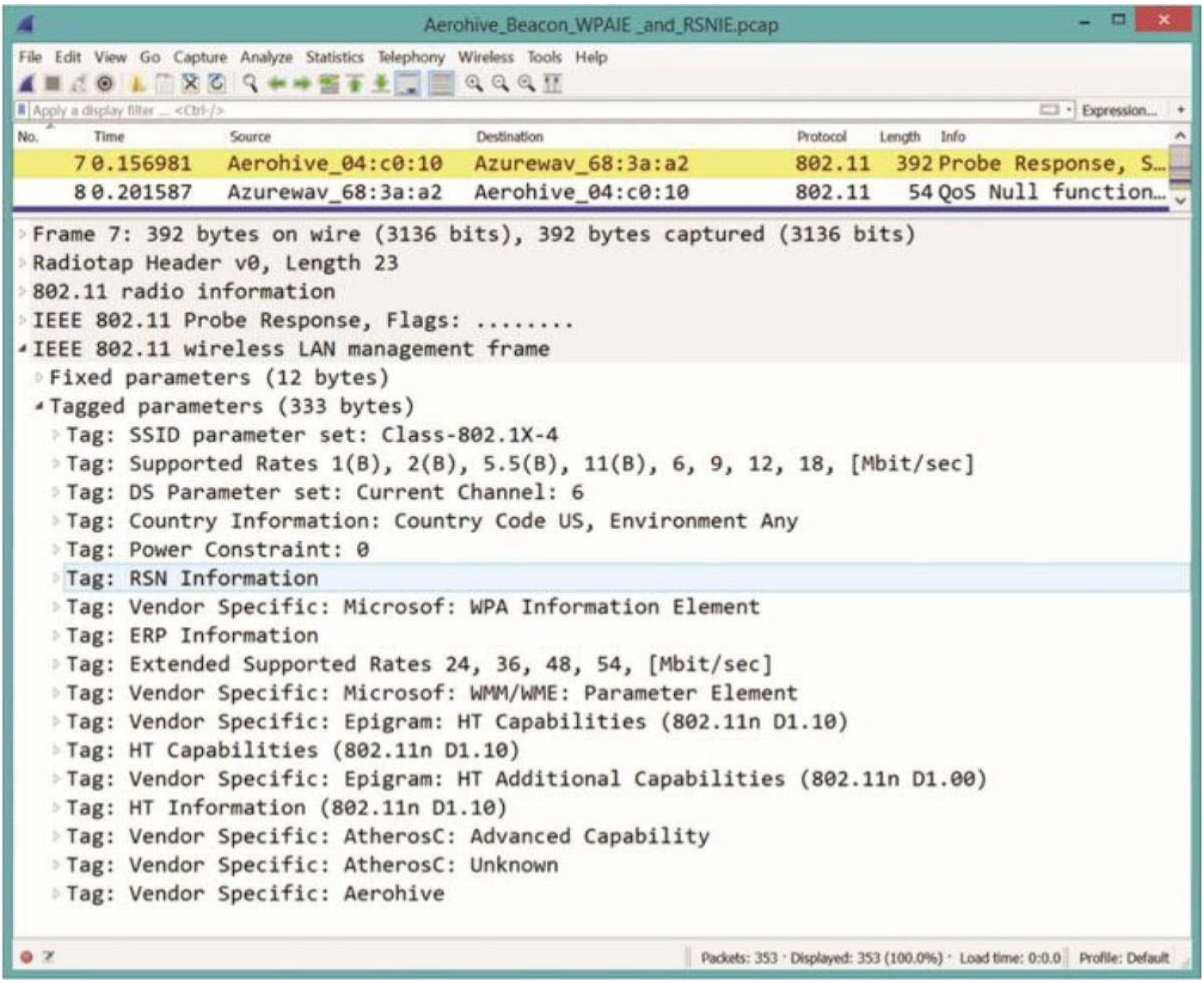


Figure 3.23: Probe Response Decode

Authentication and Deauthentication Frames

Authentication frames are used to enter the authenticated state with an AP. One frame is sent from the STA to the AP and another is sent back from the AP to the STA. This is true with all modern authentication methods that are commonly used today (WPA/WPA2 Personal and EAP). Figure 3.24 shows the authentication frames in Wireshark colorized with a red background and white foreground. Note that the first frame is from a source using an Aironet adapter, and the second frame is from a source named Cisco. The first frame is from the STA to the Cisco AP. The second frame is from the Cisco AP to the STA. The status code of “successful” in the decode frame indicates that the AP is accepting the authentication request.

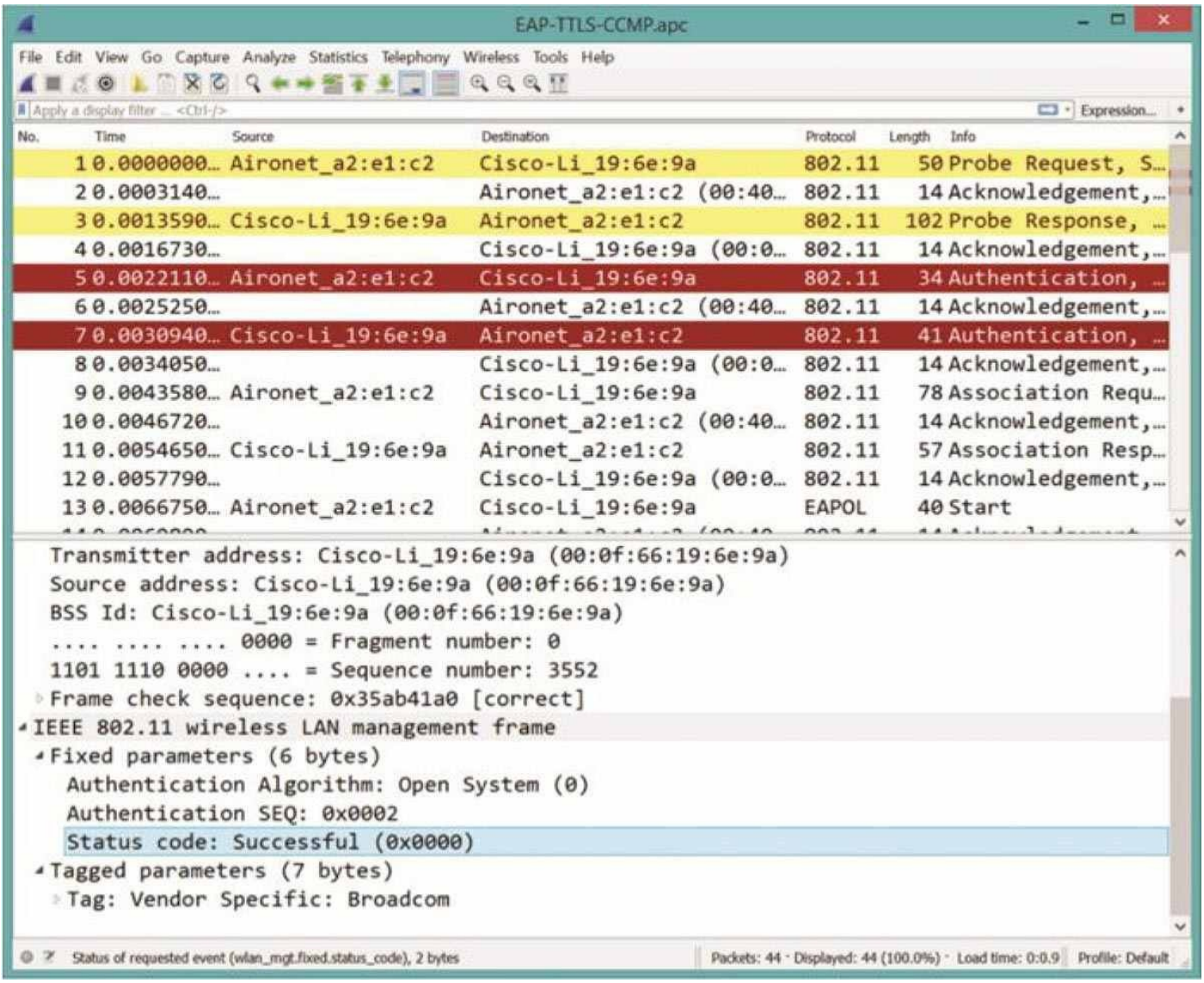


Figure 3.24: Authentication Frames in Wireshark

Deauthentication frames are used to end the authentication state with the AP. They can be sent in either direction to remove the authenticated state. If a deauthentication (deauth) frame is transmitted, it also removes the STA from the associated state, as a STA cannot be associated if it is not authenticated.

To filter on authentication frames in Wireshark, use the following filter:

```
wlan.fc.type_subtype == 0xb
```

To filter out authentication frames, use the following tiler:

```
wlan.fc.type_subtype != 0xb
```

Deauth frames have been used to perform DoS attacks and to gather information for other attacks on WLANs. For this reason, 802.11w introduced management frame protection, which protects deauth frames as well as disassociation, QoS action and Radio Measurement Action frames. The protection is the same as that for data frames in that the Frame Body field is encrypted if enabled per SSID. Frames protected under 802.11w are called protected management frames (PMFs).

Association and Disassociation Frames

Figure 3.25 shows the association request and response process. It is a simple four-frame exchange (authentication request, ACK, authentication response, ACK) used to enter the authenticated and associated state with the AP. After achieving this state, the STA may either use the network (Open System Authentication with no added security) or begin the 802.1X/EAP authentication process if used on the WLAN.

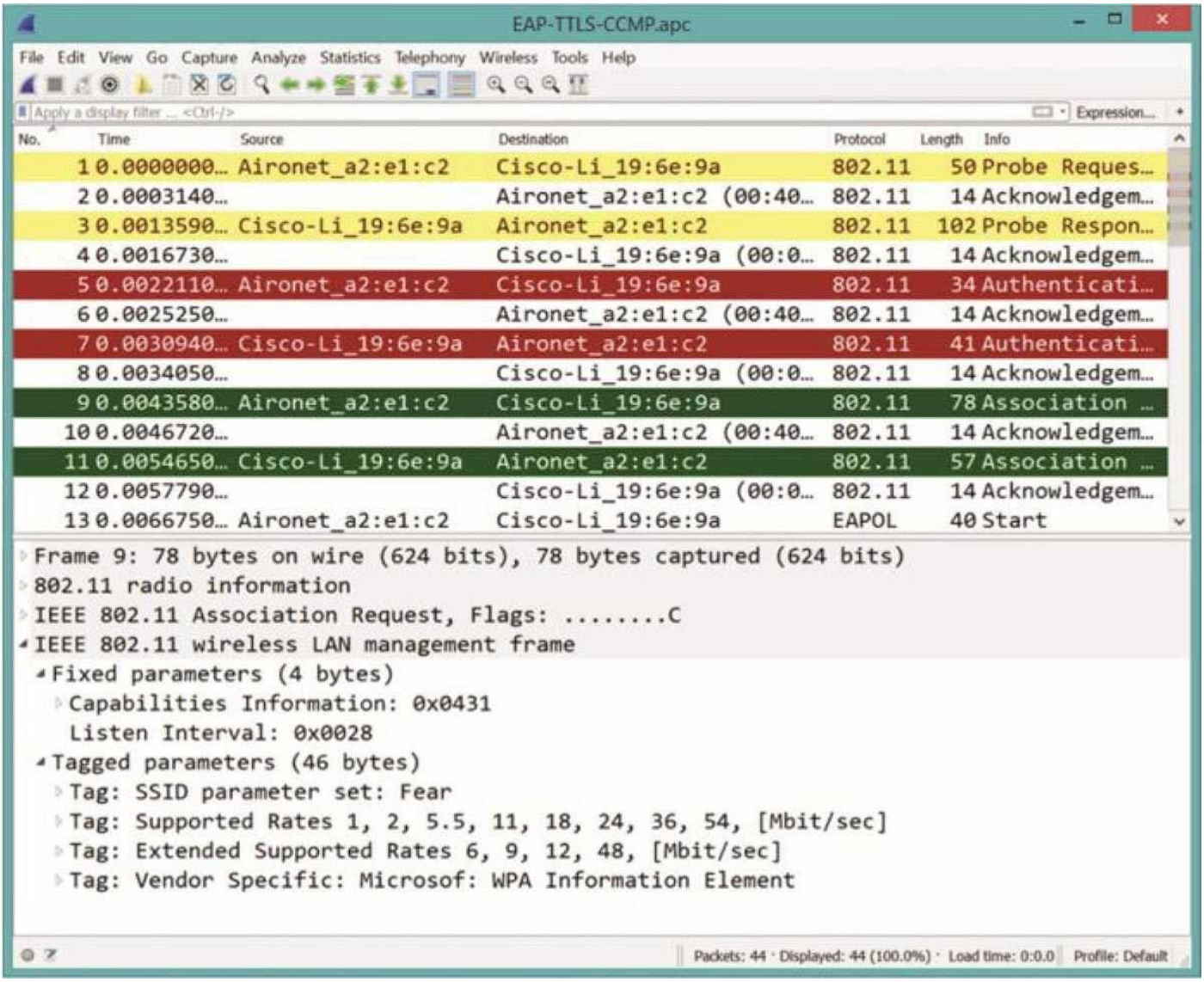


Figure 3.25: Association Request and Association Response Frames Colorized in Green

The disassociation frame is used to change from the authenticated and associated state to the authenticated not associated state. Disassociation frames are very simple. They contain a reason for the disassociation, vendor-specific information, and an integrity check when management frame protection is in use. The deauthentication frame is similar and uses the same basic structure. These two frames are in the management category and are both considered announcement frames. The concept of an announcement or notification frame is that the receiver cannot reject the request (unless management frame protection is enabled and the security checks fail). The receiver simply processes the request and either disassociates or deauthenticates the STA.

To filter on association request and association response frames in Wireshark, use the following filter:

```
wlan.fc.type_subtype == 0x0 or wlan.fc.type_subtype ==
```

```
0x1
```

To filter out association request and association response frames in Wireshark, use the following filter:

```
wlan.fc.type_subtype != 0x0 or wlan.fc.type_subtype !=
0x1
```

Reassociation Request and Response Frames

Reassociation request and response frames are used to roam to another AP within the extended service set (ESS) or to reconnect to an AP from which the STA has briefly disconnected. When used to reconnect to an AP from which the STA has briefly connected, the AP must still contain authentication information about the STA. The reassociation request frame is an acknowledged frame and works in concert with the reassociation response frame, which simply allows the association or disallows it. There is no complex back-and-forth procedure in the process.

The reassociation request frame body includes the parameters in Table 3.7.

Order	Information	Description
1	Capability	Details of this field are shown in Figure 3.26.
2	Listen Interval	Indicates how often a STA in power save mode wakes to listen to beacons.
3	Current AP address	The MAC address of the AP to which the STA is currently associated, if any.
4	SSID	Contains the SSID and is between 0-32 octets.
5	Supported rates	This field is not present if dot11DMGOptionImplemented is true.
6	Extended Supported Rates	The Extended Supported Rates element is present if there are more than eight supported rates, and it is optional otherwise. This element is not present if dot11DMGOptionImplemented is true.
	Power	The Power Capability element is present if

7	Capability	dot11SpectrumManagementRequired is true or dot11RadioMeasurementActivated is true.
8	Supported Channels	The Supported Channels element is present if dot11SpectrumManagementRequired is true and dot11ExtendedChannelSwitchActivated is false.
9	RSN	The RSNE is present only if dot11RSNAActivated is true.
10	QoS Capability	The QoS Capability element is present if dot11QosOptionImplemented is true.
11	RM Enabled Capabilities	RM Enabled Capabilities element is present if dot11RadioMeasurementActivated is true.
12	Mobility Domain	The MDE is present in a Reassociation Request frame if dot11FastBSSTransitionActivated is true, and the frame is being sent to an AP that advertised its FT Capability in the MDE in its Beacon or Probe Response frame (i.e., AP also has dot11FastBSSTransitionActivated is true).
13	Fast BSS Transition	An FTE is present in a Reassociation Request frame if dot11FastBSSTransitionActivated is true and dot11RSNAAuthenticationSuiteSelected is 00-0F-AC:3, 00-0FAC:4, or 00-0F-AC:9 (i.e., part of a fast BSS transition in an RSN).
14	Resource information container (RIC)	The set of elements that formulate a RIC-Request is optionally present in a Reassociation Request frame if dot11FastBSSTransitionActivated is true and the FT Resource Request Protocol is not used and the frame is being sent to an AP that advertised its FT capability in the MDE in its Beacon or Probe Response frame (i.e., AP also has dot11FastBSSTransitionActivated is true) and Either dot11RSNAAuthenticationSuiteSelected is 00-0FAC:3 or 00-0F-AC:4 (i.e., part of a fast BSS transition in an RSN) or dot11RSNAActivated is false (i.e., not in an RSN).
15	Supported Operating	The Supported Operating Classes element is present if dot11ExtendedChannelSwitchActivated is true.

	Classes	
16	HT Capabilities	The HT Capabilities element is present when dot11HighThroughputOptionImplemented attribute is true.
17	20/40 BSS Coexistence	The 20/40 BSS Coexistence element is optionally present when the dot112040BSSCoexistenceManagementSupport attribute is true.
18	Extended Capabilities	The Extended Capabilities element is optionally present if any of the fields in this element are nonzero.
19	QoS Traffic Capability	The QoS Traffic Capability element is present if dot11MgmtOptionQoSTrafficCapabilityActivated is true.
20	TIM Broadcast Request	The TIM Broadcast Request element is present if dot11MgmtOptionTIMBroadcastActivated is true.
21	FMS Request	The FMS Request element may be present if dot11MgmtOptionFMSActivated is true.
22	DMS Request	The DMS Request element may be present if dot11MgmtOptionDMSActivated is true.
23	Interworking	The Interworking element is present if dot11InterworkingServiceActivated is true and the non-AP STA is requesting unauthenticated access to emergency services (see 10.3.5).
24	Multi-band	The Multi-band element is optionally present if dot11MultibandImplemented is true.
25	DMG Capabilities	The DMG Capabilities element is present if dot11DMGOptionImplemented is true.
26	Multiple MAC	The Multiple MAC Sublayers element is present if dot11MultipleMACActivated is true.

	Sublayers	
27	VHT Capabilities	The VHT Capabilities element is present when the dot11VHTOptionImplemented is true.
28	Operating Mode Notification	The Operating Mode Notification element is optionally present if dot11OperatingModeNotificationImplemented is true.

Table 3.7: Reassociation Request Frame Options

B0	B1	B2	B3	B4	B5	B6	B7
ESS	IBSS	CF Pollable	CF-Poll Request	Privacy	Short Preamble	PBCC	Channel Agility
B8	**B9**	**B10**	**B11**	**B12**	**B13**	**B14**	**B15**
Spectrum Mgmt	QoS	Short Slot Time	APSD	Radio Measurement	DSSS-OFDM	Delayed Block Ack	Immediate Block Ack

Figure 3.26: Capability Field Values for Management Frames

The reassociation response frame will also include an association ID (AID) for the STA and a status code indicating reassociation success or failure, and includes additional option fields as referenced in IEEE 802.11-2012 clause 8.3.3.8.

To filter on reassociation request and reassociation response frames in Wireshark, use the following filter:

```
wlan.fc.type_subtype == 0x2 or wlan.fc.type_subtype ==
0x3
```

To filter out reassociation request and reassociation response frames in Wireshark, use the following filter:

```
wlan.fc.type_subtype != 0x2 or wlan.fc.type_subtype =!
0x3
```

Request to Send (RTS) and Clear to Send (CTS) Frames

RTS and CTS frames are used to clear the medium for transmission of larger frames. In environments with many collisions (typically detected with high retry rates), it can improve efficiency to enable RTS/CTS for communications. The RTS frame is transmitted by the STA desiring to send a larger frame. The CTS frame is sent back as a response. Figure 3.27 shows the format of the RTS frame and Figure 3.28 shows the format of the CTS frame.

The Duration field in RTS/CTS frames is very important. In the RTS frame it is a time in

microseconds represented by:

```
Data or management frame duration + CTS duration + one
ACK duration + three SIFS
```

This formula allows the medium to be cleared for the entire duration of the data frame transmission. The CTS response frame has a duration in microseconds represented by:

```
Value of the duration field from the preceding RTS frame
- CTS duration - one SIFS
```

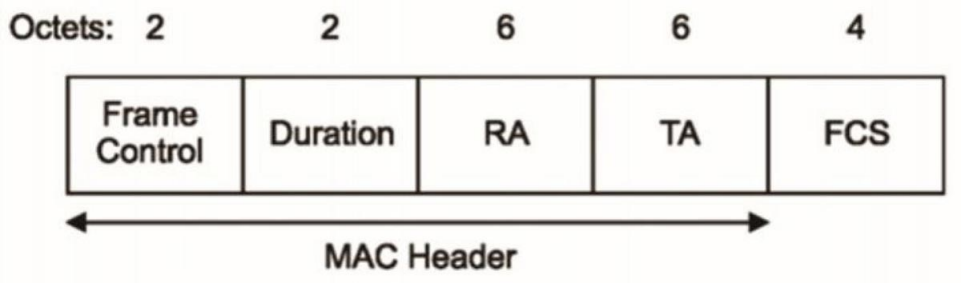


Figure 3.27: RTS Frame

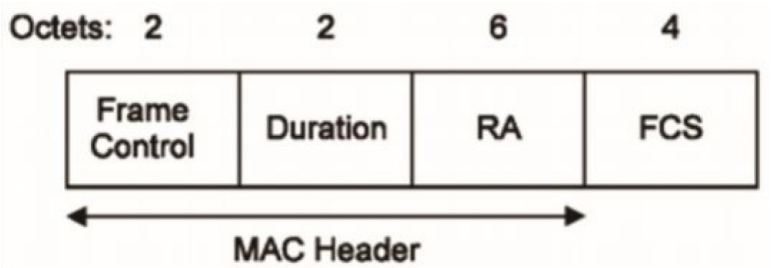


Figure 3.28: CTS Frame

What is sometimes called CTS-to-Self is a CTS frame sent without a preceding RTS frame. It is called CTS-to-Self as the RA field is set to its own address, but all STAs within range will hear the frame and set their NAV timers accordingly from the Duration field of the CTS frame. The Duration field of a CTS-to-Self frame is represented by:

```
Data or management frame duration + two SIFS + one ACK
```

This formula assumes the data or management frame requires an acknowledgement. If it does not, simply remove the ACK to determine the Duration field value.

To filter on RTS/CTS frames in Wireshark, use the following filter:

```
wlan.fc.type_subtype == 0x1b or wlan.fc.type_subtype ==
0x1c
```

To filter out RTS/CTS frames in Wireshark, use the following filter:

```
wlan.fc.type_subtype != 0x1b or wlan.fc.type_subtype =!
0x1c
```

Acknowledgement (ACK) Frames

ACK frames are sent immediately after data and management frames to inform the transmitter that the frame was received. Without an ACK frame, the transmitter assumes the frame was lost due to corruption from interference or some other issue, and so

retransmits the frame. At each retransmission, the random backoff timer length is increased until it reaches a maximum of 1023. This prevents a STA from consuming excessive airtime without doing the right thing—lowering the data rate so that the frame can get through. It is better, by far, to send a frame at 54 Mbps and get it through than to send it five times to get it through at 150 Mbps. The inability to get a frame through without excessive retries is a factor in vendor algorithms for deciding on data rate shifting events.

The ACK frame is a simple frame with Frame Control, Duration, RA and FCS subfields. The frame format is identical to a CTS frame in size. It uses the address of the STA that sent the frame being acknowledged in the RA subfield, and not the address of the STA sending the ACK frame. Unlike the CTS frame, if the immediately previous frame had the More Fragments bit set to 0, the Duration in the ACK frame is set to 0. CTS frames always have some length value in the Duration field because it is always setting up for transmission of a frame or frames. The ACK frame may be involved in a communication where more fragments are to come. In this scenario, it will set the Duration field value based on the following:

```
Duration value of previous frame + ACK time + SIFS time
```

Note: **When calculating Duration field values that include a fraction of a microsecond in the result, the value is always rounded up to the next microsecond.**

To filter on ACK frames in Wireshark, use the following filter:

```
wlan.fc.type_subtype == 0x1d
```

To filter out ACK frames in Wireshark, use the following filter:

```
wlan.fc.type_subtype != 0x1d
```

Null Data and PS-Poll Frames

Null Data frames can be used to notify an AP that a STA is awake and able to receive frames. The Null Data frame is simply a data frame with no data in the Frame Body field.

To filter on Null Data frames in Wireshark, use the following filter:

```
wlan.fc.type_subtype == 0x24
```

To filter out Null Data frames in Wireshark, use the following filter:

```
wlan.fc.type_subtype != 0x24
```

Power Save Poll (PS-Poll) frames are used to notify the AP that the client STA is awake and available for buffered frames. PS-Poll frames use the format shown in Figure 3.29. Notice the inclusion of the AID, which is used by the AP to gather and send buffered frames for the client STA.

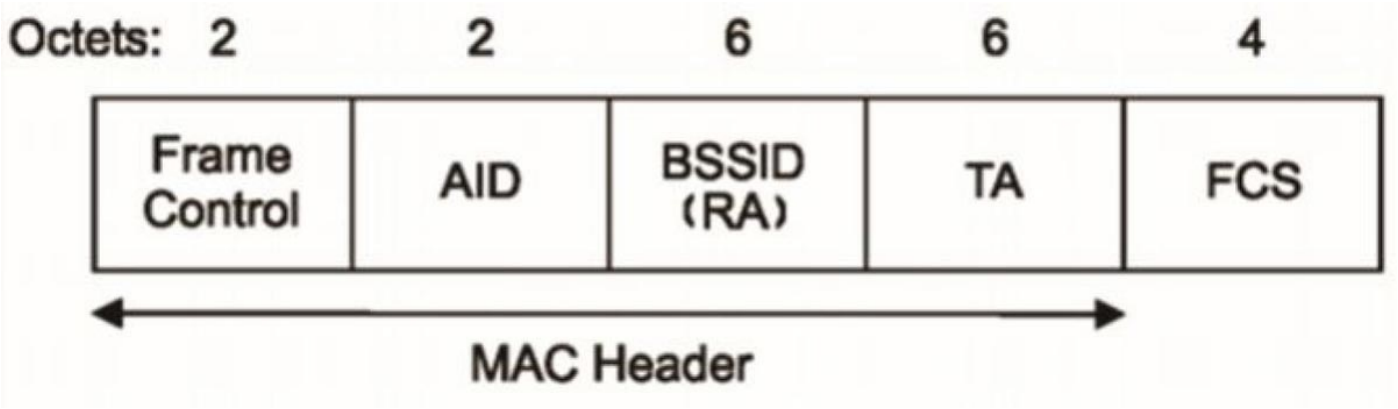


Figure 3.29: PS-Poll Frame Format

STAs indicate the power save mode using the Power Management (PM) bit in the Frame Control field. When a STA is in PM mode (PM bit = 1), it alternates between awake and dozing states. In this case, the AP buffers all unicast traffic destined to the PS STA. When one STA in the BSS is in PS mode, all group addressed traffic is also buffered until after the DTIM Beacon.

The client wakes up at every Listen Interval (a client setting) to listen for Beacon frames. In Beacon frames, the client checks AID 0 (for group traffic) and its own unique AID to check for buffered data. If it finds buffered data (indicated by a 1 bit for its AID), it sends a PS-Poll frame requesting that the AP send unicast buffered traffic one frame at a time. The data sent by the AP to the STA has the More Data bit set to 1 if there is more buffered data. If so, the client will send a new PS-Poll each time. If there are no more buffered frames, the client STA may return to sleep.

In real-world implementations, the PM bit may be used more actively. Instead of leaving the PM bit to 1 and sending PS-Polls when traffic is buffered, the client may simply flip the PM bit to 0, causing the AP to transmit all of its buffered traffic to the client. It then flips the PM bit back to 1 and begins dozing again. This is a more efficient use of the air time for both the client and the surrounding cell. This process is non-standard, but it is used by many client devices.

Two ways exist in which the AP may send the buffered data frames to the client. If the data belongs to a legacy power-save queue, transmission follows the legacy power save as documented previously. If the data belongs to a WMM Power Save queue, data frames are downloaded according to a trigger-and-delivery mechanism. WMM-PS is set for each access category (AC) separately, allowing more frequent data transmission for applications that require them.

Trigger frames are data frames that are acknowledged by the AP. One of the important enhancements of WMM was allowing a data frame to be a trigger frame. In this way, the client can send data to the AP while also triggering delivery of the AP’s buffered frames for the client. This is especially useful in bi-directional applications, such as voice. For example, every 20 ms the client can wake up, send its uplink voice data frame to the AP, and also use this voice data frame as a trigger frame for the buffered downlink frame. Since voice codecs send frames at known intervals (factoring in network delays), the client can time its frame delivery and trigger process based on the data frame interval, such as 20 ms.

When the AP has multiple buffered frames for the client, the data frames can be sent during an EDCA transmit opportunity (TxOP) burst with interleaved ACKs. WMM-PS addresses the inefficiencies of legacy PS while adding enhancements for performance offered by WMM.

The 802.11 specification defines both scheduled (for either contention-free or contention-based access) and unscheduled service periods, but the WMM-PS program uses only unscheduled service periods. The terms delivery- and trigger-enabled relate to a client STA's ability to trigger (with a data frame) the downlink delivery of buffered frames.

WMM-PS has multiple advantages over legacy power save, including:

- No need to wait for Beacon frames. Application requirements can dictate how often the STA will wake up.
- Downlink frames can be sent in a burst instead of requiring a separate trigger frame for each downlink frame.
- The trigger frame can be a data frame instead of requiring a PS-Poll control frame.
- Applications experience lower latency when power-saving features are used.
- The client spends more time sleeping, thus it has better power save efficiency.

To filter on PS-Poll frames in Wireshark, use the following filter:

```
wlan.fc.type_subtype == 0x1a
```

To filter out PS-Poll frames in Wireshark, use the following filter:

```
wlan.fc.type_subtype != 0x1a
```

Beacon Frame Timing

Now that you have explored additional frame types and are aware of the contention or arbitration algorithms used on WLANs, it is important to know that beacons are sent at a target beacon transmission time (TBTT). That is, they are configured by default to be transmitted every 100 TUs as discussed earlier. However, you have now seen that many frames are transmitted on the wireless medium. For this reason, it is likely that occasions will occur when the beacon frame simply cannot be sent every 100 TUs, but will be sent as soon as possible after 100 TUs. Figure 3.30 illustrates this concept. Due to the busyness of the wireless medium, at times, the beacon is sent outside or at longer time windows than the TBTT.

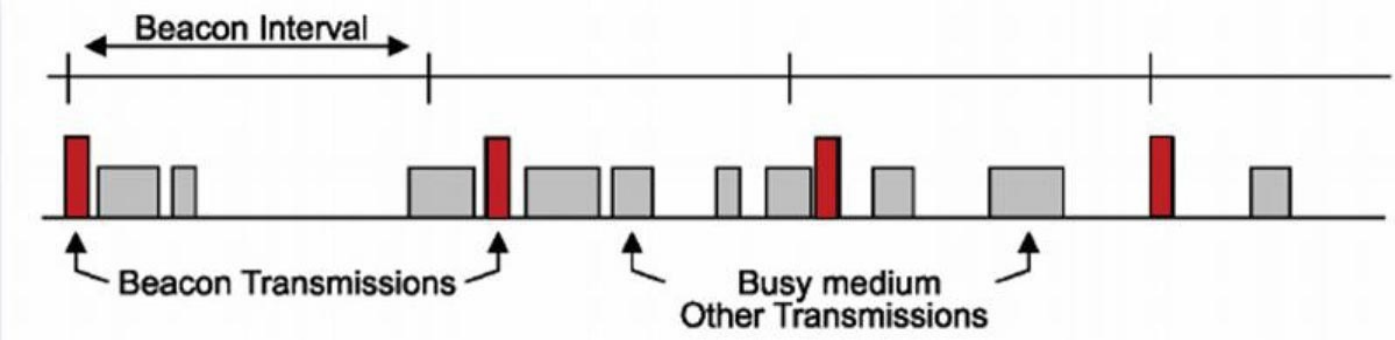


Figure 3.30: TBTT and Beacon Transmission

EXAM MOMENT: Beacon frames simply are not sent every 100 TUs, they are sent when they can be sent after or at 100 TUs. Beacon frames must contend for the medium like other frames. The reality is that they are sent as soon as possible and often immediately after or on the TBTT. However, the beacon interval is set and the AP will move back to the time interval on subsequent beacon transmissions assuming the medium is not busy.

Security Communications

Today, with the exception of the protected bits and information of security capabilities as covered in tables in the preceding section, most secure WLANs use WPA or WPA to secure the networks and they do not use 802.11 frame exchanges alone, but take advantage of additional protocols. Of course, these protocols still rely on 802.11 frame transmissions, but the exchanges that allow secure setup use EAP over LAN (EAPoL), RADIUS packets, and LDAP packets. This section provides a brief overview of WPA and WPA2 and then the EAP, RADIUS and LDAP exchanges.

WPA and WPA2 Personal

WPA and WPA2 are certifications of the Wi-Fi Alliance. They validate that a device implements portions of the security within 802.11. For example, WPA validates that a device properly implements the Temporal Key Integrity Protocol (TKIP) for authentication and key management and Rivest Cipher 4 (RC4) for encryption. WPA2 validates that a device properly implements CCMP for authentication and key management and the Advanced Encryption Standard (AES) for encryption.

WPA and WPA2 come in two basic forms: Personal and Enterprise. The Personal form is also known as Pre-Shared Key (PSK) because it uses a PSK or passphrase instead of key derivation exchanges with an authentication server. WPA Personal and Enterprise (TKIP/RC4) should no longer be planned for new implementations, as you learned in CWSP. It was provided as a transitional security solution to move away from WEP to CCMP/AES (WPA2).

For more details on WPA-Personal and WPA-Enterprise, please see the CWSP Official Study Guide. This section will focus primarily on the Enterprise form of WPA2. Figure 3.31 shows a Wireshark TKIP PSK capture.

EXAM MOMENT: TKIP/RC4 is deprecated in the 802.11 standard. It should not be planned or implemented for newer installations. TKIP/RC4 roughly equals WPA.

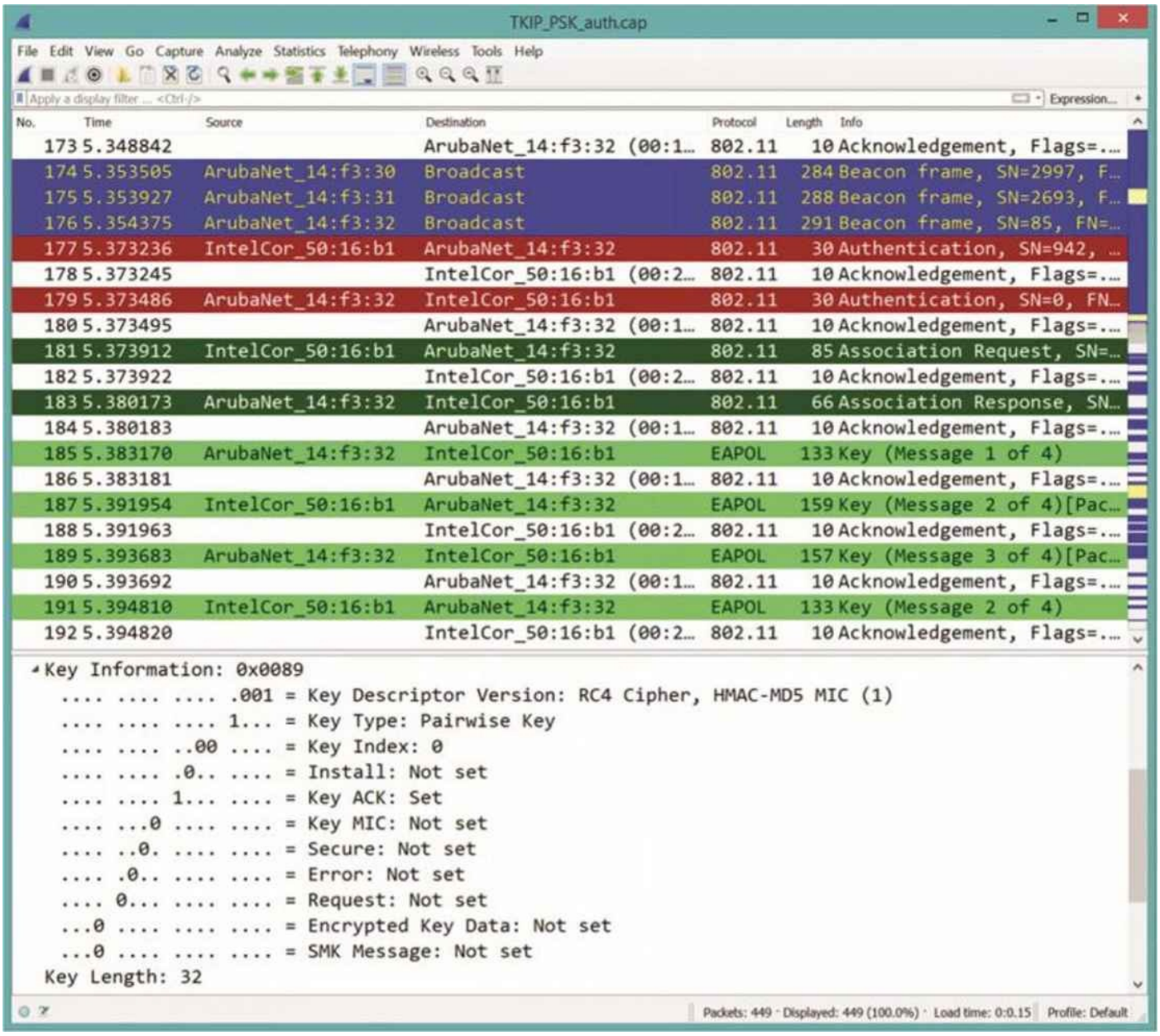


Figure 3.31: Wireshark TKIP (WPA) PSK Capture

WPA2 Enterprise

WPA- and WPA2-Enterprise utilize 802.1X as a framework for authentication and key management. Figure 3.32 shows the basic architecture of WPA2-Enterprise. Note the three primary components of 802.1X:

- Supplicant (client STA)
- Authenticator (AP or controller)
- Authentication Server (usually RADIUS)

The EAPoL protocol is used between the client STAs and the AP or controller, and the RADIUS protocol is used between the AP or controller and the authentication server. To capture EAPoL packets, you must use a WLAN protocol analyzer or capture at the AP. To capture the RADIUS packets, you must capture on the wired side of the AP or at the AP or controller.

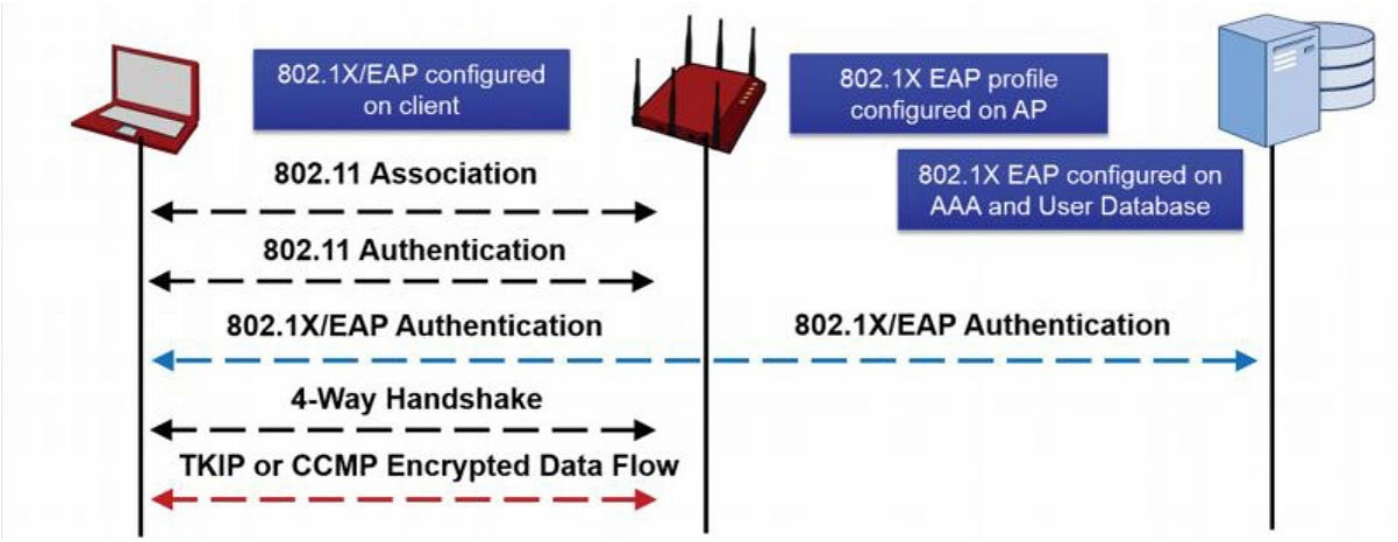


Figure 3.32: WPA2-Enterprise Architecture

When using WPA2-Enteprise, the following order of processing occurs:

- Perform Open System Authentication (authentication and association must be completed).
- Perform EAP authentication with the RADIUS server.
- Process the 4-way handshake to generate and provision encryption keys for the STA and the AP.
- Begin encrypted communications.

The 4-way handshake occurs with either WPA2-Personal or WPA2-Enterprise. However, when using WPA2-Personal, the RADIUS server is not required because the PSK provides the keying materials. When using WPA2-Enterprise, the keying materials are derived during the EAP authentication process. Figure 3.33 shows the 4-way handshake used in both WPA2-Personal and Enterprise.

The remainder of this section will explore EAP frames, RADIUS packets and LDAP packets to provide you with a basic understanding of the exchanges that occur.

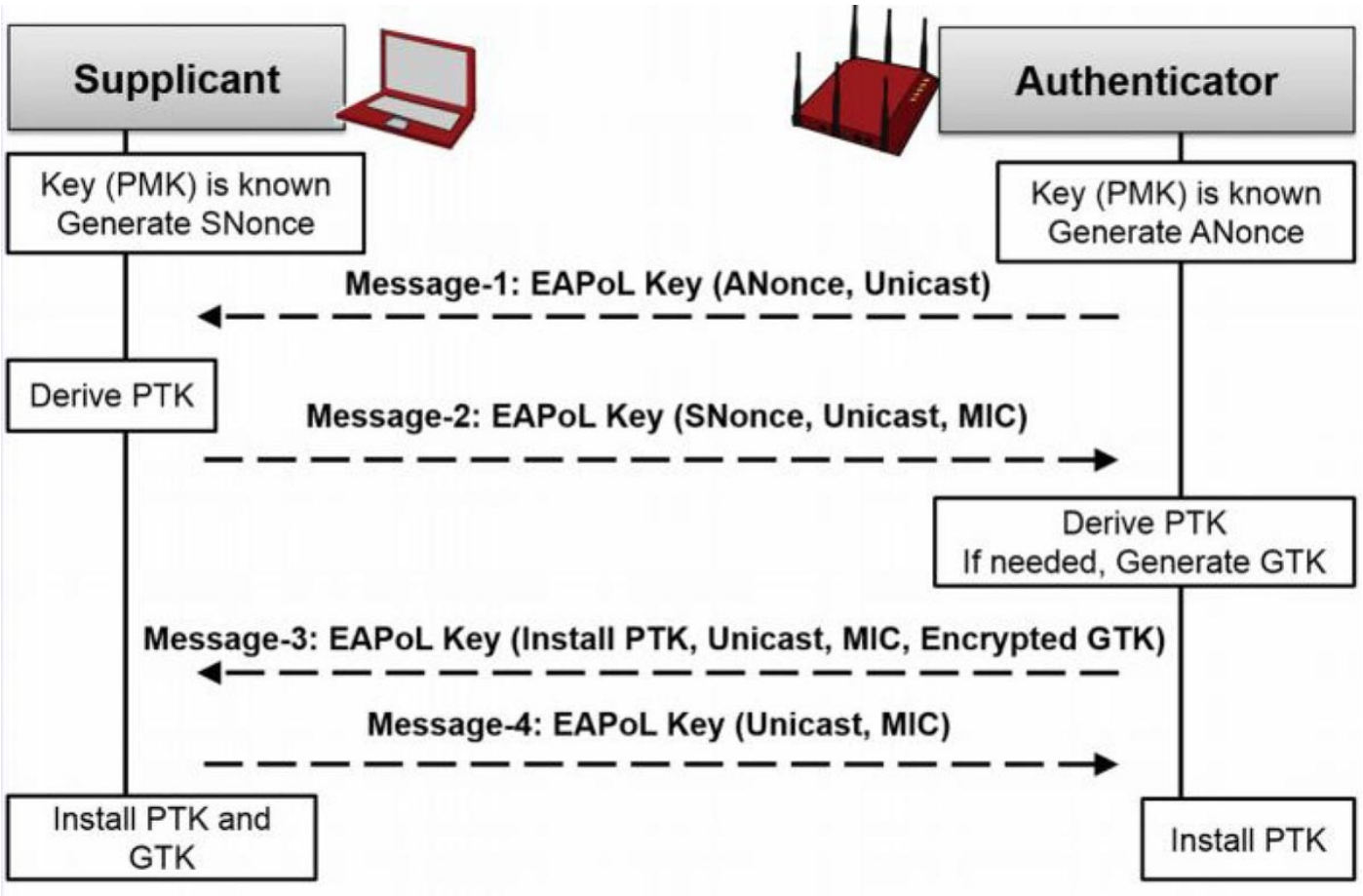


Figure 3.33: 4-Way Handshake

EAP Frames

On the WLAN side of the link (between the AP and the client STA), EAP frames will be used to authenticate and set up encryption. Figure 3.34 shows an entire capture from active scanning through to the successful 4-way handshake using LEAP (which is not considered a secure solution for modern WLANs).

The EAP packets are shown in light green in Figure 3.34. Notice the identity request and response, which is followed by EAP-LEAP negotiations. The EAP-LEAP negotiations result in a pairwise master key (PMK), which is derived from the master session key (MSK). The PMK is used in the 4-way handshake to generate a pairwise transient key (PTK) for encryption, and the group transient key (GTK) is also provided to the STA in an encrypted channel in this process. However, notice that even with secure encryption that Open System authentication is used first, as referenced earlier. The Open System authentication is highlighted in red and the association is highlighted in dark green.

Note: **This section does not describe the various EAP types in detail. They are explained in the CWNA Official Study Guide and in even greater depth in the CWSP Official Study Guide.**

RADIUS Packets

On the wired side of the network, during the WPA2-Enterprise process, Remote Authentication Dial-In User Service (RADIUS) packets are passed back-and-forth between the AP/controller and the RADIUS server. RADIUS is defined in request for comments (RFC) 2865. This document can be viewed by simply searching the Internet for RFC 2865. It is in standard ASCII text format and describes the RADIUS protocol. Originally developed for dial-up network connections, it is now heavily used in WLANs and occasionally on Ethernet LANs.

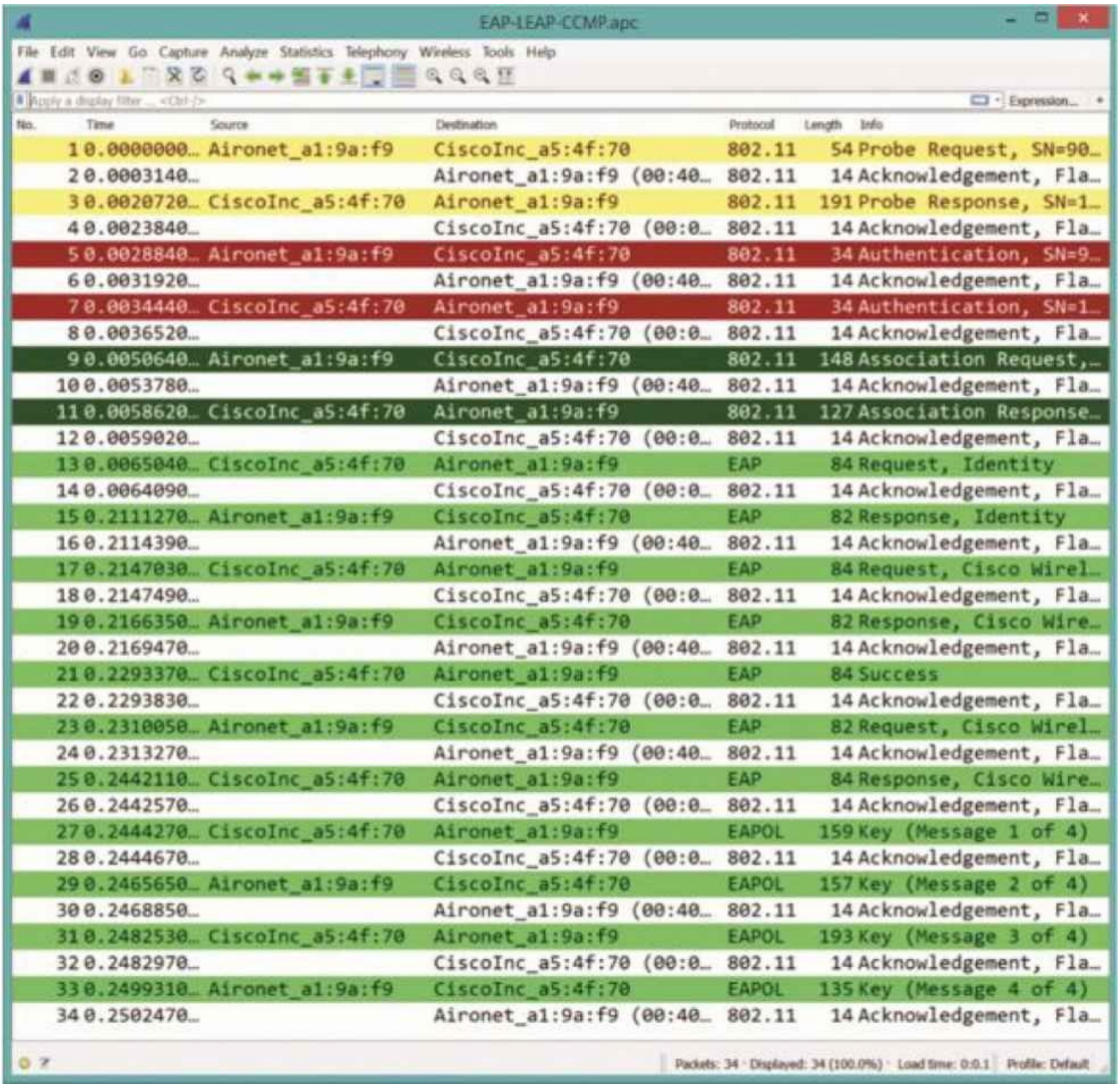


Figure 3.34: Open System Authentication followed by EAP-LEAP

The basic RADIUS process includes:

- Access Request
- Access Challenge
- Access Accept/Reject

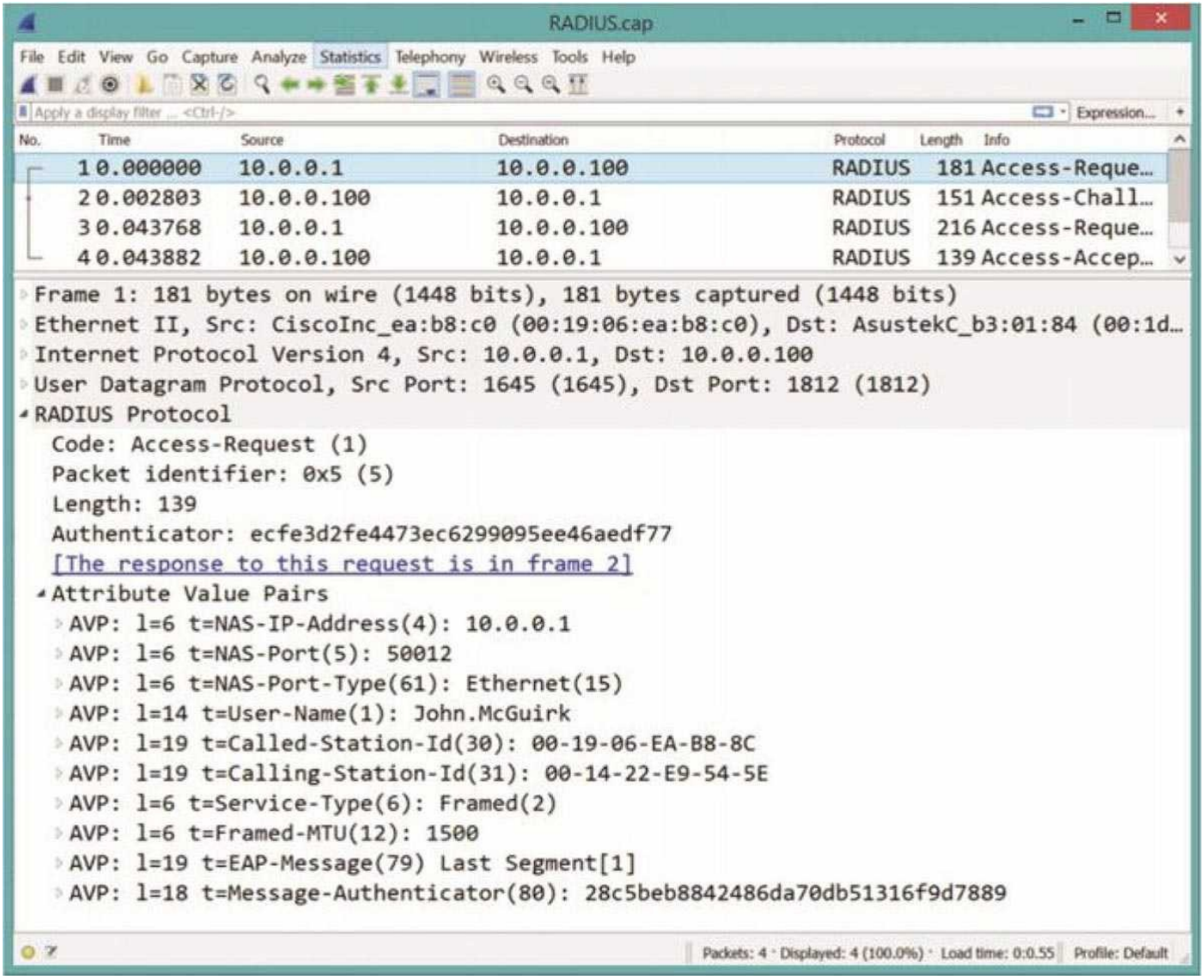


Figure 3.35: RADIUS Access Request to Initiate Authentications with RADIUS

RADIUS also supports accounting, but for our purposes, these three steps suffice. Depending on the EAP type used, either a username/password pair or a certificate is used in the access request procedure. Figures 3.35 through 3.38 show the four essential RADIUS packets used to authenticate. More packets may be used (and in the case of very weak methods fewer), but these four basic packets build the framework. They include an access request message followed by a challenge. Next is another access request message based on the challenge, and finally an access accept or reject message (Figure 3.38 shows the accept message).

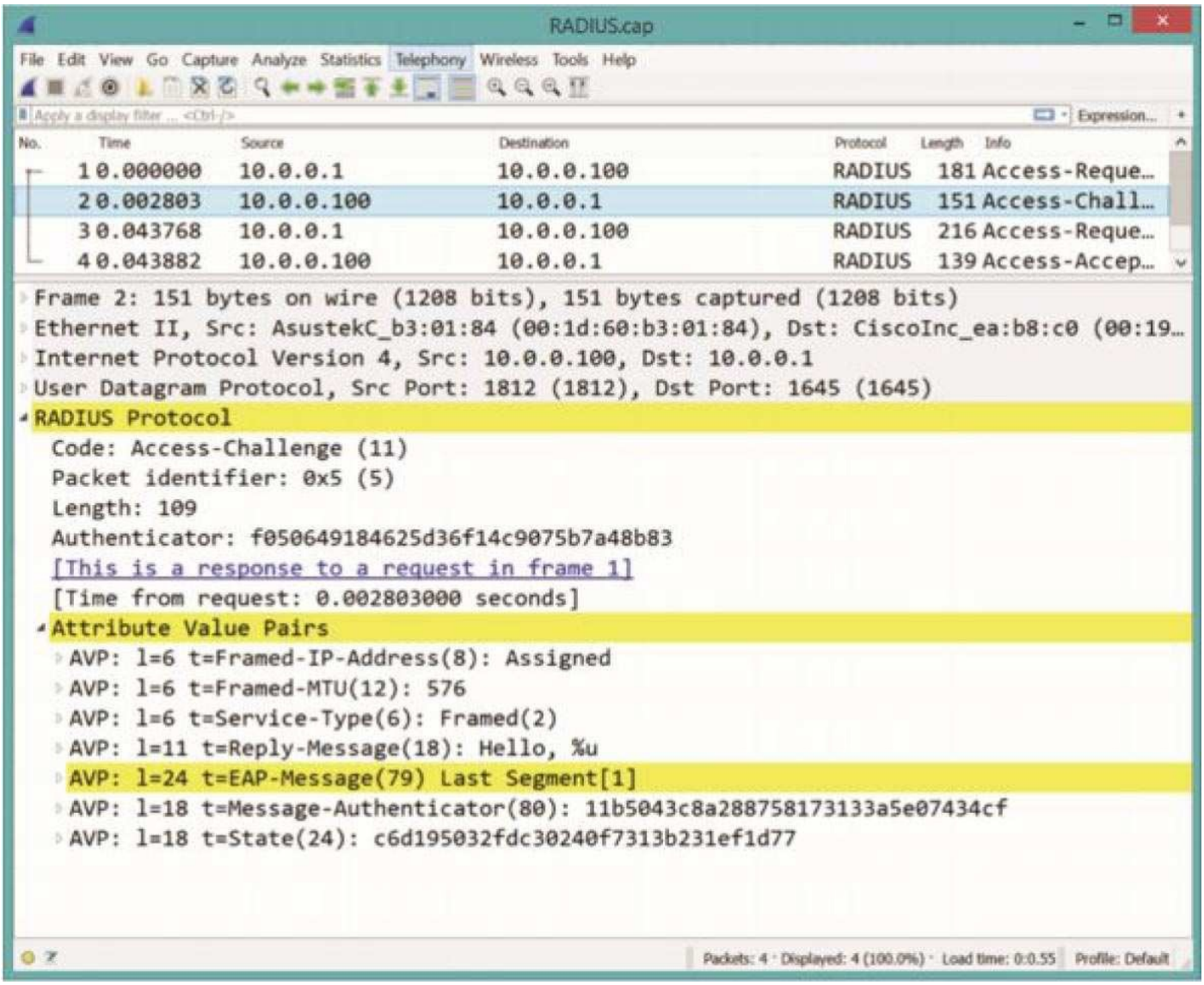


Figure 3.36: Radius Access Challenge from the Server

RADIUS.cap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.1	10.0.0.100	RADIUS	181	Access-Reque…
2	0.002803	10.0.0.100	10.0.0.1	RADIUS	151	Access-Chall…
3	0.043768	10.0.0.1	10.0.0.100	RADIUS	216	Access-Reque…
4	0.043882	10.0.0.100	10.0.0.1	RADIUS	139	Access-Accep…

```
▸ Frame 3: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits)
▸ Ethernet II, Src: CiscoInc_ea:b8:c0 (00:19:06:ea:b8:c0), Dst: AsustekC_b3:01:84 (00:…
▸ Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.0.0.100
▸ User Datagram Protocol, Src Port: 1645 (1645), Dst Port: 1812 (1812)
▾ RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0x6 (6)
    Length: 174
    Authenticator: 6a6f38e6dae830304d2333e5d5364643
    [The response to this request is in frame 4]
  ▾ Attribute Value Pairs
    ▸ AVP: l=6 t=NAS-IP-Address(4): 10.0.0.1
    ▸ AVP: l=6 t=NAS-Port(5): 50012
    ▸ AVP: l=6 t=NAS-Port-Type(61): Ethernet(15)
    ▸ AVP: l=14 t=User-Name(1): John.McGuirk
    ▸ AVP: l=19 t=Called-Station-Id(30): 00-19-06-EA-B8-8C
    ▸ AVP: l=19 t=Calling-Station-Id(31): 00-14-22-E9-54-5E
    ▸ AVP: l=6 t=Service-Type(6): Framed(2)
    ▸ AVP: l=6 t=Framed-MTU(12): 1500
    ▸ AVP: l=18 t=State(24): c6d195032fdc30240f7313b231ef1d77
    ▸ AVP: l=36 t=EAP-Message(79) Last Segment[1]
    ▸ AVP: l=18 t=Message-Authenticator(80): 2726e2713194ebf2bc894f6a6202af38
```

Packets: 4 · Displayed: 4 (100.0%) · Load time: 0:0.55 Profile: Default

Figure 3.37: Access Response from the Client Based on the Challenge

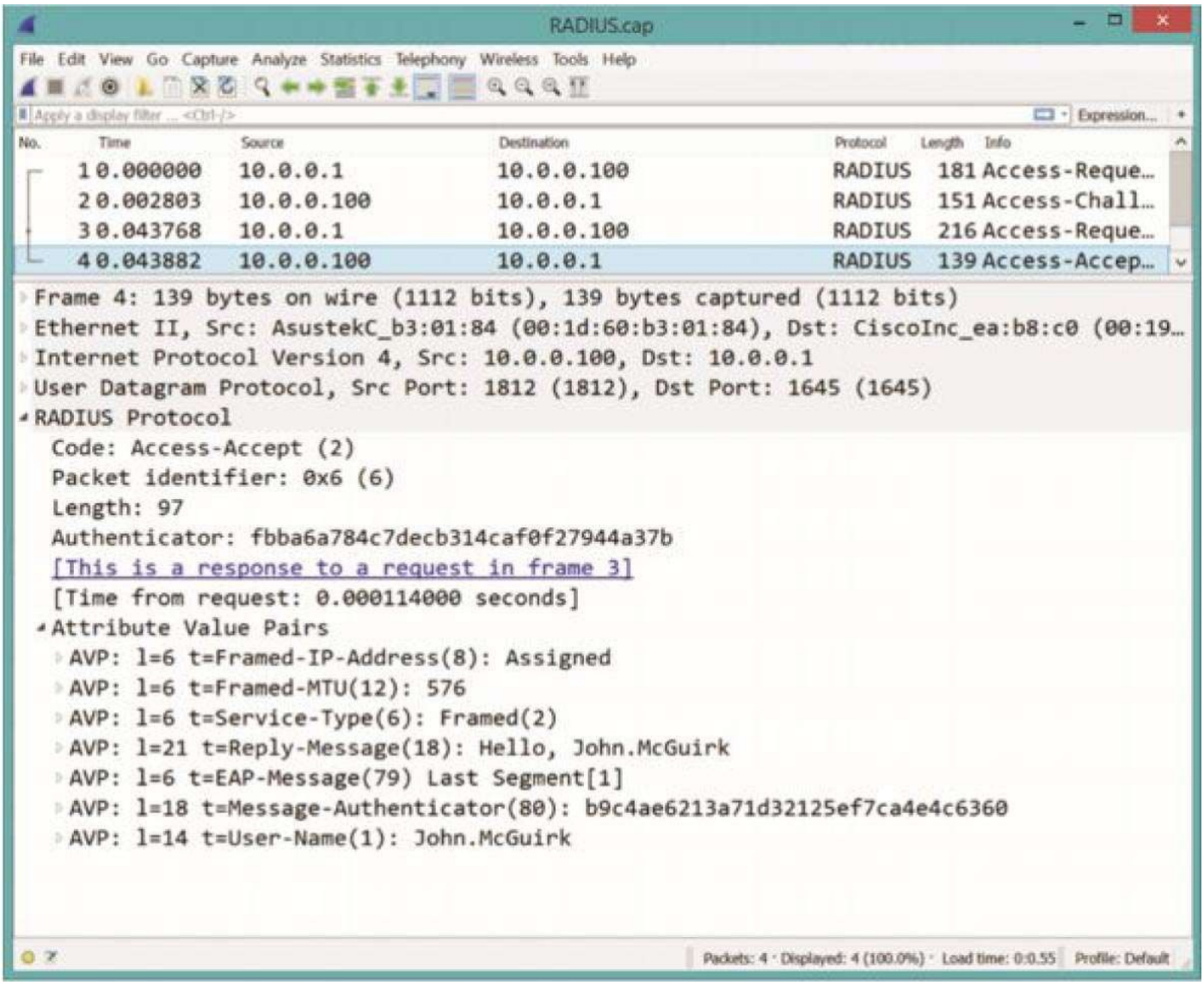


Figure 3.38: Access Accepted from the RADIUS Server (Successful Authentication)

LDAP Packets

Between the RADIUS server and the identity management system, the Lightweight Directory Access Protocol (LDAP) is often used. In some cases, the RADIUS server may contain the identities internally. In larger installations, organizations typically take advantage of existing identity management systems, like Active Directory Services. LDAP is defined in RFC 4511 and works based on the following basic procedure:

- Bind to an LDAP database.
- Search the database.
- Based on search results determine the validity of information provided through RADIUS.

Figure 3.39 shows an example of an LDAP capture using bind and search messages.

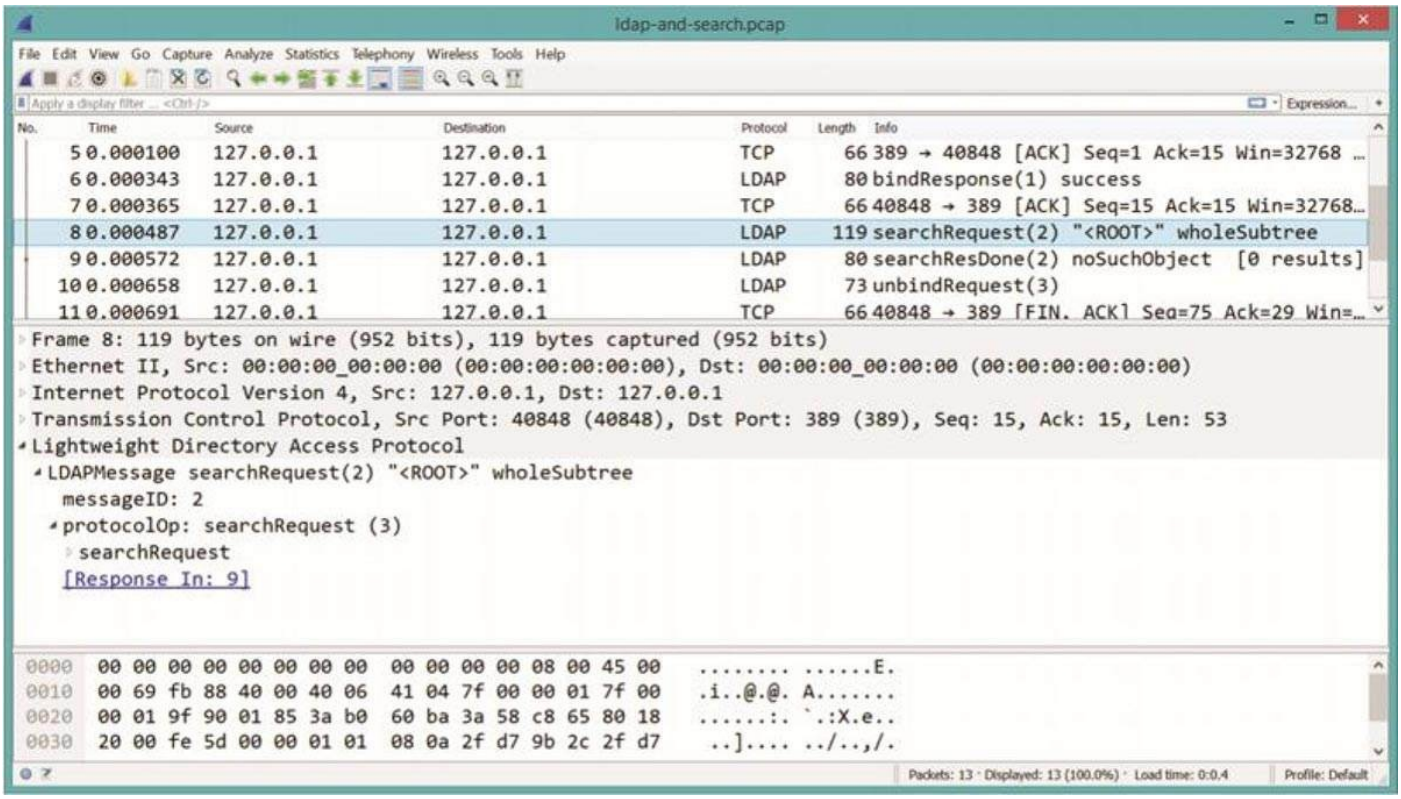


Figure 3.39: LDAP Packet Capture

802.11 PHY

The 802.11 PHY is divided into two sublayers. The Physical Layer Convergence Protocol (PLCP) and the Physical Medium Dependent (PMD) sublayers are used. The MAC layer communicates with the Physical Layer Convergence Protocol (PLCP) sublayer via primitives (a set of “instructive commands” or “fundamental instructions”) through a service access point (SAP). When the MAC layer instructs it to do so, the PLCP prepares MAC protocol data units (MPDUs) for transmission. The PLCP minimizes the dependence of the MAC layer on the PMD sublayer by mapping MPDUs into a frame format suitable for transmission by the PMD. The PLCP also delivers incoming frames from the wireless medium to the MAC layer.

The PLCP appends a PHY-specific preamble and header fields to the MPDU that contain information needed by the Physical layer transmitters and receivers. The 802.11 standard refers to this composite frame (the MPDU with an additional PLCP preamble and header) as a PLCP protocol data unit (PPDU). The MPDU is also called the PLCP Service Data Unit (PSDU), and is typically referred to as such when referencing physical layer operations. The frame structure of a PPDU provides for asynchronous transfer of PSDUs between stations. As a result, the receiving station's Physical layer must synchronize its circuitry to each individual incoming frame.

Both MAC and PHY layers conceptually include management entities, called the MAC sublayer management entity and the PHY sublayer management entity. These entities are referred to as the MAC Layer Management Entity (MLME), and the Physical Layer Management Entity (PLME). These entities provide the layer management service interfaces through which layer management functions may be invoked. In order to provide

correct MAC operation, a station management entity (SME) shall be present within each station. The SME is a layer-independent entity that may be viewed as residing in a separate management plane or as residing "off to the side." The exact functions of the SME are not specified in the 802.11 standard, but in general this entity may be viewed as being responsible for such functions as the gathering of layer-dependent status from the various layer management entities, and similarly setting the value of layer-specific parameters. The SME would typically perform such functions on behalf of general system management entities and would implement standard management protocols. Figure 3.40 depicts the relationship among management entities.

The various entities within this model interact in various ways. Particular interactions are defined explicitly within the 802.11 standard, via a service access point (SAP) across which defined primitives are exchanged. Other interactions are not defined explicitly within the 802.11 standard, such as the interfaces between MAC and MLME and between PLCP and PLME. The specific manner in which these MAC and PHY management entities are integrated into the overall MAC and PHY layers is not specified within the 802.11 standard.

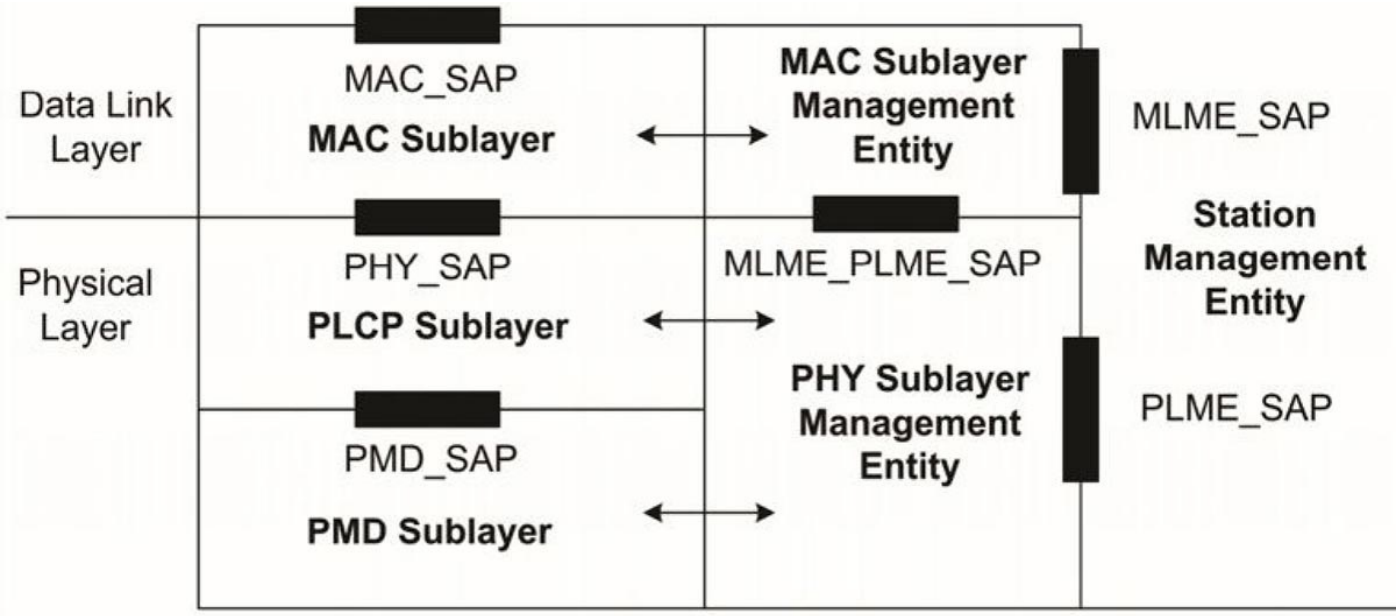


Figure 3.40: PHY Layer Architecture

The management information specific to each layer is represented as a management information base (MIB) for that layer. The MAC and PHY layer management entities are viewed as "containing" the MIB for that layer. The generic model of MIB-related management primitives exchanged across the management SAPs is to allow the SAP user-entity to either GET the value of a MIB attribute, or to SET the value of a MIB attribute.

The practical usage example of management primitives is when the user configures an access point or a mobile station's wireless utilities. This is done through a configuration interface such as CLI, GUI, SNMP, or custom software. Configuration of the access point's features through its web interface, for example, will SET a MIB attribute value to perhaps true/false or to some logical value.

> **EXAM MOMENT:** Due to lack of direct relevance of PHY service primitives to protocol analysis, they will not be explained in detail in this text. For more information on PHY primitives, refer to the 802.11 standard as amended. Learning

about primitives themselves is not relevant for the CWAP exam.

The general operation of the various Physical layers is very similar. To perform PLCP functions, the 802.11 standard specifies the use of state machines. Each state machine performs one of the following functions:

- Carrier Sense/Clear Channel Assessment (CS/CCA)
- Transmit (Tx)
- Receive (Rx)

Carrier Sense/Clear Channel Assessment is used to determine the state of the medium. The CS/CCA procedure is executed while the receiver is turned on and the station is not currently receiving or transmitting a packet. The CS/CCA procedure is used for two specific purposes: to detect the start of a network signal that can be received (CS), and to determine whether the channel is clear prior to transmitting a packet (CCA).

Transmit (Tx) is used to send individual octets of the data frame. The transmit procedure is invoked by the CS/CCA procedure immediately upon receiving a PHY-TXSTART.request (TXVECTOR) from the MAC sublayer. The CSMA/CA protocol is performed by the MAC with the PHY PLCP in the CS/CCA procedure prior to executing the transmit procedure.

Receive (Rx) is used to receive individual octets of the data frame. The receive procedure is invoked by the PLCP CS/CCA procedure upon detecting a portion of the preamble sync pattern followed by a valid SFD and PLCP Header. Although counter-intuitive, the preamble and PLCP header are not truly “received”. Only the MAC frame is “received”.

802.11 PHY Preamble

At the PHY level, framing includes the preamble and the PLCP header. The preamble is used to prepare the receiver for the actual frame, including the PLCP header. The preamble differs among the various PHYs (for example, DSSS, HR/DSSS, ERP, OFDM, HT and VHT), but serves the same purpose—to provide synchronization for the receiver. The differences in the preambles and the PLCP headers are important because they may provide benefits, but they may also impact compatibility. That is, for coexistence with older PHYs, the preamble and PLCP header may have to use protection mechanisms.

Figure 3.41 shows the PHY frame format from the original DSSS PHY. A short preamble was introduced with HR/DSSS, but would only work with other receivers also supporting the short preamble. The short preamble was 72 bits as opposed to the 144 bits shown in Figure 3.41. When ERP was ratified, which also works in 2.4 GHz with DSSS and HR/DSSS, support for the short preamble was mandatory; however, when coexisting with older DSSS radios, the long preamble was still required. Today, most networks can use the short preambles without concern.

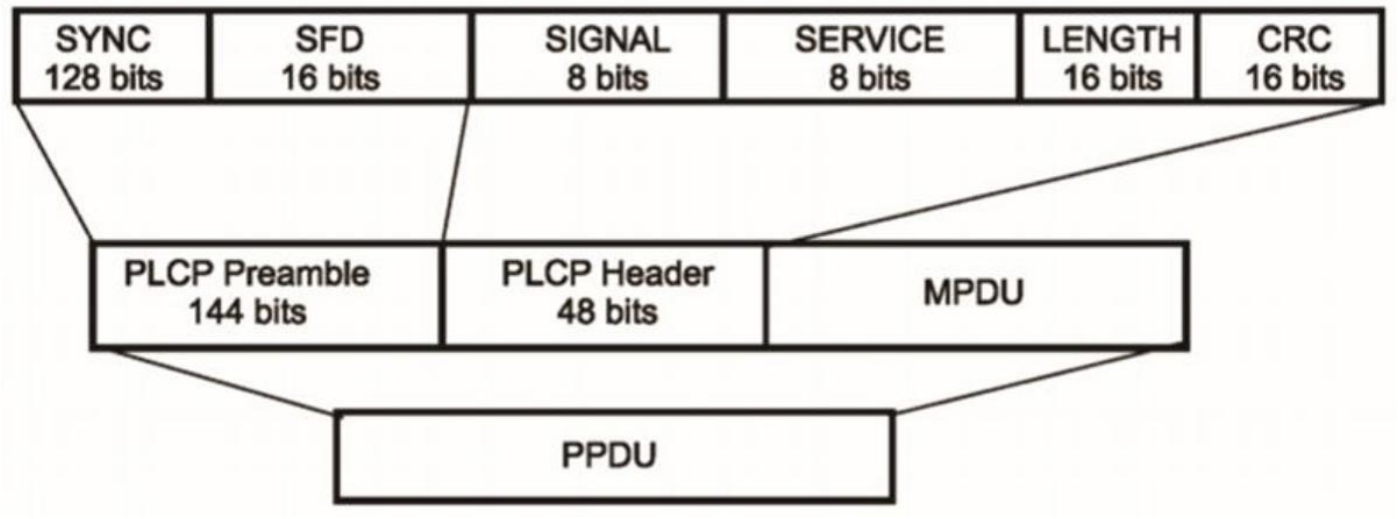


Figure 3.41: DSSS PLCP Frame Format

To understand the preamble better, consider the details of the original DSSS preamble. The preamble is the first of three parts of a PPDU. The preamble consists of two parts: The Synchronization (Sync) field and Start Frame Delimiter (SFD) field.

The Sync field consists of a string of 0s or 1s, alerting the receiver that a potentially receivable signal is present. A receiver will begin to synchronize with the incoming signal after detecting the Sync. Consider that receivers may not receive the entire Sync field, but rather only catch part of it. Since the Sync field is a continuous stream of 0s or 1s, it really does not matter where in the stream the receiver realizes that there is a Sync signal being transmitted so long as it synchronizes before the SFD arrives.

The Start Frame Delimiter field defines the beginning of a frame. The bit pattern for this field is always 1111001110100000 when using long preambles and reversed when using short preambles. These patterns are unique to the DSSS PLCP.

Starting with 802.11b, short preambles were optional, and there were various implementations of short preambles in the market. For example, some APs implemented short preambles as, “short preambles only.” Other access points implemented short preambles as “short or long preambles are ok.” In a, “short preambles only” implementation where the AP is configured for short preambles, a station using long preambles will not be able to associate. In a “short or long preambles are ok” implementation where the access point is configured for short preambles, stations using either long or short preambles may associate, but the lowest common denominator (long preambles) is always used in the BSS. Stated differently, if a long preamble station enters the BSS, the AP will declare that all stations must now use long preambles.

The 802.11g standard made support of both long and short preambles mandatory, such that all implementations where the AP has short preambles enabled meant, “short or long preambles are ok.” To see whether the AP has enabled short preamble support, see the Short Preamble bit of the Capability Information fixed field.

When only ERP stations are present in the 2.4 GHz BSS, the AP uses an OFDM PHY (and thus OFDM preambles) for the beacon frames. When a NonERP station associates to the BSS, the AP uses the DSSS PHY (and thus DSSS preambles) for the beacon frames. When the NonERP stations are all short-preamble capable, the AP sends the beacon with a short preamble. When any of the NonERP stations are long-preamble-only capable, the AP

sends the beacon using a long preamble. When a NonERP station sends a probe request frame to the AP using a long preamble, the AP must reply with a probe response frame using a long preamble. When a NonERP station sends a probe request frame to the AP using a short preamble, the AP must reply with a probe response frame using a short preamble. This was sometimes considered the “preamble echo” rule, though it is not called by this name in the 802.11 series of standards.

It is important to understand that this rolling backward compatibility still exists in the HT and VHT PHYs. That is, the least common denominator tends to win and, therefore, one older PHY device forces all other devices to deal with slower beacon frames and possibly longer preambles. Ridding the network of older devices can help with this problem and, thankfully, very few 802.11-prime devices are still in use today.

> **EXAM MOMENT:** It is not important, for the CWAP exam, that you know all the details of the variations of the PHY preambles; however, you should know that the preamble adds extra overhead to the communications and that older devices may introduce a preamble that reduces performance overall and forces all devices in the BSS to communicate based on that long preamble.

The HT PHY introduced the concept of three PPDUs (remember, the MPDU plus the PHY preamble and header):

- *Non-HT PPDU:* This is simple the OFDM PPDU used by 802.11a and 802.11g.
- *HT-Mixed PPDU:* This includes a starting preamble matching 802.11a and 802.11g and then adds training information for HT for backward compatibility in a mixed environment.
- *HT-Greenfield:* This uses only the HT preamble and PLCP header and only functions properly when no earlier PHYs (OFDM, ERP, etc.) are present.

The VHT PHY simplified things by having only one PPDU format, which is similar to the HT-Mixed PPDU, except it accommodated VHT operations. Now, it is important to know that any 802.11ac (VHT) radio will be able to process the OFDM, HT and VHT PHY formats; however, an HT radio cannot process a VHT PHY frame with full understanding, and an OFDM radio cannot process either the HT or VHT PHY frame (when targeted at another HT or VHT device) with full understanding. However, in such cases the older PHY can gather enough information to perform carrier sense and remain silent during transmission assuming a backward compatible PHY frame is used (such as HT-Mixed or the standard VHT PPDU).

802.11 PHY (PLCP) Header

The PLCP header includes information about the bandwidth, coding, streams, and guard interval used (short (400 ns) vs. standard or long (800 ns)), single user versus multi-user transmission (MIMO versus MU-MIMO), beamforming information, and error checking information. Older PLCP headers may lack some of this information, such as the short-guard interval and MU-MIMO and beamforming information.

> **EXAM MOMENT:** The full details of the PLCP header are beyond the scope of the

CWAP exam as sufficient information is readily revealed in a protocol analyzer designed for WLAN capture as shown in Figure 3.42 to understand the data rates used and, therefore, the PHY operations.

After the bits of the PLCP header are formed, they are modulated onto a carrier wave. The terms carrier wave and carrier signal are sometimes used interchangeably. Wireless engineers and technicians must deal with many different wireless technologies. In the 802.11 standard (as amended) alone, you are dealing with multiple modulation techniques, which are methods used to impose information onto carrier waves to create a carrier signal. Therefore, a brief summary of carrier waves and why they are important is in order.

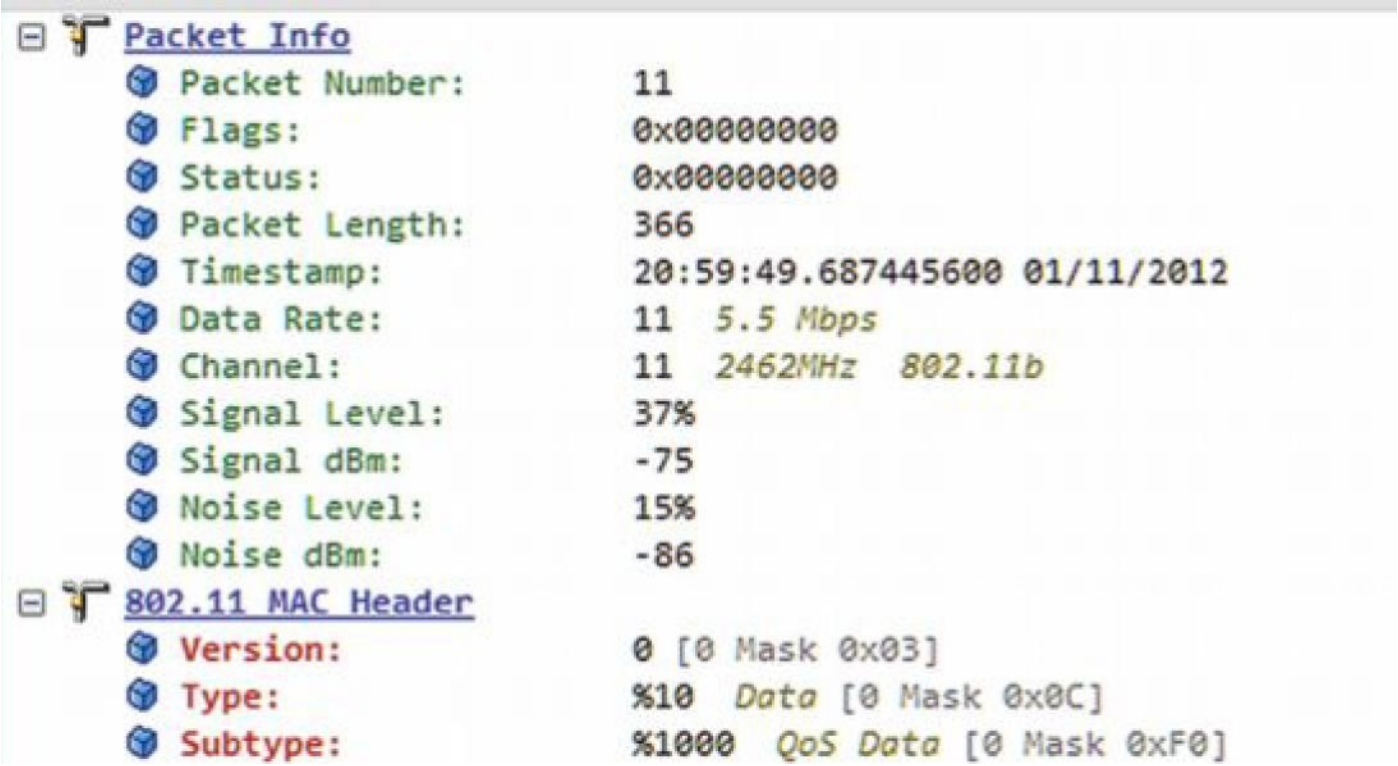


Figure 3.42: A Packet Decode in Omnipeek from Savvius Showing Packet Info

In Tom Standage's exceptional book, The Victorian Internet, he documents the many signaling methods we humans have used throughout the recent centuries. The book documents how Claude Chappe and his brother communicated over great distances using time-bound audio signals. The signal was unary in nature in that there was only one signal—clanking a pot. However, the brothers had synchronized their clocks so that a clank was linked to a second on the clock, and each number was linked to a letter to that a message could be sent. If the transmitting brother clanged the pot when the second hand was pointing to 12, the listening (receiving) brother new to translate the number 12 into the appropriate message.

As you can imagine, this system would not allow for rapid communications, but it did allow for communications over a short distance. Eventually, the brothers realized that sound waves were not good carriers of signals (since they attenuate so quickly and they take so long to arrive at the destination) so they developed a new system based on visual cues (light waves). Using a simple black and white two-sided panel (black on one side and white on the other) and a telescope, the brothers successfully communicated over a distance of about 10 miles.

What did both of these communications devices have in common? They both used waves to carry a signal. The first used sound waves and the second used light waves. Since light waves travel much faster than sound waves, the latter device worked much better and over greater distances.

However, a dilemma remained. Both of these early devices required a human interpreter on the other end at all times. The instrument of the human ear and the instrument of the human eye were used to interpret the data that was carried on the sound and light waves, respectively. In order to send information without a human interpreter, scientists and engineers had to develop concepts and tools related to electricity.

Today's carrier waves are almost always electromagnetic waves. Mechanical devices can be formed that transmit the waves and also receive the waves (called transmitters and receivers or combined as transceivers). This means that data can be sent and received by modulating the data onto the carrier waves by manipulating the waveform in some way. For example, the frequency can be modified to represent a binary 1 or a binary 0. The wave is generated, but it is manipulated in such a way so that it carries binary data and this makes it a carrier signal.

Modulation is defined as the process of manipulating a carrier signal so that it can represent intelligent information. Multiple kinds of modulation exist, but they fall into two general categories: digital modulation and analog modulation.

An RF signal can be modulated by manipulating the frequency, phase, or amplitude. Amplitude modulation is not sufficient alone for wireless LAN technologies since the amplitude is often affected by interference. This leaves frequency and phase modulation, and newer wireless LAN technologies use different kinds of phase modulation to achieve communications. Frequency modulation is also used, though it is less common today. In addition amplitude modulation may be combined with phase modulation to increase potential data rates.

Keep in mind that all computer processing is the manipulation of binary 1s and 0s. You can think of them as positive or negative, on or off, true or false; but they are usually referred to as bits and we call combinations of these bits binary numbers. For example, the computer byte is eight bits and these eight bits are said to form an eight bit binary number. The binary number 01101101 is one byte (also called an octet) and can represent anything that a coding system specifies. If it is used to represent whether eight different lights are off or on and a 0 means the light is off while a one means the light is on, we know that three of the lights are off and five of the lights are on, in this case. The point is simple: once you define what the 0s and 1s mean you can use them to communicate massive amounts of information and any kind of information.

How does this relate to modulation? RF signals are modulated so that they can represent these 0s and 1s. As long as a 0 or 1 can be represented, any computer information can be transferred on the signal.

Consider the following very simple example. Assume that two devices are configured to read signals at 1 millisecond intervals and that a change in phase would indicate a change in bit representation. In other words, every time the phase changes we toggle the bit. If there is no phase change, the devices assume the bit should stay the same as it was during

the last 1 millisecond interval. Therefore, once communications are established and a starting bit (let us say 0) is defined, any sequence of bits can be transmitted going forward. Let us further say that when actual data communications are about to begin, there is always a flip from 0 to 1 to 0 so that the receiving device knows to begin processing the next phase changes as information.

In this example, the sending alert—which you could refer to as a preamble—is sent first as 180 degree phase shifts from 0 to 1 and then back to 0. Next, two 0s are sent so there is no phase shift and these two 0s are followed by four 1s indicated by a phase shift at millisecond 6. Finally, another phase shift at millisecond 10 indicates that the transmission should now represent a 0 and the two 0s end the eight bit binary number that was transmitted.

While this is not an actual "in-use" modulation on 802.11 wireless LANs, it simplifies the modulation concept and helps you to begin understanding how phase-based modulation can function. Even this simple modulation example is dependent on the devices knowing the modulation scheme, which includes both the phase-shifting algorithm and the time window within which to accept a single bit. This phase-shifting algorithm is often called the keying mechanism of the modulation, and the time window is called the symbol or symbol period. Technically, the symbol is the smallest unit of data transmitted at one time. For example, BPSK modulation transmits one bit at a time where 16 quadrature amplitude modulation (16-QAM) transfers four bits at a time.

Physical Layers included in the 802.11 standard as amended and still used today with 802.11ac include:

- *DSSS*—Direct Sequence Spread Spectrum
- *HR/DSSS*—High Rate DSSS
- *OFDM*—Orthogonal Frequency Division Multiplexing
- *ERP*—Extended Rate PHY
- *HT*—High Throughput
- *VHT*—Very High Throughput

The FHSS PHY is now defunct in 802.11 WLANs; however, a frequency-hopping network is still commonly used and that is the Bluetooth communications networks.

The modulations used include:

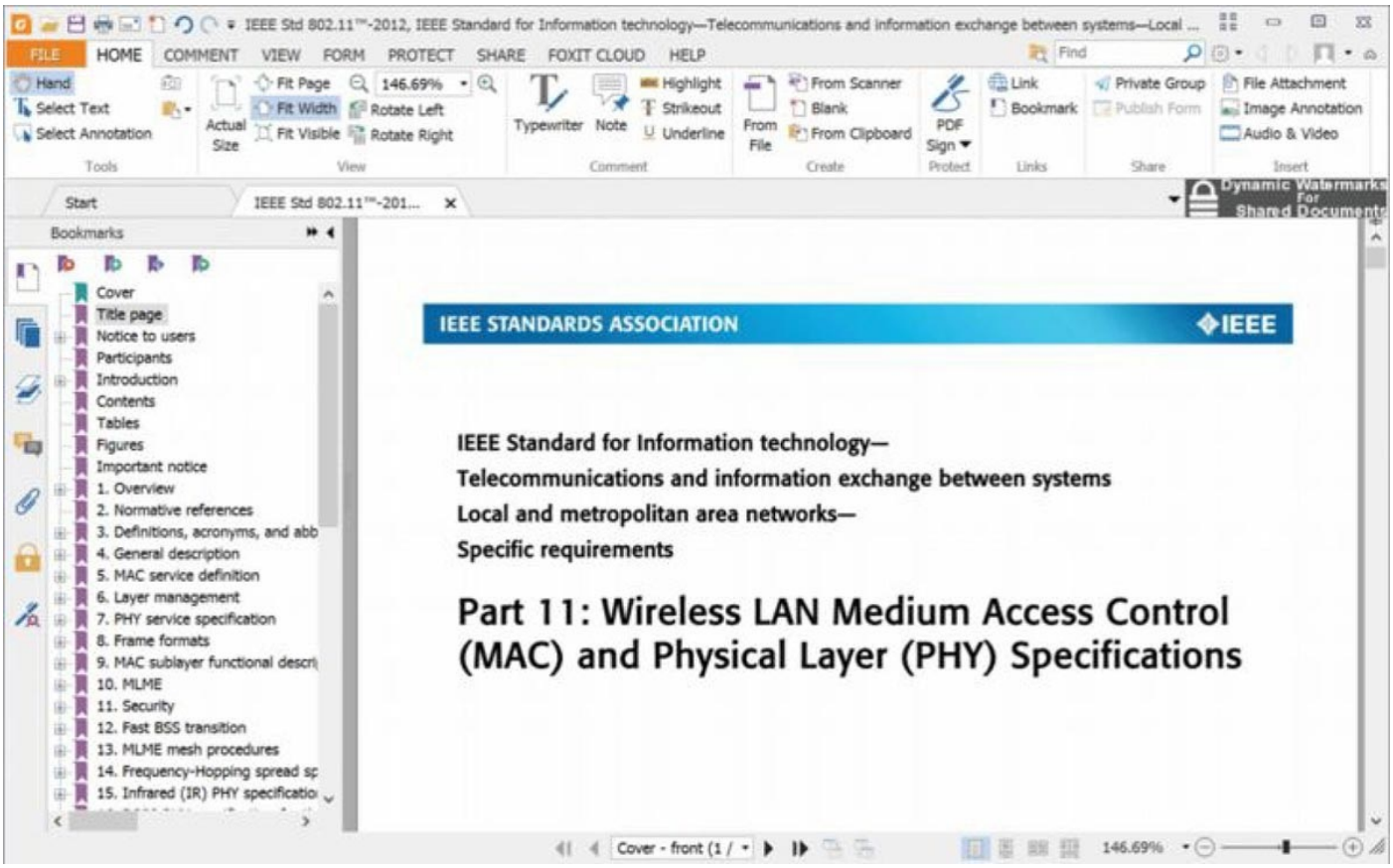
- *DBPSK*—Differential Binary Phase Shift Keying (shortened to BPSK at times)
- *QBPSK*—Quadrature Binary Phase Shift Keying (shortened to QPSK at times)
- *QAM*—Quadrature Amplitude Modulation (includes 16, 64 and 256 QAM)

Note: **The details of the modulations are not tested on the CWAP exam as the WLAN analyst cannot modify them, he or she can only analyze and optimize a network for use of them.**

Exercise 3

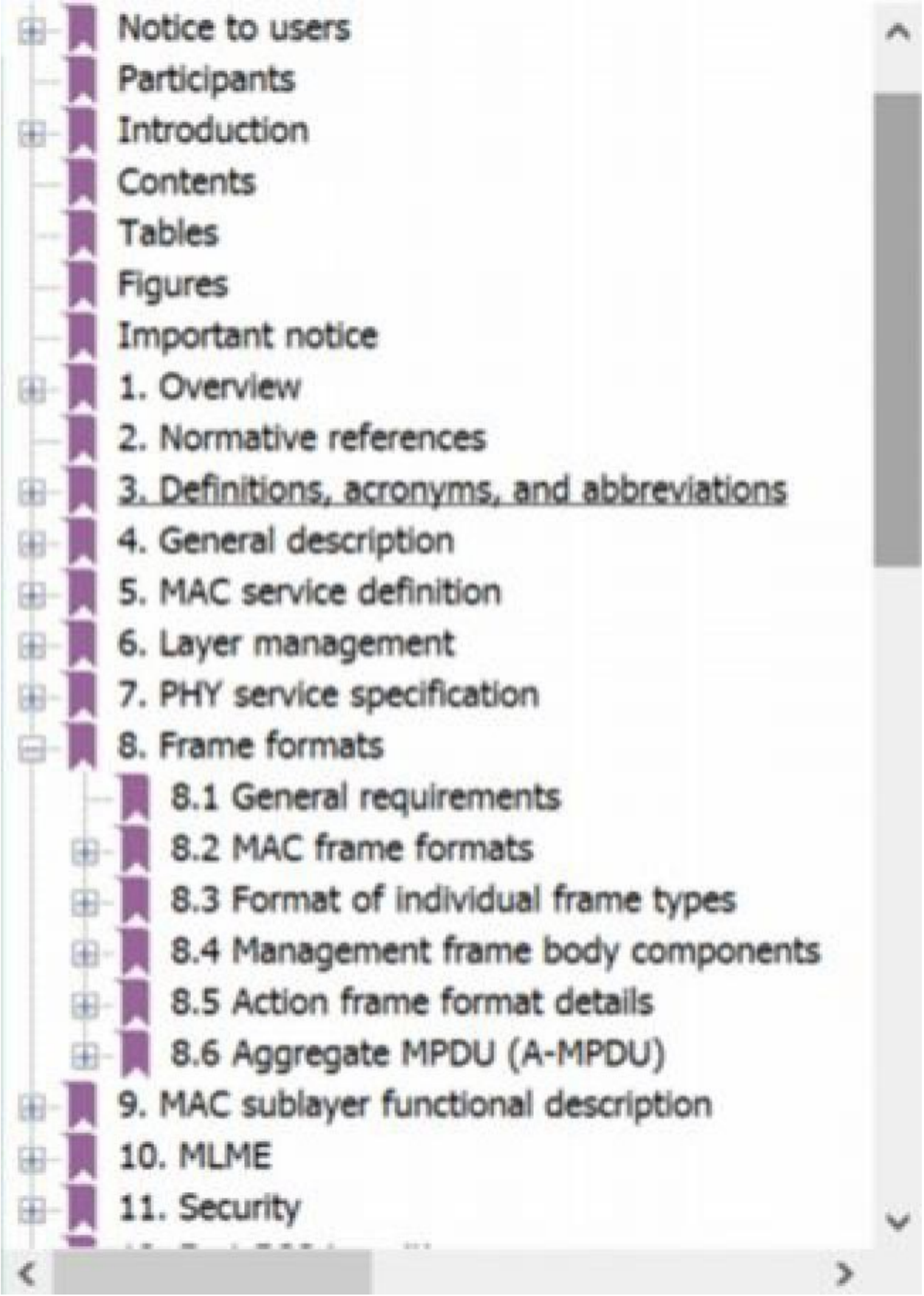
In this exercise, you will explore the 802.11-2012 standard and identify the frame definition sections of importance. If you wish to perform this exercise, you will need access to the PDF of the standard, which is available at goo.gl/wMLIxO. To view a video demonstration of this exercise, visit YouTube and search for “CWNPTV Exploring the 802.11-2012 Standard.”

1. Assuming you have downloaded the 802.11-2012 standard in PDF format, open it in a PDF viewer (such as FoxIt or Acrobat reader).



Graphic 3.1

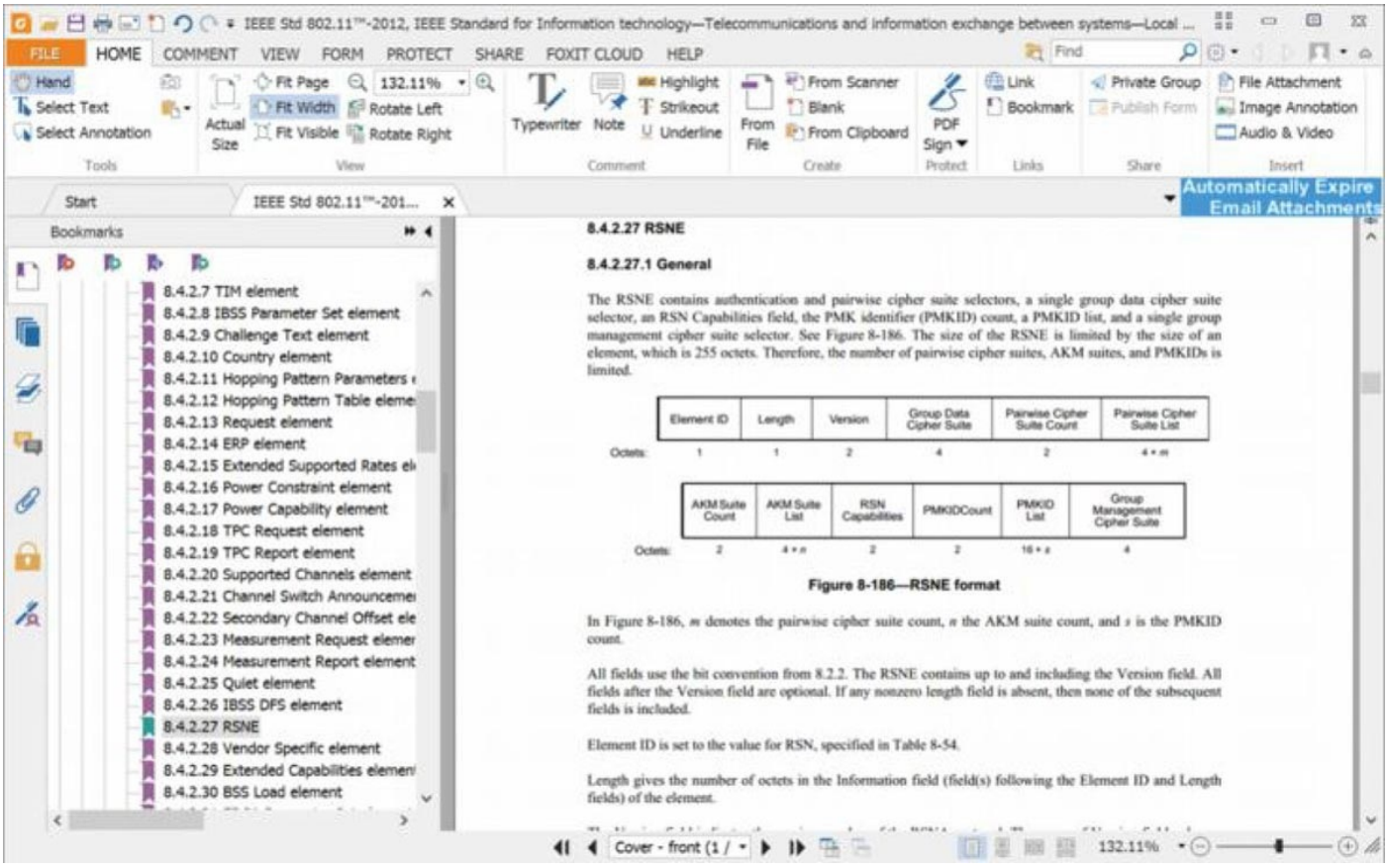
2. In the navigation pane to the left, expand the `8. Frame Formats` node to open Clause 8 of 802.11-2012.



Graphic 3.2

3. Browse the `MAC Frame Formats node` (8.2) to read about the general frame format and frame fields.
4. Browse the `Format of individual frame types` node (8.3) to view an overview of Management, Control and Data frames.

5. To see specific management frame details, expand the Management frame body components node. For example, view the RSNE entry as shown in Graphic 3.3.



Graphic 3.3

Chapter Summary

In this chapter, you learned about Ethernet and Wi-Fi frames and the PHY layer preamble and header. You explored the MAC frame types, including Management, Control, and Data Frames. You learned about the importance of framing, and the basic process used to encode data so that it can be understood when a shared protocol is used.

Review Questions

1. A frame is a collection of what?
    a. Upper layer data only
    b. Meaningful bits
    c. Lower layer data only
    d. Disorganized octets
2. When standards reference an octet, to what do they refer?
    a. Eight organized frames
    b. Eight bytes
    c. Eight bits
    d. Eight symbols
3. What field is typically at the end of a Layer 2 frame?
    a. FCS
    b. Preamble
    c. Header
    d. Destination address
4. In the general frame format for 802.11, when are all four address fields used?
    a. When four STAs or more are associated in a BSS
    b. Only in an IBSS
    c. When the addresses are too long to fit in three fields
    d. In a mesh network
5. In a CTS-to-self frame, to what is the DA field set?
    a. The transmitter’s address
    b. The BSSID
    c. The SSID
    d. A broadcast address
6. What frame type is attempted to be sent by an AP every 100 TUs by default?
    a. ACK
    b. Beacon
    c. PS-Poll
    d. Null Data

7. What frame type can be transmitted by a client STA to trigger power save buffer release from an AP?
    a. Null Data
    b. ACK
    c. Beacon
    d. SIFS
8. What frame is used to respond to an RTS?
    a. CTS
    b. Probe Response
    c. Reassociation Response
    d. EAPoL
9. What protocol is used between the AP and STA in a WPA2-Enterprise negotiation?
    a. RADIUS
    b. LDAP
    c. EAPoL
    d. RSTP
10. What protocol is used between a RADIUS server and an identity system?
    a. RADIUS
    b. EAPoL
    c. IGMP
    d. LDAP
11. In addition to PS-Poll and Null Data frames, what other frame can indicate to an AP that a STA is awake and ready to receive data?
    a. Data Frame
    b. Probe Request Frame
    c. Association Request Frame
    d. Reassociation Request Frame
12. What is a purpose of the RSN Information field in a beacon frame?
    a. To reveal the cipher suite supported in the BSS
    b. To reveal support for VHT parameters in the BSS
    c. To indicate the power management modes supported in the BSS
    d. To indicate the name of the BSS
13. In an Ethernet frame, for what fields does the FCS field provide integrity?

a. DA and SA only
b. Type and Data only
c. Data only
d. DA, SA, Type and Data

14. In what amendment was the HT Control field added to the 802.11 general frame format?
    a. 802.11a
    b. 802.11n
    c. 802.11ac
    d. 802.11e
15. What Management frame subtype is indicated by the bits 1011?
    a. Authentication
    b. Beacon
    c. Association
    d. Action
16. What bits define a frame as a Control frame?
    a. 00
    b. 01
    c. 10
    d. 11
17. When the To DS and From DS fields are both set to 1, what is indicated?
    a. A mesh network
    b. An IBSS network
    c. A standard BSS
    d. The frame is a broadcast frame
18. What may the Duration/ID field contain instead of the time required to transmit?
    a. The AID of the STA
    b. The MAC address of the STA
    c. The IPv4 address of the STA
    d. The IPv6 address of the STA
19. To what access category (AC) do the 802.1d UPs of 6 and 7 map?
    a. AC_VI
    b. AC_BE

c. AC_BK

d. AC_VO

20. What access category (AC) has the lowest aCWmax setting by default?

    a. AC_VO

    b. AC_VI

    c. AC_BE

    d. AC_BK

21. Which one of the following is not a management frame?

    a. RTS

    b. Beacon

    c. Probe Request

    d. Association

22. What filter can be used to remove beacon frames from the display in Wireshark?

    a. wlan.fc.type_subtype != 0x08

    b. wlan.fc.type_subtype == 0x08

    c. wlan.fc.type_subtype != 0x4

    d. wlan.fc.type_subtype == 0x4

23. Which one of the following is not a factor in determining the Duration value in an RTS frame?

    a. Data frame duration

    b. One ACK

    c. Three DIFS

    d. CTS duration

24. In addition to the Frame Control, RA, TA and FCS fields, what field is in a PS-Poll frame?

    a. AID

    b. DA

    c. HT Control

    d. Sequence

25. By default, how often are beacon frames transmitted by 802.11 APs?

    a. Every 100 TUs in all circumstances

    b. Every 100 TUs if the medium is clear

    c. Every 102 TUs in all circumstances

d. Every 102 TUs if the medium is clear

Review Question Answers

1. **B** is correct. A frame, in computer networking, is a collection of agreed upon meaningful bits.
2. **C** is correct. An octet is eight bits of information. An 8-bit byte is equivalent to one octet.
3. **A** is correct. The frame check sequence (FCS) or CRC is typically at the end of a frame. It is used to provide integrity checks upon reception.
4. **D** is correct. All four address fields are used in a mesh network.
5. **A** is correct. The DA address field of a CTS frame sent without an immediately preceding RTS frame (CTS-to-self) is the transmitting STAs address. For example, if the AP sends the CTS-to-self, it is the APs MAC address.
6. **B** is correct. The beacon frame is transmitted every 100 TUs assuming the medium is clear.
7. **A** is correct. A Null Data frame can be transmitted to indicate to the AP that the STA is awake and can receive any buffered frames.
8. **A** is correct. The response to an RTS frame is a CTS frame. The RTS/CTS exchange is used to clear the medium for transmission of data frames (or possible other frames) in an environment with high levels of frame retransmissions (retries).
9. **C** is correct. EAP over LAN (EAPoL) is used between the AP and the client STA for EAP authentication and the 4-way handshake.
10. **D** is correct. The lightweight directory access protocol (LDAP) is used between the RADIUS server (or another authentication server) and the identity system.
11. **A** is correct. A standard data frame can be transmitted from the STA to the AP to trigger a buffer dump. The data frame sets the PS bit to 0 to indicate that the STA is no longer in power save mode. After receiving all buffered data, the STA can set the bit back to 1 to enable power save mode again.
12. **A** is correct. The RSN Information field can reveal many security-related parameters of the BSS. One such parameter is the cipher suite supported in the BSS.
13. **D** is correct. The frame check sequence (FCS) field of the Ethernet frame provides integrity for the destination address, the source address, the type and the data fields.
14. **B** is correct. 802.11n introduced the high throughput (HT) PHY and the HT Control fields to the general frame format.
15. **B** is correct. The beacon frame is equal to 1011 in the subtype field.
16. **B** is correct. Control frames are indicated by 01 in the type field. Management frames are 00, and data frames are 10.
17. **A** is correct. Only a mesh network uses the value one in both the To DS and From

DS fields at the same time.

18. **A** is correct. The STA's association identifier (AID) may be in the Duration/ID field.
19. **D** is correct. The highest 802.1d priorities are 6 and 7. These priorities map to the access category (AC) of AC_VO for voice.
20. **A** is correct. AC_VO has the lowest aCWmax with a default of 7. This value may be changed by the administrator in enterprise systems, but it seldom is changed.
21. **A** is correct. Control frames are used to "control access to the medium" and the RTS frame is such a frame, therefore it is not a management frame.
22. **A** is correct. The filter "wlan.fc.type_subtype != 0x08" can be used to remove beacon frames from the Wireshark display. Remember, the == operator is used to display the matching packets and the != operator is used to hide the matching packets.
23. **C** is correct. Three SIFS are used to determine the Duration field value in an RTS frame, not three DIFS.
24. **A** is correct. Because a PS-Poll frame is used to indicate a wake state to the AP, it also includes the association identifier (AID) of the transmitting STA.
25. **B** is correct. The target beacon interval is 100 TUs, but that is the target. If the medium is not clear, the AP will send the beacon using standard contention. However, if a beacon is sent late, the next beacon will not wait another 100 TUs, but will get back on schedule, if possible.

Chapter 4:

WLAN Hardware

Objectives

3.1 Understand client devices and operations including radios, drivers, supplicants, and implementations.

3.2 Describe and discover access point (AP) options, configurations and behaviors, including internal and external antennas, Ethernet connections, power options, and management options.

3.3 Explain the functionality of WLAN controllers and managers including protocols used, installation locations, and supported data communication options.

3.4 Describe and implement WLAN analysis hardware for protocol analysis and spectrum analysis.

3.5 Describe and analyze wired infrastructure hardware including routers and switches, as well as servers and services.

WLAN hardware can be divided into four basic categories:

- Client Devices
- Infrastructure Devices
- Analysis Devices
- Supporting Devices (wired devices, services, and servers)

This chapter addresses all four categories. Understanding the hardware used on the network is the first step to being able to troubleshoot problems. Without this knowledge, you are shooting in the dark and unable to resolve most issues. We'll begin by discussing client device types. Some of this material is review from your CWNA studies, but new and important information has been included, as well.

Client Device Types and Functions

WLAN client devices play an extremely important role in your wireless network and come in many different form factors with a range of different features and capabilities. Choosing the right wireless network interface card (NIC) among the many options and understanding their features and capabilities is key. Choosing your devices wisely involves understanding the requirements of each client device such as operating system requirements and form factor specifications. This section provides some review material from CWNA and additional material important to the WLAN analyst.

Device Internals

Each WLAN client device is composed of a similar set of hardware components and software elements. The hardware components include chipsets for radio control and management, antennas for RF transmission and reception, and interfaces for connectivity to the device intended to communicate on the wireless network.

The form factor, whether it be integrated, Universal Serial Bus (USB) or Mini-PCIe, determines the interface to the communicating device (laptop, tablet, etc.). The chipset and antenna are points of differentiation. Chipsets provide the actual implementation of the 802.11 PHYs that are supported by the client device. For example, a chipset may support only the transmission of 2.4 GHz signals and support the DSSS, HR/DSSS, ERP and HT PHYs. Alternatively, a chipset may support both the 2.4 GHz signals and the 5 GHz signals, as well, which allows for support for the OFDM, HT, and VHT PHYs in addition to the PHYs operating in the 2.4 GHz band.

A device that supports both the 2.4 GHz and 5 GHz PHYs is often referenced as an 802.11a/b/g/n/ac adapter. The CWNP certifications and the industry refer to such a device as a dual-band device because it actually implements the 2.4 GHz and 5 GHz PHYs. Most of these devices cannot operate both bands at the same time, but must switch between them or operate on only one of them. Modern devices are either HT or VHT devices (whether single stream, 2 stream, 3 stream, and even some 4 stream). The HT and VHT

clients can only operate in one frequency band at a time, and many only support one frequency band. If a client supports both bands concurrently, like most modern enterprise APs, it means that the client actually has two NICs.

> **EXAM MOMENT:** Sadly, it is still not uncommon for 802.11n client to support only the 2.4 GHz band, which means that they are not as useful in enterprise deployments. In most enterprise deployments, the 5 GHz bands will be used since more 40 MHz bonded channels are available in these bands and far more 20 MHz channels are available. 802.11ac clients all support 5 GHz and most also support 2.4 GHz.

Client devices usually have built-in antennas, but some devices do also support the use of external antennas. By supporting external antennas, the vendor allows for the device to be used in very unique ways for testing and site surveying purposes. For example, the device can be set up with an external semi-directional antenna to compare communications quality as opposed to a dipole antenna.

An excellent way to learn about the capabilities of a client is to perform an FCC ID search when the FCC ID is visible. This ID may or may not be immediately visible. For example, laptops may have to be disassembled to view the FCC ID on the adapter. Many mobile phones and tablets list the FCC ID on the back of the case. Figure 4.1 shows the back of an iPhone 6 revealing the FCC ID. Figure 4.2 shows the FCC ID of a USB adapter from Edimax (model EW-7822UAC). The Edimax adapter ID is NDD9578221212. Exercise 4 steps you through searching for an FCC ID and viewing the related documents and photos. From this exercise, you can see that significant and useful information is provided to the WLAN analyst from the FCC ID search.

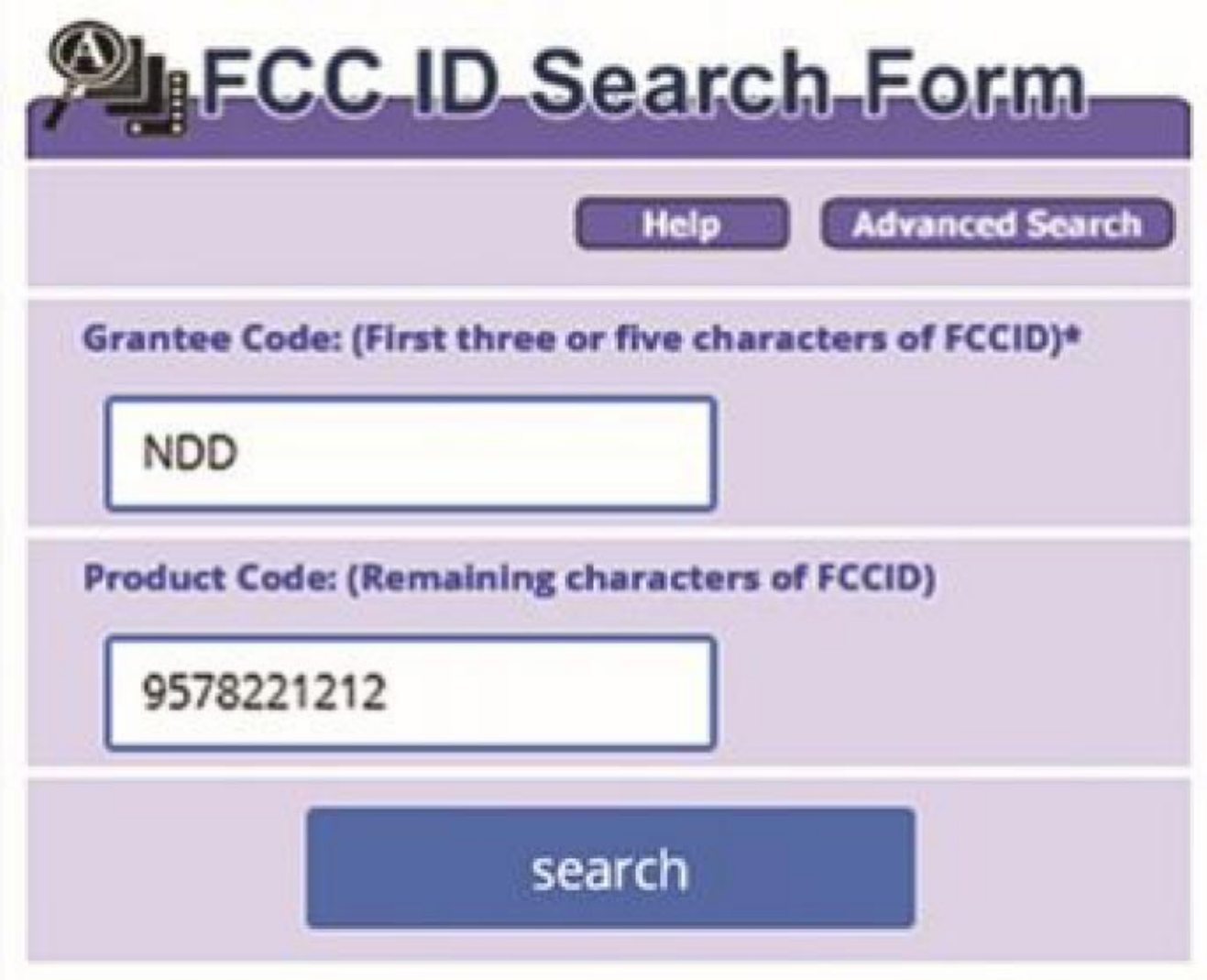
Figure 4.1: iPhone® 6 FCC ID

Figure 4.2: Edimax EW-7822UAC FCC ID

Exercise 4

In this exercise, you will perform an FCC ID search on the Edimax EW-7822UAC adapter. If you wish to perform this exercise, you will need an Internet connection and a Web browser. No other software is required. If you want to view a video demonstration of this exercise, visit YouTube.com and search for “CWNPTV Performing an FCC ID Search.”

1. To begin the FCC ID search, open a Web browser and navigate to: www.fcc.gov/general/fcc-id-search-page
2. In the search fields enter the FCC ID information as shown in Graphic 4.1 and click search.



Graphic 4.1

3. The search results show the available reports on the adapter. In some cases many reports will be available. Notice, in the right-most column, it indicates the band for which the report is targeted. For example, the first report in the list in Graphic 4.2 is for the 2.4 GHz band. One piece of valuable information revealed in an FCC report is the supported bands and channels of the adapter. Some vendors readily report this information on their websites and others do not. The FCC report will typically provide more in-depth information.

8 results were found that match the search criteria:
Grantee Code: NDD Product Code: 9578221212

Displaying records 1 through 8 of 8.

View Form	Display Exhibits	Display Grant	Display Correspondence	Applicant Name	Address	City	State	Country	Zip Code	FCC ID	Application Purpose	Final Action Date	Lower Frequency In MHz	Upper Frequency In MHz
	Detail Summary			Edimax Technology Co Ltd	No.3 , Wu-Chuan 3rd Road , Wu-Ku Industrial Park	.Taipei Hsien	N/A	Taiwan	N/A	NDD9578221212	Original Equipment	03/04/2013	2412.0	2462.0
	Detail Summary			Edimax Technology Co Ltd	No.3 , Wu-Chuan 3rd Road , Wu-Ku Industrial Park	.Taipei Hsien	N/A	Taiwan	N/A	NDD9578221212	Original Equipment	03/04/2013	2422.0	2452.0
	Detail Summary			Edimax Technology Co Ltd	No.3 , Wu-Chuan 3rd Road , Wu-Ku Industrial Park	.Taipei Hsien	N/A	Taiwan	N/A	NDD9578221212	Original Equipment	03/04/2013	5745.0	5825.0
	Detail Summary			Edimax Technology Co Ltd	No.3 , Wu-Chuan 3rd Road , Wu-Ku Industrial Park	.Taipei Hsien	N/A	Taiwan	N/A	NDD9578221212	Original Equipment	03/04/2013	5755.0	5795.0
	Detail Summary			Edimax Technology Co Ltd	No.3 , Wu-Chuan 3rd Road , Wu-Ku Industrial Park	.Taipei Hsien	N/A	Taiwan	N/A	NDD9578221212	Original Equipment	03/04/2013	5775.0	5775.0
	Detail Summary			Edimax Technology Co Ltd	No.3 , Wu-Chuan 3rd Road , Wu-Ku Industrial Park	.Taipei Hsien	N/A	Taiwan	N/A	NDD9578221212	Original Equipment	03/04/2013	5180.0	5240.0
	Detail Summary			Edimax Technology Co Ltd	No.3 , Wu-Chuan 3rd Road , Wu-Ku Industrial Park	.Taipei Hsien	N/A	Taiwan	N/A	NDD9578221212	Original Equipment	03/04/2013	5190.0	5230.0
	Detail Summary			Edimax Technology Co Ltd	No.3 , Wu-Chuan 3rd Road , Wu-Ku Industrial Park	.Taipei Hsien	N/A	Taiwan	N/A	NDD9578221212	Original Equipment	03/04/2013	5210.0	5210.0

Graphic 4.2

4. Click the Detail link for the first entry in the list.
5. In the resulting Exhibit List, click the link that reads Test Report (not Test Report

5G).

6. Browse through the Test Report and note the information it reveals about the adapter. For example, consider the table in Graphic 4.3 from the Test Report. Notice that it supports up to 2 spatial streams and note the output power (in dBm, decibel-to-milliwatts) supported by the adapter.

RF General Information						
Frequency Range (MHz)	IEEE Std. 802.11	Ch. Freq. (MHz)	Channel Number	Transmit Chains (N_{TX})	RF Output Power (dBm)	Co-location
2400-2483.5	b	2412-2462	1-11 [11]	1	24.50	N/A
2400-2483.5	g	2412-2462	1-11 [11]	1	20.88	N/A
2400-2483.5	n (HT20)	2412-2462	1-11 [11]	2	24.68	N/A
2400-2483.5	n (HT40)	2422-2452	3-9 [7]	2	22.78	N/A

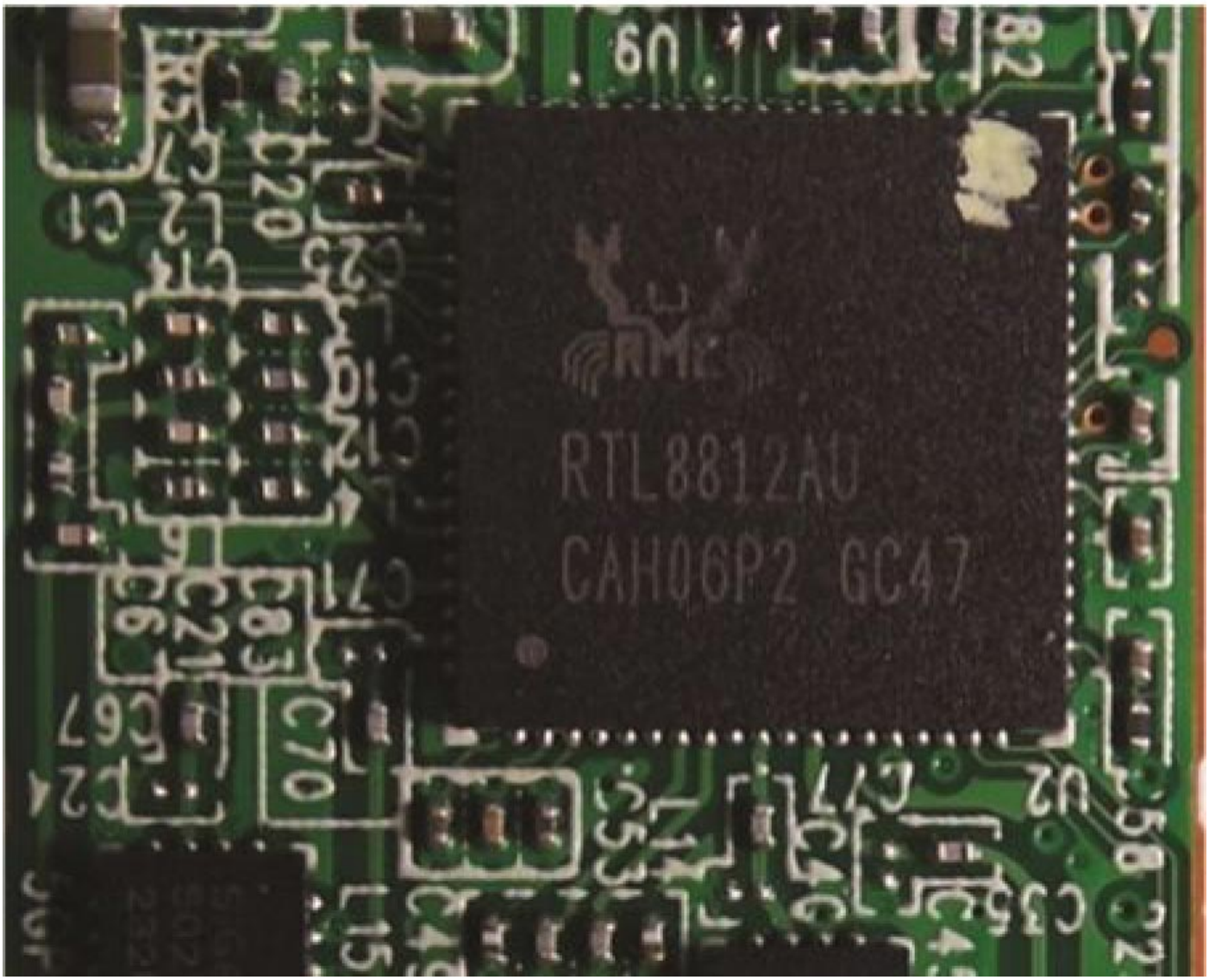
Note 1: RF output power specifies that Maximum Peak Conducted Output Power.
Note 2: 802.11b uses a combination of DSSS-DBPSK, DQPSK, CCK modulation.
Note 3: 802.11g/n uses a combination of OFDM-BPSK, QPSK, 16QAM, 64QAM modulation.
Note 4: Co-location, Co-location is generally defined as simultaneously transmitting (co-transmitting) antennas within 20 cm of each other. (i.e., EUT has simultaneously co-transmitting that operating 2.4GHz and 5GHz.)

Graphic 4.3

7. In addition to the Test Report, the internal photos show details of the antennas and chipsets. On the search results page, click the Internal Photos link (note that many FCC IDs will return multiple internal photo documents).

8. As you browser through the photos, notice the antenna placement and configuration. Also notice the chipset used as shown in Graphic 4.4. The Edimax adapter uses the RTL8812AU chipset. With this knowledge, you can determine compatibility with different operating systems and also determine the capabilities of the radio according to the chipset manufacturer. This happens to be a popular chipset in USB adapters and is, therefore, likely to be widely supported on different operating system platforms. A simple search on the chipset also reveals that it is a 2x2:2 radio configuration with support for 802.11a/b/g/n/ac in 2.4 GHz and 5 GHz.

802.11a/b/g/n/ac in 2.4 GHz and 5 GHz.



Graphic 4.4

9. Continue browsing the remaining documents in the report to see the information they reveal. Graphic 4.5 shows the final piece of information from this exercise, which is the 5 GHz channels supported and tested by the adapter revealed in the RF Exposure report. Note the lack of support for channels 52–144, a total of 16 channels unavailable, which is not uncommon in client devices. These devices simply avoid using the channels that may not be available due to radar-related regulations in a regulatory domain. The result is support for 9 20 MHz channels or 4 40 MHz channels without overlap.

IEEE 802.11 average power(dBm)				
Channel	Ant B	Ant A+B		
	802.11a	802.11n HT20/ VHT20	802.11n HT40/ VHT40	802.11n VHT80
36	11.5	14		
38			13.5	
40	11.5	14		
42				15
44	12.5	14.5		
46			14.5	
48	13	15		
149	12.5	12		
151			13.5	
153	12.5	12		
155				18
157	13	12		
159			13	
161	13	12		
165	13	12.5		

Graphic 4.5

As you can see from Exercise 4, the FCC ID search can be very revealing and helpful in identifying the capabilities of a WLAN client adapter. As an analyst, you should take advantage of this resource when troubleshooting client connectivity issues. Much of the information needed in relation to the client capabilities can be discovered through the documentation in the FCC database.

Device Form Factors

Over the years, many form factors have been used for WLAN adapters, including Compact Flash (CF), Secure Digital (SD), USB, PCI, PCI-express, and mini-PCI or mini-PCI-express. This section will review the USB and PCI-class adapters as they are more common in today's devices.

USB adapters have become very common for both laptop and desktop computers. They come in two primary implementation models. The first is a dongle-type adapter that plugs directly into the USB port, and the second is a device that connects to the USB port through a connector cable. Figure 4.3 shows the Edimax USB 3 adapter researched in Exercise 4.

The primary advantage of USB devices is that they are fairly universal (after all, the term USB stands for Universal Serial Bus). Saying that the USB device is universal is a reference to the fact that USB devices can be used with desktops, laptops, tablet PCs (with the appropriate interface), and any other device that supports the USB interface and provides proper drivers for the WLAN NIC.

Figure 4.3: Edimax USB EW-7822UAC Adapter

Compact Flash cards are frequently called CF cards. They are small form factor WLAN devices and were most frequently used in handheld computers and specialty equipment. CF cards can be connected directly to the supporting device or they can be connected through a PCMCIA adapter card when used in laptop or desktop computers. The CF cards do have a tendency to drain the battery power of handheld devices very quickly. This is particularly true of the IEEE 802.11g devices. CF cards are not common today, and are hard to find for newer PHYs such as 802.11n (HT) and 802.11ac (VHT). Figure 4.4 shows an older Linksys 802.11g CF card.

Figure 4.4: Linksys 802.11g CF Card

The Secure Digital IO, or SD, cards are very similar to the CF cards. They were small form factor WLAN-client devices that were used in portable and desktop computers. Devices could be purchased that supported both flash storage and Wi-Fi connectivity in one unit. This multifunction capability made them attractive to users of portable devices, so organizations should be careful to specify the appropriate use of such devices, if still in use, in the acceptable use policies. Figure 4.5 shows an SD WLAN-client device. Like CF devices, SD adapters are harder to find in 802.11n and 802.11ac implementations.

Support for similar features as those found in PC Cards can be found in USB, CF, and SD devices. It is more difficult to find support for advanced technologies in the CF and SD form factors than for the USB form factor. For example, the Linksys WCF54g pictured in Figure 4.4 only supports WEP encryption and does not support WPA or WPA2 for enhanced security. For this reason, these older devices should be removed from the network as soon as possible. USB devices are usually capable of supporting all modern security standards and capabilities, but it is important that you ensure the specific device you are selecting does support the security specifications that you demand.

Figure 4.5: SD WLAN NIC

Installation of a USB WLAN NIC is very similar to that of PC Cards. Install the drivers and/or software, and then connect the USB device or cable to an available USB port. In some situations, you may be required to connect the USB device before you perform the driver installation.

The CF and SD cards will require the installation of appropriate driver software on the device in which they are being installed, or you may be forced to purchase an adapter stated as supported by the device. This installation may require synchronization with a laptop or desktop computer before or after the insertion of the WLAN device. Check the vendor installation manuals to be certain.

The WLAN NICs covered up to this point are all devices that are connected through external connectors to laptops, desktops, and handheld devices. PCI and Mini-PCI adapters differ in that they are installed internally. If you choose not to use a USB device for a desktop computer, you will most likely select an internal WLAN card. This means you will be using a PCI or PCI Express (PCIe) device. Figure 4.6 shows a PCIe adapter from ASUS supporting 802.11ac and dual-band operation. You must ensure that your desktop computer supports the interface specification of the WLAN NIC (either PCI or PCIe).

Mini-PCI cards are used in laptop computers as well as some WLAN infrastructure devices. Those used in WLAN infrastructure devices are used to provide supports for differing PHYs while sharing consistent software and logic processing. Many newer laptops support the Mini-PCI specification; however, not all laptops provide easy access to the Mini-PCI port. For this reason, some network administrators choose to use PC Cards, ExpressCards, or USB devices when upgrading the WLAN support in these laptops. The internal Mini-PCI card is usually just disabled in such situations. Figure 4.7 shows a PCIe Mini-PCI card.

Figure 4.6: ASUS PCIe Desktop Adapter

Figure 4.7: Mini-PCI Adapter

In addition to the Mini-PCI, you should be aware of the Mini-PCIe or Mini-PCI express. Most laptops built after 2005 or 2006 use Mini-PCIe and can support Mini-PCIe upgrades. The major advantage of Mini-PCIe over Mini-PCI is that Mini-PCIe is half the size. This benefit allows for more Mini-PCIe devices in a laptop or for smaller laptops.

Wireless NICs in the PCI and Mini-PCI form factors are available for most PHYs specified in the 802.11 standards, including the HT PHY (802.11n) and VHT PHY (802.11ac). In most cases, the devices are backwards compatible with PHYs that operate in the same frequency band. For example, HT-based PCI devices that operate in the 5 GHz bands will usually be backwards compatible with the OFDM or 802.11a devices.

PCI and Mini-PCI cards may support all of the 802.11 standards as well as proprietary features. Because of the internal connection to the system bus, power is usually not a problem, and the overall capabilities are only limited by the chipset used.

The difference between PCI/Mini-PCI cards and the other devices mentioned in this chapter is that the PCI/Mini-PCI cards will require screwdrivers and other tools as you remove cases and covers to access the device. Desktops will require the removal of the computer case cover in order to access the PCI or PCIe card, and laptops will require the removal of one or more covers to access the Mini-PCI or Mini-PCIe card. In extreme situations with poorly designed laptop cases, you may even be required to remove the keyboard in order to access the area where the card is installed.

Note: **I am not always a big fan of internal wireless NICs for desktop computers because they usually require that the antenna be under the desk or smashed back against a cubicle wall, which may inhibit the ability to receive a consistent and strong signal. Just make sure your device gets a sufficient signal before implementing it in hundreds of desktops. A USB device with a USB extension cable may actually be preferred.**

The final part of the client puzzle is the vendor specifications (spec) sheet. The spec sheet should reveal important information, including:

- Output power
- Frequency bands supported
- PHYs supported
- Ideal temperature for operation
- Size and weight

Figure 4.8 shows the spec sheet for the 802.11ac adapter from Edimax referenced earlier in this chapter.

SPECIFICATIONS

HARDWARE	STANDARDS	FREQUENC BAND
•1 x USB 3.0 Type A •1 x Hardware WPS Button •1 x Link/Activity LED •2 x Antennas	•2.4GHz: IEEE 802.11b, 802.11g, 802.11n •5GHz: IEEE 802.11ac (Draft), 802.11a, 802.11n	•2.4000 - 2.4835GHz (subject to local regulations) •5.150 - 5.825GHz (subject to local regulations)
OUTPUT POWER	**INSTALLATION**	**OPERATING RANGE**
•2.4GHz 11b (11Mbps): 16dBm±1.5dBm 11g (54Mbps): 14dBm±1.5dBm 11n (20MHz, MCS7): 14dBm±1.5dBm 11n (40MHz, MCS7): 12dBm±1.5dBm •5GHz 11a (54Mbps): 12dBm±1.5dBm 11n (20MHz, MCS7): 10dBm±1.5dBm 11n (40MHz, MCS7): 10dBm±1.5dBm 11ac (80MHz, MCS7): 9.5dBm±1.5dBm	•Multi-language easy setup wizard •Hardware WPS button for easy wireless connections	•11a: 6/9/12/24/36/48/54Mbps •11b: 1/2/5.5/11Mbps •11g: 6/9/12/24/36/48/54Mbps •11n (20MHz): MCS0-15 (up to 144Mbps) •11n (40MHz): MCS0-15 (up to 300Mbps) •11ac (40MHz): MCS0-9 (up to 400Mbps) •11ac (80MHz): MCS0-9 (up to 867Mbps)
LED	**SECURITY**	**TEMPERATURE & HUMIDITY**
•Link/Activity	•WEP 64/128-bit, WPA, WPA2, 802.1x •Hardware & Software WPS Configuration	•Max. 95% (non-condensing) •32 - 104°F (0 - 40°C)
WEIGHT	**DIMENSIONS**	**CERTIFICATIONS**
•23g	•18 (H) x 27 (W) x 87.1 (L) mm	•CE/FCC

Figure 4.8: Edimax EW-7822UAC Spec Sheet

Some vendors will provide more information useful to the analyst, such as the receive

sensitivity of the adapter and other specs that help the analyst understand its behaviors and abilities.

In order to use an adapter with a given operating system, the device driver must be available. Some adapters are provided with driver support for Windows and no support for other operating systems. However, in many cases, once the chipset is identified you can locate adapter drivers for use with other unsupported operating systems. If you take this action you will not be able to gain support from the adapter vendor, but you may be able to utilize the device to meet your needs. Figure 4.9 shows the driver download section for the Edimax EW-7822UAC USB 3.0 adapter. Notice that support exists for Windows, MAC and Linux.

Driver

Version	Note	Date	File Type	File Size	
v1.0.1.6	Support OS:MAC 10.4/10.5/10.6/10.7/10.8 Languages:English	2013-09-24	ZIP	19.11 MB	
v1.0.1.6	EW-7822UAC_Linux_driver_v1.0.1.6 (Linux)	2013-09-24	ZIP		
v1.0.1.7	Support OS:MAC 10.9/10.10 Languages:English	2015-02-06	ZIP	2.48 MB	
v1.0.2.4	Support OS:Windows XP/Vista/7/8/8.1 Languages:English	2014-10-07	ZIP	34.76 MB	

Figure 4.9: Edimax Driver Download

Access Points

While the client adapters are important for troubleshooting certain scenarios, the access points (APs) are involved in nearly all problem scenarios. This fact does not mean that the APs cause the problems. It means only that they are central to network operations. Therefore, understanding APs, their options, configuration, and behaviors is important. This section provides a review of APs and details important to the WLAN analyst.

APs are the most frequently installed infrastructure (non-client) devices. They provide access to the WLAN and usually bridge to a wired LAN. They also provide a point of access to the WLAN and get their name from this functionality. Each BSS has one, and only one, AP. When multiple APs work together to form a larger network throughout which clients may roam, they form an ESS. While each BSS has only one AP, a single AP may provide more than one BSS. Hopefully, this all sounds very familiar from CWNA study.

In most cases, an AP will provide connectivity to a wired LAN or WAN for wireless client stations (STAs); however, this does not have to be the case. APs are often used at construction sites to form controlled and secure networks that are entirely wireless (with the exception of the power cords connected to the APs) as just one example of the use of APs where direct access to wired networks is not the intent.

Autonomous Access Points are APs that contain the software for complete management of

the WLAN processes within themselves. Autonomous APs were the only kind of APs in early WLANs, prior to the development of the lightweight AP. Lightweight Access Points contain limited software and depend on centralized WLAN switches or controllers to provide the remaining functionality. No complete standard for implementing lightweight versus autonomous APs exists, and the way in which they are implemented varies from vendor to vendor. Autonomous APs are sometimes called fat or thick APs, and lightweight APs are also called access ports (as opposed to access points) or thin APs. Figure 4.10 shows a network implementation using autonomous APs, and Figure 4.11 shows the use of lightweight APs. As you can see in these two images, the implementation will not look any different in the physical world, but at the logical level things are very different. In the lightweight APs, much less of the work is happening at the AP, and much more of the work is happening at the controller or switch.

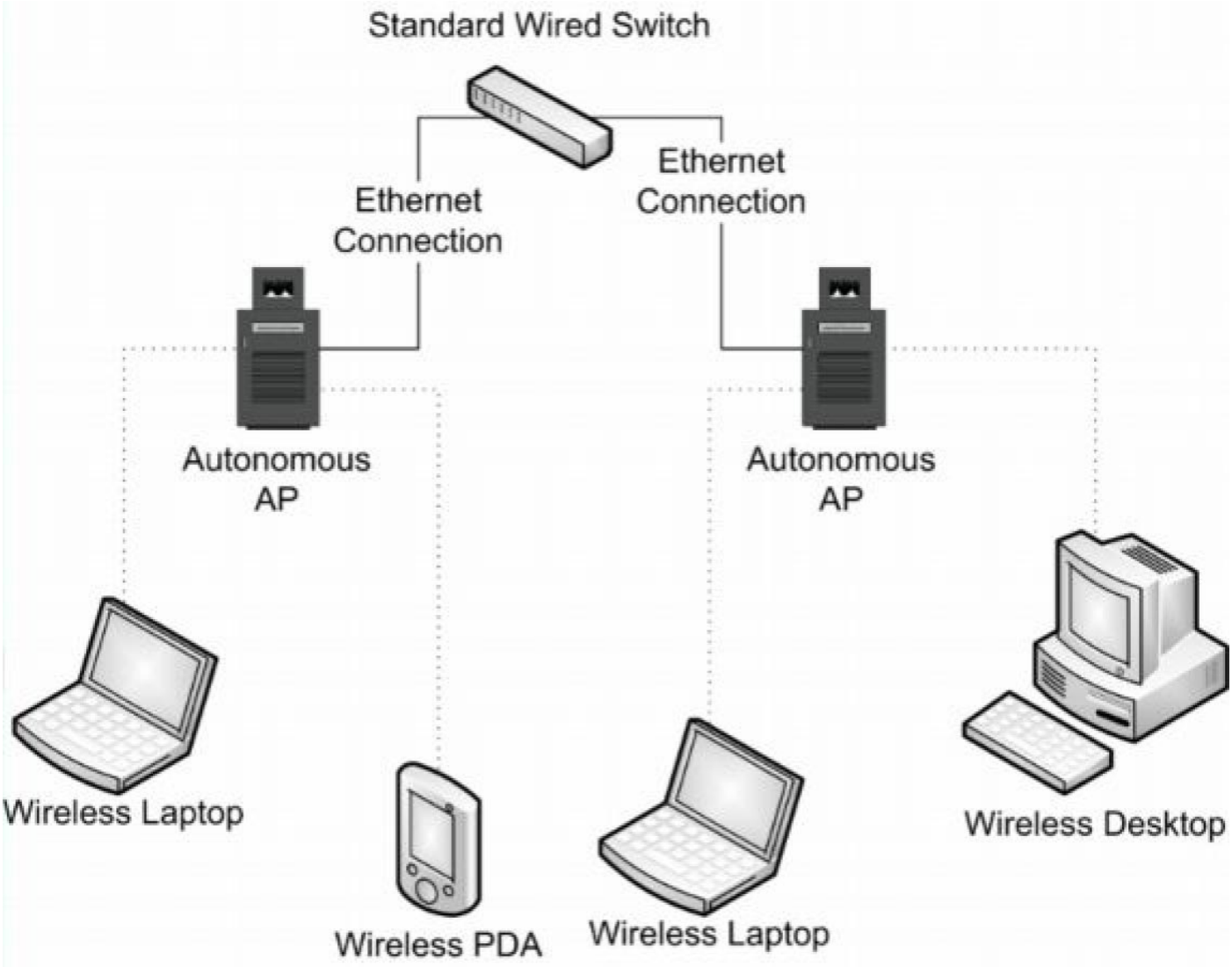


Figure 4.10: Autonomous AP Implementation

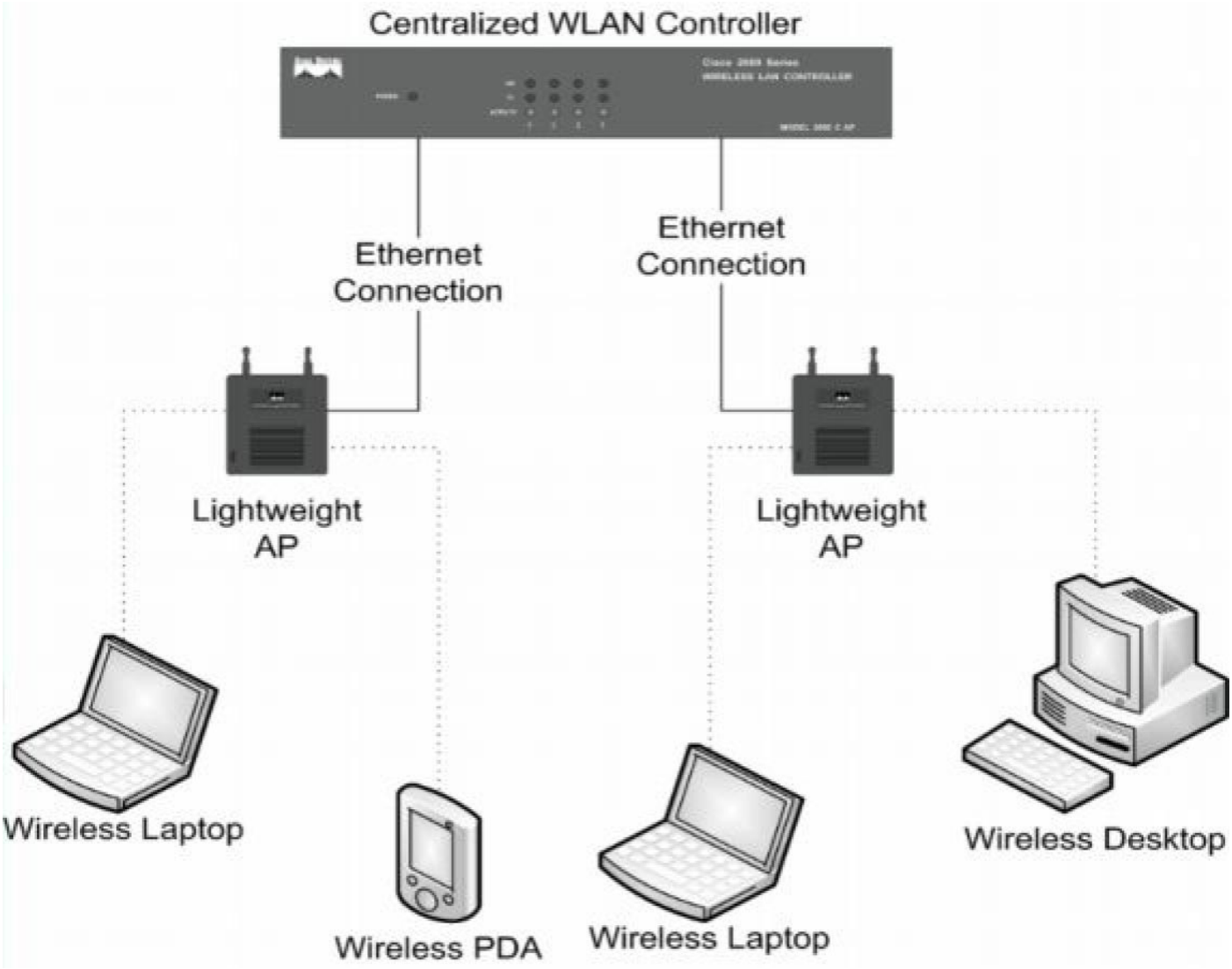


Figure 4.11: Lightweight AP implementation

Some APs can act as either an autonomous or lightweight AP depending on the configuration determined by the WLAN administrator. When used as an autonomous AP, all the AP software features are enabled. When used as a lightweight AP (or access port), many of the AP software features are disabled or simply controlled by the centralized WLAN switch or controller.

When lightweight APs are brought online (powered up and connected to the WLAN controller through their Ethernet port), they are automatically configured by the WLAN controller or switch. The automatic configuration may include the installation or update of firmware (internal software used to run and manage the AP). Many vendors ship their lightweight APs with no or incomplete firmware loaded, and the firmware is actually installed when it first connects to the WLAN controller.

When an AP is converted to become an access port or lightweight AP, features may include:

- Automatic updates of firmware files
- Support for multiple ESSs and BSSs with BSSIDs in a single AP
- Support for multiple VLANs
- Centralized management of all APs

- Automatic management of QoS features
- More encryption types than those supported by the AP internals

Autonomous APs that are converted to lightweight APs may also lose capabilities such as access via the serial port, support for wireless bridging and repeater operational modes, and other vendor-specific features. Generally speaking, you gain centralized management, and you may lose unique features of the autonomous AP. However, since conversion of autonomous APs to lightweight APs is usually only supported when the same vendor APs are used as the WLAN controller being implemented, few features are available in the fat AP that are not in the WLAN controller's software.

An AP is basically a small computer that includes one or more radios and usually one Ethernet port. Inside the AP is a processor and memory. In fact, one of the big differences between enterprise-class APs and those designed for small office/home office (SOHO) implementations is the processing power and the amount of memory available in the AP. Many WLAN administrators are surprised when they first learn that many APs either run a flavor of Linux or can run Linux through flash updates. It is important to remember that you may lose support from the device vendor if you flash the device with an operating system that is not supplied by the vendor. For example, firmware is floating around on the Internet that converts the older and very popular Linksys WRT-54g WLAN routers into more enterprise-like devices with advanced features usually only provided in WLAN controller/AP combination installs. These features include VPN endpoint support for client connections, more powerful filtering, and centralized management and control. Again, if a WLAN administrator chooses to install such a firmware update, she will likely lose all support from the hardware vendor.

Note: **A moment of realization can occur when you realize that a Raspberry Pi, which is a small form factor computing board, running Linux with a USB Wi-Fi adapter can be made to function as an AP. This should reveal the reality that APs are nothing more than computers with specialized hardware (granted, better quality hardware than that found in most USB adapters) for 802.11 processing.**

APs, both autonomous and lightweight, come in many shapes and sizes. Some have built-in antennas, and others use external antennas. They come in round enclosures, rectangular housings, and in other shapes. Some are designed for mounting on walls or ceilings and others are designed to be placed on desktops or shelves.

APs come with common features and require various configuration processes. The following sections document each of these important factors. First, the common features will be covered. It is important to note that while these features are common, they are not available in all APs. Second, I will walk you through the basic installation and configuration of an AP.

Common Features

By common features I mean features that are commonly seen in APs but not necessarily present on all APs. Some APs will have all of the features listed here and more, while others may lack one or more of the listed features. Features that will be covered include:

- Operational Modes
- IEEE Standards Support
- Fixed or Detachable Antennas
- Filtering
- Removable and Replaceable Radio Cards
- Variable Output Power
- Ethernet and Other Wired Connectivity
- Power over Ethernet Support
- Security Capabilities
- Management Capabilities
- Mounting Options

Operational Modes

The 802.11 standard defines an AP only as a STA that provides access to the distribution services via the wireless medium for associated STAs. It does not define the three common operational modes that are found in APs. These modes (root, bridge and repeater) are specific implementations of a WLAN STA for varied purposes, and in some cases, they may be proprietary in function rather than derived from an IEEE standard. For example, in bridge mode an AP is implementing a network functionality that is not directly stipulated in the 802.11 standard. Technically speaking, bridge mode is just a point-to-point (PtP) or point-to-multi-point (PtMP) connection constrained to the devices configured. Root mode is the closest to the 802.11 standard, and many APs meet the 802.11 standard exactly when running in root mode.

The first and default mode offered by most APs is root mode. An AP operating in root mode provides wireless clients with access to the WLAN and usually a wired network. Root mode is the default mode of operation for all WLAN devices sold as APs. Some WLAN bridges are not much more than APs that come with the operating mode set to bridge mode, and they are nothing more than a standard AP operating in bridge mode. However, others are designed with ruggedized cases and more geared for outdoor-specific installation. Full-function WLAN bridges will implement a complete 802.1D bridging feature set. When APs operate in root mode, they may still communicate with each other, but the communications are not related to bridging. In root mode, inter-AP communications are usually related to the coordination of STA roaming. Figure 4.12 shows a typical installation of an AP in root mode.

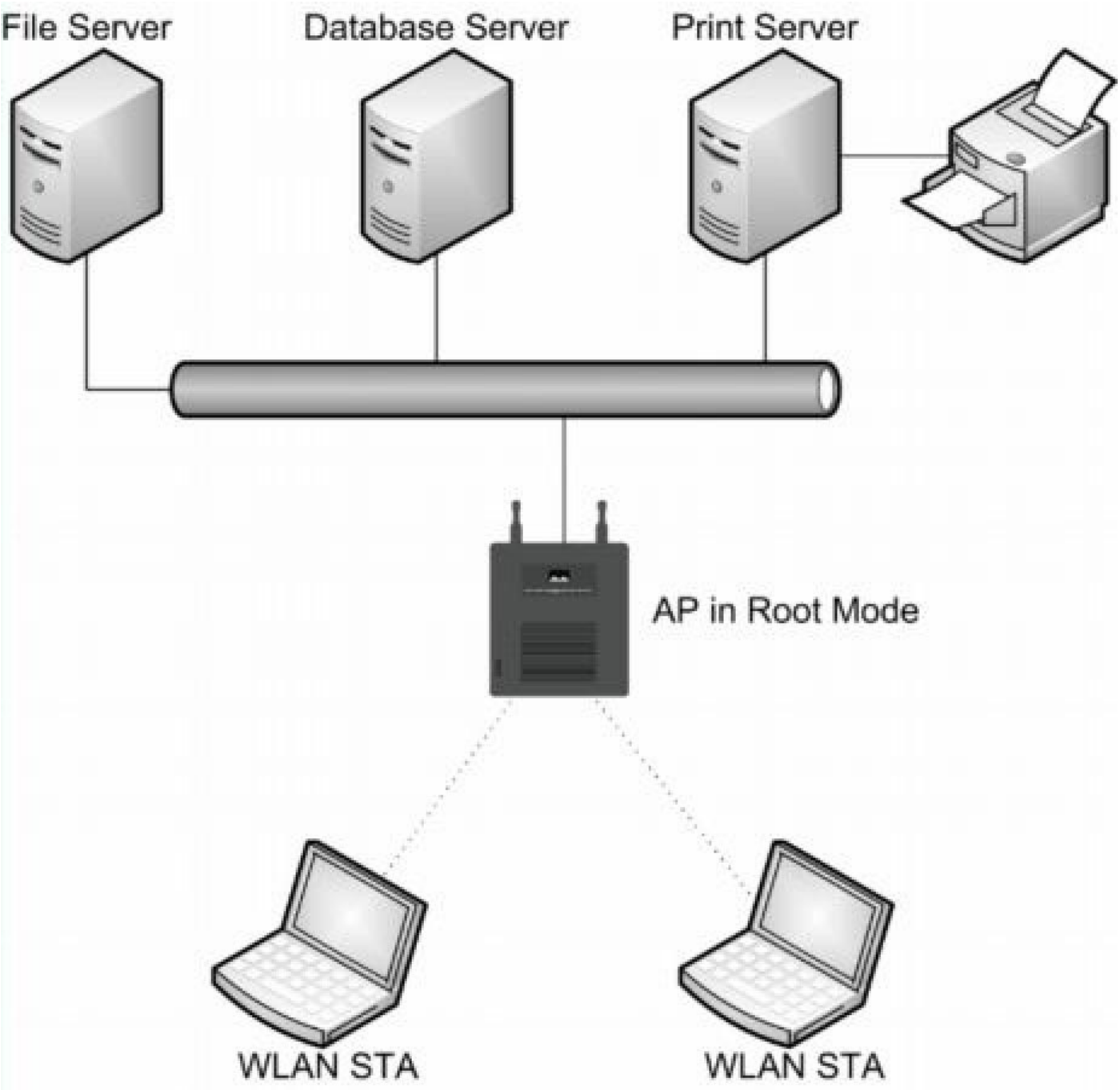


Figure 4.12: AP Implemented in Root Mode

Bridge mode is used to create a link between two access points. When only two APs are used, a PtP link is created. When more than two APs are involved, a set of PtMP links is created. In a bridge mode implementation, the APs involved usually associate only with each other and do not accept client STA associations. Exceptions to this exist, but it is not the normal implementation since it would reduce the throughput available for the bridge link connection. Figure 4.13 shows a typical installation of a set of APs in a point-to-point bridge mode implementation.

Figure 4.13 shows an implementation of bridge mode that reveals one possible scenario where this option may be beneficial. The AP in the Administration building is associated with the AP in the Research building. The two otherwise disconnected LANs are merged into one via the WLAN bridge link created using the bridge mode of the APs.

The final mode, repeater mode, is used to extend the range of a WLAN beyond its normal usable boundaries. The repeater AP acts as the AP for clients that would otherwise be out

of range of the distant AP operating in root mode. Where a root AP is the connection point for many clients and is a client to no other APs, the AP in repeater mode is a client to the AP in root mode while also accepting connections from client stations itself.

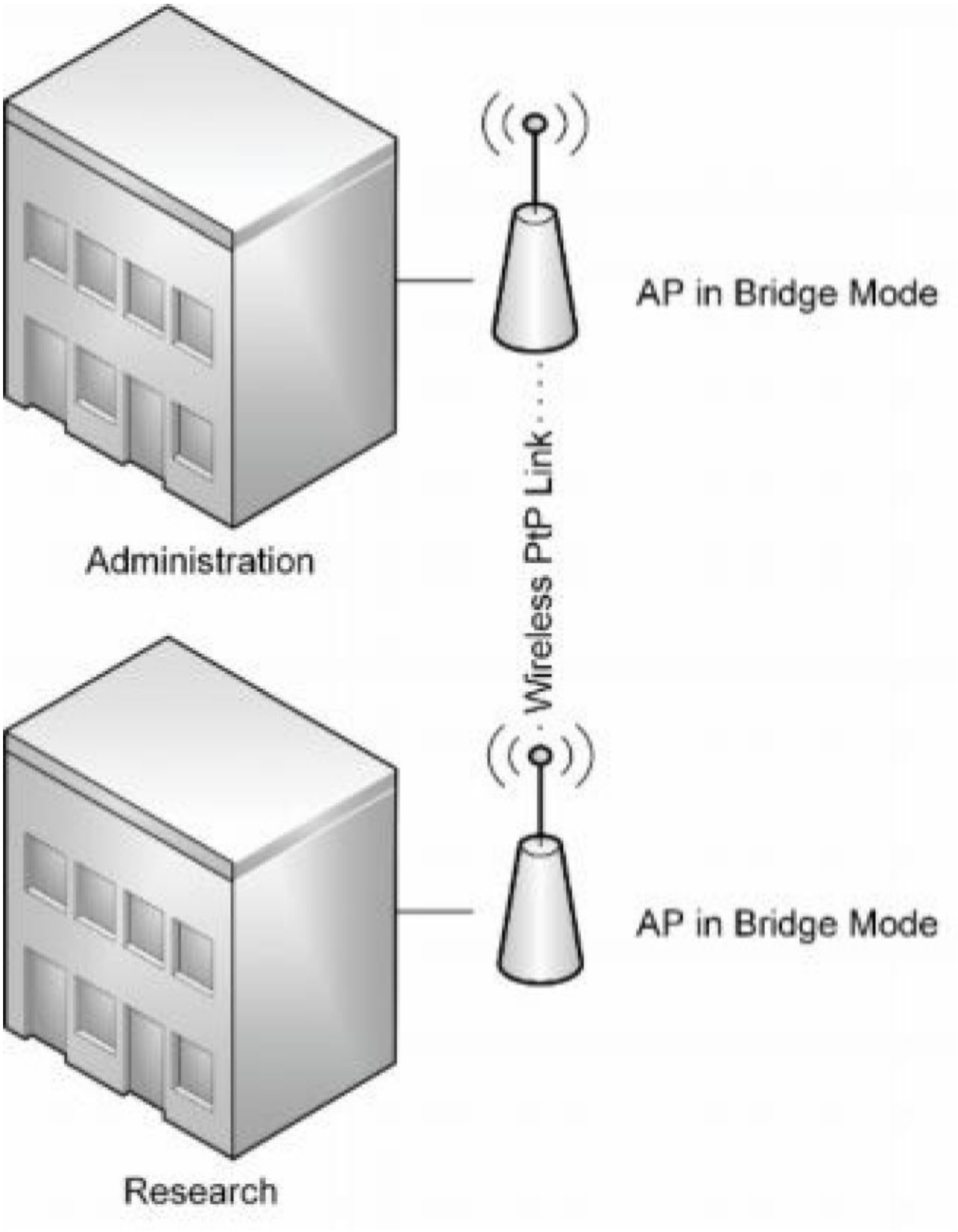


Figure 4.13: APs Implemented in Bridge Mode

Repeater mode in a WLAN AP should not be confused with the functionality of an Ethernet repeater. Ethernet repeaters regenerate the received signal in order to allow it to travel farther than it would otherwise travel. They do not decapsulate and encapsulate data as a WLAN repeater will. The AP running in repeater mode will decapsulate the data

frames received from the clients and encapsulate them for transmission to the root mode AP. In other words, the WLAN AP in repeater mode will receive data from the WLAN clients associated with it, and then retransmit that data to the root mode AP with which it is associated. Figure 4.14 shows an AP operating in repeater mode to provide access to remote clients.

Keep in mind that an AP operating in repeater mode must be able to communicate with the clients associated with it as well as the root mode AP with which it is associated. Because of this, the repeater mode AP will usually have to implement a Basic Service Area (BSA) that overlaps with the BSA of the root mode AP by at least 50 percent. This reduces the overall coverage area that may be provided if each AP were operating in root mode and forming an ESS; however, Ethernet connectivity is not always available to provide for the preferred implementation and repeater mode may be used in these scenarios.

Note: **In addition to the automatic loss of 50 percent throughput, consider that a repeater enlarges the physical size of the collision domain and may introduce reductions in throughput much larger than 50 percent. Mesh solutions should be used instead, when available.**

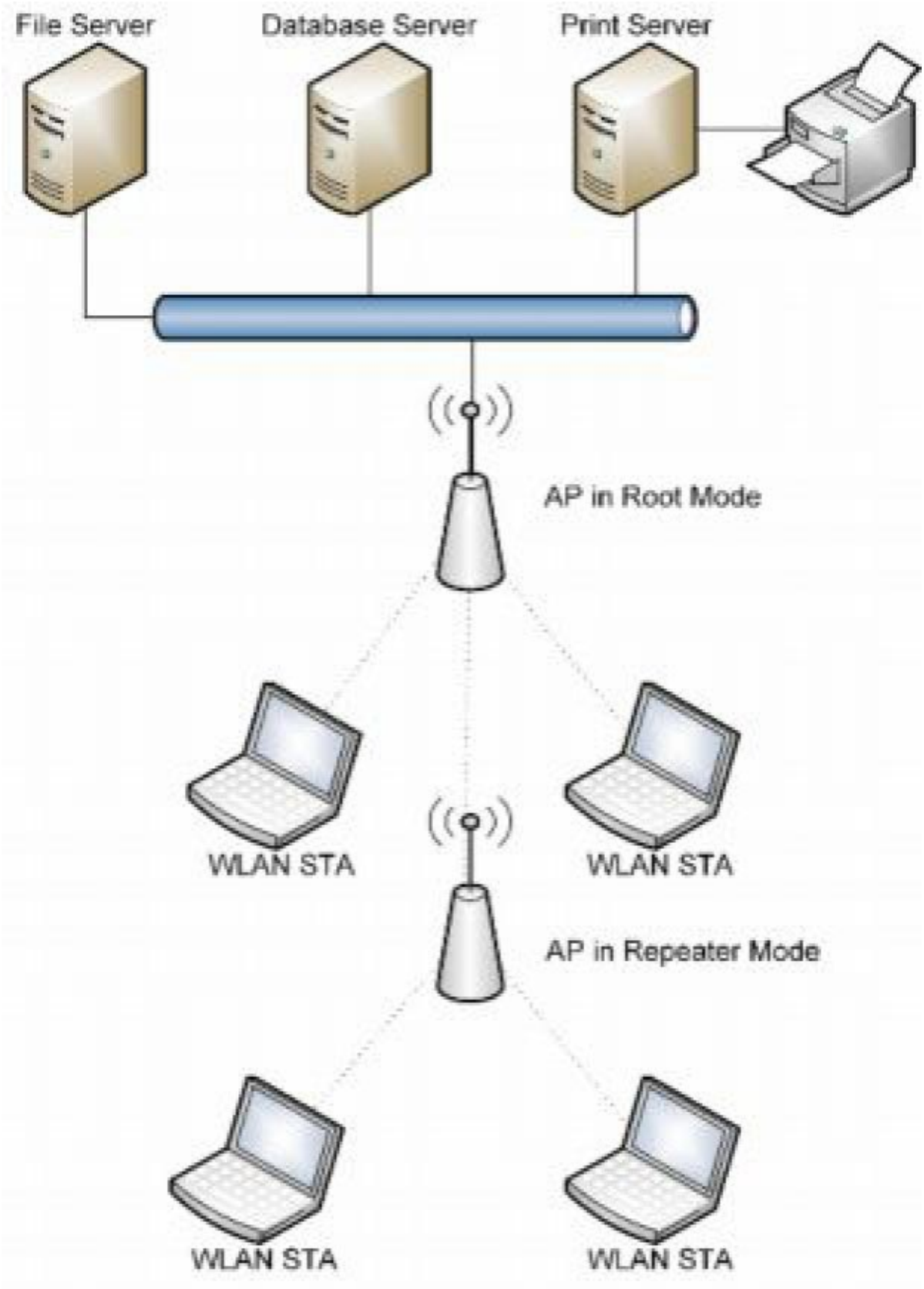


Figure 4.14: AP in Repeater Mode

IEEE Standards Support

APs on the market today support a wide range of 802.11 amendments, but it is difficult to find hardware that supports some of the older PHYs such as FHSS. Most equipment supports ERP, HR/DSSS, DSSS, OFDM, and HT. The newest APs also support VHT. Remember that a device that implements the 802.11g amendment (ERP) will almost always support backward compatibility, which means it must support DSSS and

HR/DSSS. Additionally, a device that implements the 802.11n amendment (HT) in the 5 GHz band will support backward compatibility with 802.11a (OFDM). Of course, HT devices in the 2.4 GHz band will support backward compatibility with ERP, which results in backward compatibility with HR/DSSS and DSSS. The good news for networks containing mostly newer clients is that most APs allow you to disable backward compatibility, as well, but this can be dangerous as you are often surprised by the client devices that enter the BSS.

Vendors usually report this standards support as 802.11ac, 802.11n, 802.11g, 802.11b, 802.11, or 802.11a. Many devices are said to be 802.11b/g devices, for example. This simply means that the devices implement the ERP PHY, which is capable of communicating with HR/DSSS PHY devices, as well. If a device is said to be 802.11a/b/g/n compatible, it means it has support for 802.11n with backward compatibility in both the 2.4 GHz and 5 GHz unlicensed bands.

In addition to the PHYs that are supported, you should consider the standards-based security features that you may require. Some APs support 802.11i (Robust Security Networks (RSNs)) and some do not. The vast majority of devices likely to be used in business wireless settings on the market today support RSN security. Some still support only WEP encryption if they are very old, but thankfully these devices are becoming scarce. Most modern APs will support both WPA and WPA2 with pre-shared keys (PSK), and all enterprise devices will support WPA and WPA2 Enterprise, which utilizes a RADIUS authentication server.

Another standards-based feature to consider is Quality of Service (QoS). If you need support for QoS extensions, you should ensure that the AP has support for 802.11e (EDCA) or the Wireless Multimedia (WMM) certification by the Wi-Fi Alliance. These QoS features will be very important if you intend to support Voice over WLAN or video conference over the WLAN.

Newer APs tend to support the newer IEEE standards while also supporting older standards. One of the benefits of a newer VHT PHY-based device that is dual-band is that it can communicate at the 54 Mbps data rate with other OFDM PHY devices, and it can also communicate at the 11 Mbps data rate with older HR/DSSS PHY devices, assuming it is a dual-band AP. Of course, the protection mechanism kicks in whenever an HR/DSSS, ERP or OFDM PHY device is associated with the VHT AP. This protection mechanism means that the AP will transmit a frame that can be understood by the older machine(s) before transmitting the frame that can only be understood by the VHT machine(s). The first frame is used to cause a backoff timer to kick in on the older machines so they will not interfere during the VHT frame transmission. Protection mechanisms reduce overall throughput as compared to a pure VHT or HT network. The lesson of the story is simple: one older device associated to your AP will cause the entire BSS to slow down to some extent—possibly by as much as 50 percent depending on the number of devices and the specific PHY that the older devices support.

In addition to the benefit of backward compatibility with the older PHYs, newer devices are able to support more data rates than older devices do. As the data rate changes it does not necessarily drop by half at a single step like an old HR/DSSS device does when it goes from 11 Mbps to 5.5 Mbps in one step.

Finally, APs may not support use in every regulatory domain. You should be sure to verify that the APs you are purchasing are authorized for utilization within your regulatory domain. IEEE 802.11h is the specified support for European nations and 802.11j is the specified support for the regulatory domain of Japan. For more specific information regarding your regulatory domain, check with the regulatory organization in your country or region.

Fixed or Detachable Antennas

Many enterprise-class APs support detachable antennas. Some SOHO APs may also support detachable antennas. Detachable antennas are becoming less common with the release of 802.11n and 802.11ac devices designed for indoor use, as internal antennas generally work fine for indoor coverage and capacity. That is not to say that they do not exist, it’s just less common since the antennas must be configured appropriately for the MIMO technology to function properly. Detachable antennas are beneficial from at least two perspectives: the ability to change the physical location of the antenna and the option to use a different antenna type.

The ability to move the physical location of the antenna to a different location than that of the AP is a valuable one. You can use RF cabling to relocate the antenna to a place that is more practical for the transmission and reception of RF signals, while locating the AP itself closer to power outlets if needed. The second benefit is that of replacing the antenna with a different antenna type. You may want to provide coverage down long narrow corridors (patch or panel antennas), or you may want to provide coverage in an area horizontally with as little RF energy propagating upward and downward as possible (higher gain omni antennas). Whatever the motivation, a detachable antenna provides you with the capability to better control how the RF energy is radiated from the antenna, and therefore, how the AP provides coverage in the BSA. Figure 4.15 shows an AP with a detachable antenna.

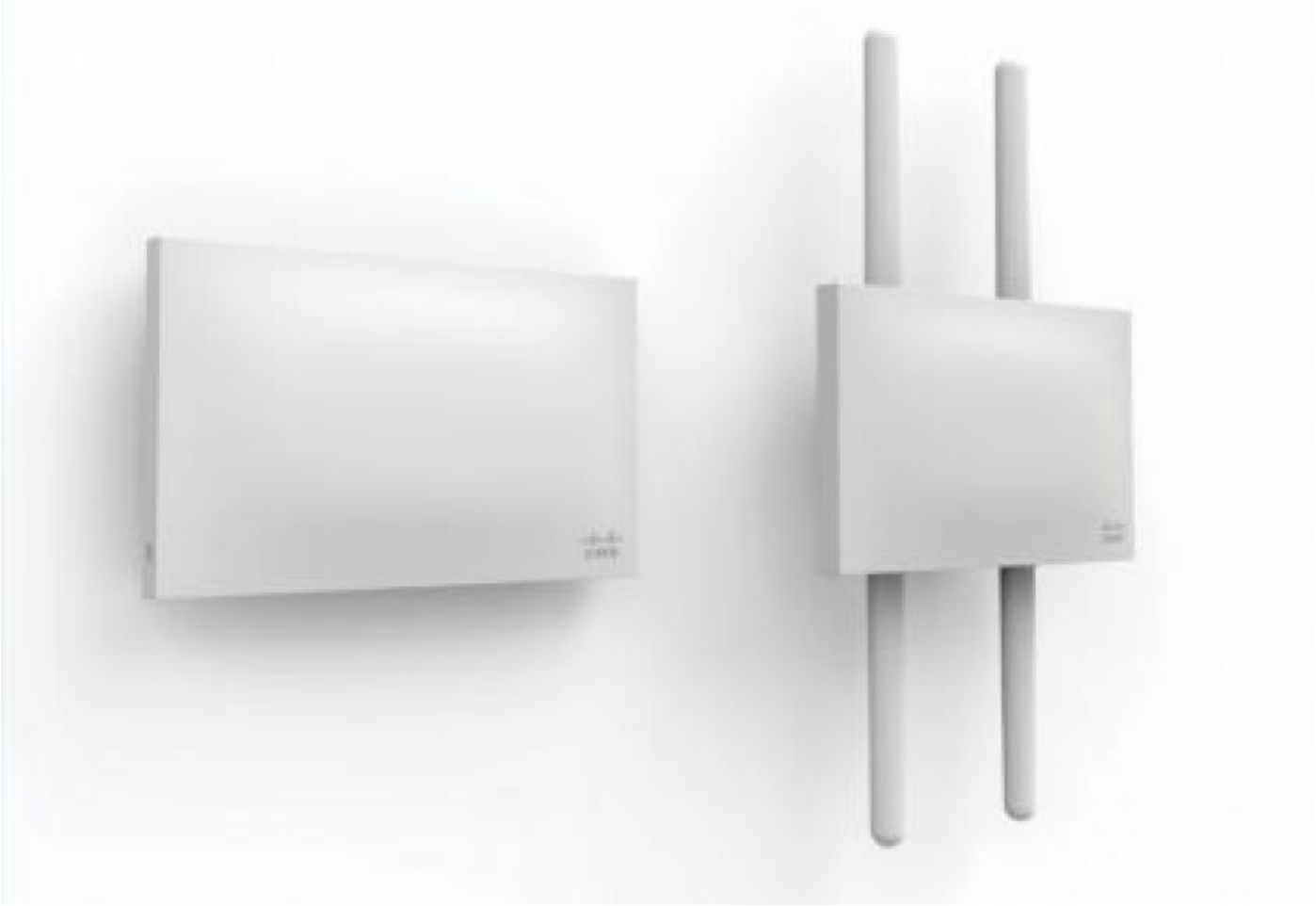


Figure 4.15: Cisco Meraki 802.11ac APs, One with External Antennas

Filtering

Most APs offer two kinds of filtering at a minimum. The first kind is MAC address filtering while the second is protocol filtering. Filtering functionality provides the WLAN administrator with the capability to limit which STA frames can pass through the AP based on the hardware configuration of the STA (MAC address) or the protocol being used, such as HTTP.

MAC filtering has often been referenced as a security solution, but it should not be thought of as such. It may be useful from the perspective of making it harder to accidentally associate with the wrong AP, but MAC filtering should not be considered as a viable security solution in WLANs. This is because MAC spoofing is easy to do and basic instructions are available on the Internet. The only common value seen from MAC filtering today is its use in specific association limitation scenarios. For example, a training center near my home office uses laptop computers in the training rooms. They do not want the laptop computers to be moved from room-to-room, but instead want them to stay in designated rooms. The simple solution was to use MAC filtering in the AP in each room. Each room's AP contains the MAC addresses of the laptops that are supposed to be in that room. The AP's output power is throttled back to reduce the coverage area provided. Now, if someone takes a laptop from the designated room to another room, the laptop will have to associate with an AP with a very weak signal in the remote room. Throughput suffers and, in most cases, the laptops cannot connect in such scenarios because the rooms are far enough apart. Again, if this were being done as a security solution, it would be a very bad idea. Any moderately skilled cracker can spoof a MAC

address very quickly. Therefore, it cannot be emphasized enough that MAC filtering should not be considered a security solution.

> **EXAM MOMENT:** MAC filtering may be useful for some management scenarios, but it simply adds unnecessary processing overhead in the AP or controller when it is implemented as an assumed security solution. WPA2-Personal or Enterprise should be used instead.

Protocol filtering can be used to disallow specific protocols or only allow specific protocols. This feature usually allows for filtering of both the frames arriving through the radio and through the Ethernet port. You may also filter only the radio-side (wireless) frames or only the wired frames, depending on the AP and vendor. Some APs can filter out frames based on the actual file extensions the user or machine is trying to access on the Internet. For example, if the user attempts to access a WMV file and the WLAN administrator has chosen not to allow access to such streaming media for performance reasons, the AP can disallow such requests. Most APs can blindly block all HTTP requests or FTP requests and other such Internet protocols, as well.

An additional kind of filtering, though less common, is that of wireless STA to wireless STA filtering. Some APs will allow you to create Virtual APs (VAPs) within one physical AP. You can then determine if wireless STAs associated with one VAP can communicate with wireless STAs associated with another VAP (inter-VAP filtering). You can also determine if wireless STAs can communicate with other wireless STAs associated with the same AP (intra-VAP filtering). Finally, you can disallow all client-to-client communications and only allow the STAs to use the AP for access to the wired medium. This type of filtering can be useful when you want one physical AP to service public and private clients. The public clients may have limited access to the network, and therefore to the private clients. The private clients may have normal access to the network. In this way, one AP effectively provides access to both internal users and public guests.

Removable and Replaceable Radio Cards

Some APs are designed to support only one PHY while others are designed to allow for multiple radios, and therefore multiple PHYs. These multiple radio APs are usually called dual radio or dual-band APs because one radio is needed for the 5 GHz PHYs and another is needed for the 2.4 GHz PHYs (though some APs can support two 5 GHz radios instead).

Some APs provide for replaceable radio cards or upgradeable modules. This allows you to upgrade the device for future standards by upgrading the firmware or operating system and the radio cards or modules. Figure 4.16 shows the modularity of Cisco 3600 series APs. These APs are shipped as 802.11n APs, but support an 802.11ac module for upgrades.

Figure 4.16: Cisco 3600 Series AP with 802.11ac Module

Many APs support replacement radios through the use of adapter WLAN NICs. In these cases, the replacement radio cards usually have to be purchased from the vendor that created the AP. This is due to the limited cards supported by the software running within the AP. Few of these APs are in production today.

Variable Output Power

Variable output power provides the WLAN administrator with the capability of sizing cells more accurately. Remember, this should not be considered a security solution by itself because a remote client with a powerful WLAN card and the right antenna can often still pick up the signal of the WLAN and also transmit data to the WLAN. However, as an RF management philosophy, cell sizing makes a lot of sense.

As an example, consider a facility with the need for four different WLANs (for security reasons or otherwise) that must coexist in a fairly small space. Throughput is not a paramount concern since the users of the WLAN perform minimal data transfers, though these data transfers happen several times per hour. Figure 4.17 shows a simplified floor plan of this facility. In order to implement the four distinct WLAN BSAs (cells), APs can be installed in areas A and D that use antennas that direct the majority of the RF energy inward. These antennas could be mounted on the walls near areas B and C and facing away from them. In areas B and C, APs could be installed centrally to the areas using standard omnidirectional antennas. These APs could have their output power settings lowered to ensure that there is minimal overlap into areas that are not intended for coverage by these APs.

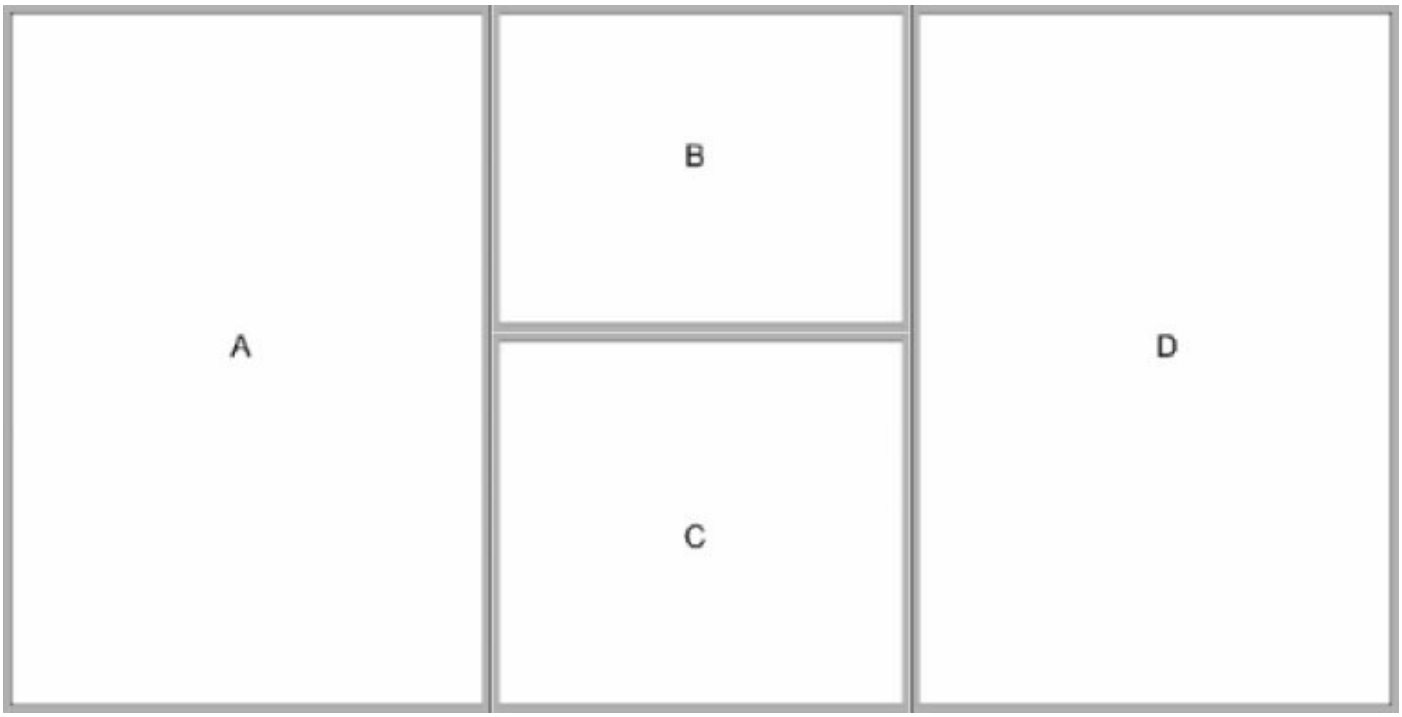


Figure 4.17: Simplified Floor Plan needing Four Distinct Cells

Of course, a scenario like this can be implemented to provide unique configuration parameters for each BSA; however, you must remember that this type of cell size reduction does not in itself equal security, but it would help in RF spectrum management in small areas that need different types of WLAN access such as that depicted here.

Some APs provide variable output power management based on percentages, while others are based on actual output power levels. For example, an AP may allow you to specify that the output power be 25, 50, or 100 mW. Other APs may only allow you to state that the output power should be at 25, 50, or 100 percent. These are just examples, but it is important to know what you're looking for when you enter an AP configuration interface. Figure 4.18 shows the variable output power management (Transmission Power) interface for a Cisco RRM implementation. You can see that this device provides numeric management of the output power, and Cisco documentation would have to be analyzed to determine the actual meaning of the settings.

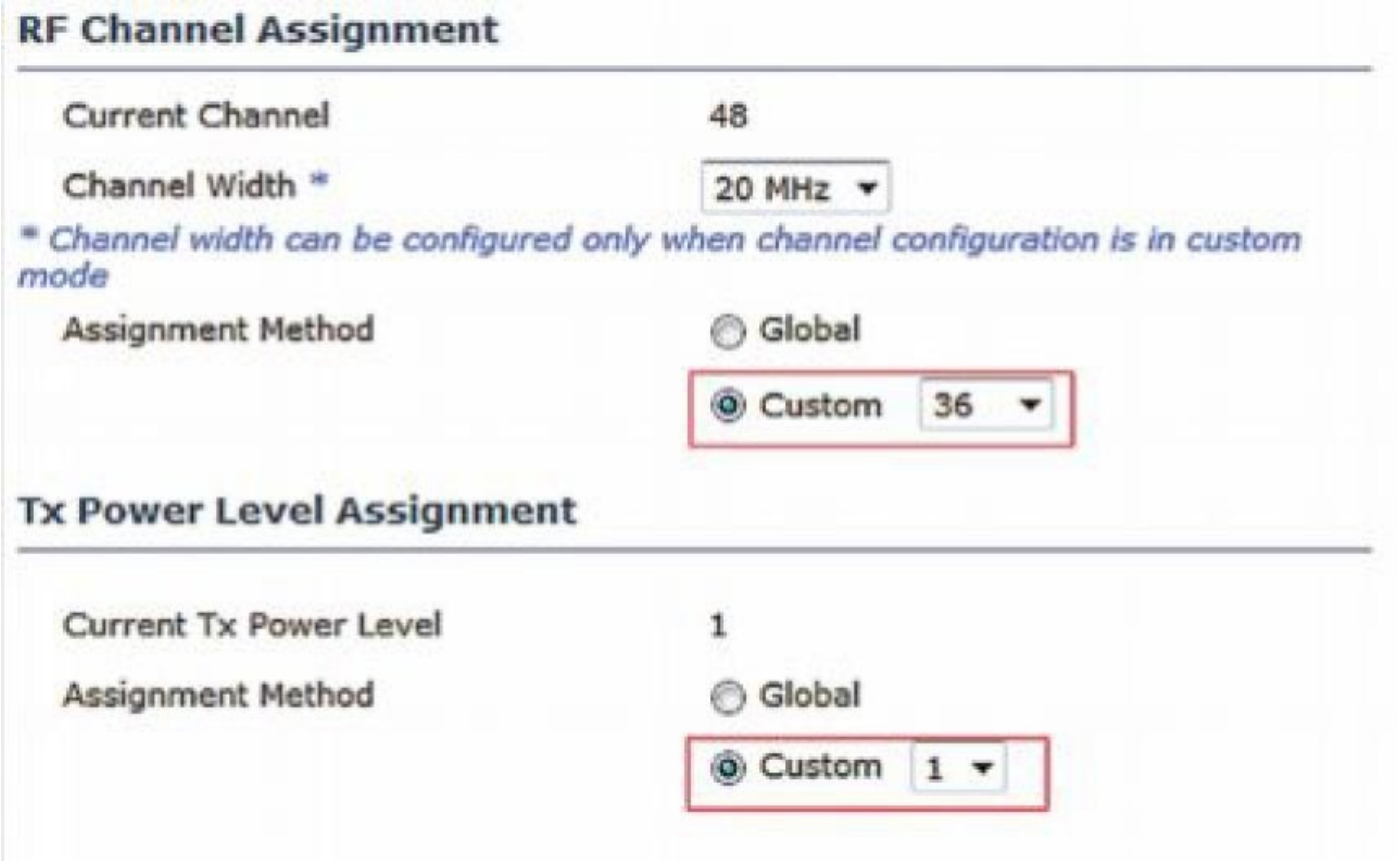


Figure 4.18: Cisco RRM Output Power Settings

Ethernet and Other Wired Connectivity

Unless an AP is providing WLAN services and access to a wireless-only LAN, the AP must have some interface through which it can connect to a wired LAN. In most APs this will be an Ethernet connection. Depending on the generation and model of the AP, it may support only 10 Mbps Ethernet, but this is rare today. Newer models should support 100 Mbps (802.11a/g and some 802.11n) and even Gigabit Ethernet (802.11n and 802.11ac). With an OFDM, ERP, or HT PHY you should ensure that the AP provides at least a 100 Mbps Ethernet connection. This way the wired side can keep up with the wireless side. If the device supports a 54 Mbps PHY (which will likely give up to 26 Mbps data throughput) and a 10 Mbps Ethernet connection, the wired side will likely fail to keep up with the wireless side, and it could give the illusion of poor wireless performance. In multi-radio APs and 3-stream HT APs and VHT APs, you will want an access point with a Gigabit Ethernet port. Of course, the switch to which the AP is connected must also support Gigabit rates, and you may have to analyze other links in the chain from the AP to the common service providers users will be accessing. This is where data flow analysis can benefit you in your planning of the WLAN.

> **EXAM MOMENT:** All 802.11n and newer APs should have at least 1 Gbps Ethernet ports. If they do not, they will be unable to keep up with the potential demands of the wireless network clients.

It is also important to remember management overhead that will be incurred on the wired side of the AP. Most centralized management systems, whether in a WLAN controller or in a computer-based application, will perform their management through the Ethernet connection. This prevents the management activity from interfering with wireless activity; however, it may also utilize measurable portions of the Ethernet connection, which may be

enough to warrant the use of multiple gigabit Ethernet ports in newer APs. However, such management overhead is typically less than 1 Mbps and should not result in major problems. The more likely driver for multiple gigabit Ethernet ports is a dual-radio 802.11ac 3x3:3 or greater AP.

In addition to standard CAT5 or CAT6 cabling, rare APs may support 100Base-FC fiber connections. Since fiber is rated for longer cable runs, it may provide a solution to a scenario where the AP needs to be located more than 100 meters (the limit of CAT5) from the switch port. Of course, this means the switch must support fiber as well as the AP. Such APs are rare but may fill a need in a specific scenario.

Power over Ethernet Support

More enterprise class APs support Power over Ethernet (PoE) than not. Support for PoE allows for the installation of APs in areas where no power outlets are found but where you can run network cables to carry the power. While PoE is very popular for WLAN devices, because it can provide extra features such as power cycling the device as well as powering the device in the first place, it is sometimes more cost effective to run the power to the area rather than using PoE. This is usually the case when only one location needs the power outlet, the power run would only be a few feet, and the organization currently has no PoE switches. As you can see, the scenario where running power would be more cost effective than PoE is quite rare, hence in part, the popularity of PoE.

Consider the implications of PoE carefully before deciding against it. You often hear that the primary benefit of PoE is the ability to install APs where there is no AC power outlet; however, it is certainly a major benefit to be able to power cycle (stop and start the device) an AP that is installed in the ceiling and plugged into a PoE connection there. Many PoE switches support the stopping and starting of power injection on the PoE ports using the command line or graphical management tools the vendor provides. This means you can restart an AP from your desk even if you cannot get into the management interface of the AP, and even if the AP has stopped responding to other management interfaces that communicate with the device through the network layers. To me, this is an equally valuable benefit to that of being able to place an AP where there is no power outlet. Stated differently, even when a power outlet is available, it may be advantageous to power the AP through a switch-based PoE. This allows the WLAN analyst to simply restart the AP from remote if users report problems as a first step instead of getting involved in heavy analysis. (This assumes no mission critical applications are on the BSS, and the analyst knows it is safe to restart it.)

PoE support is usually not found in SOHO APs like those from Linksys or Netgear. Most enterprise APs do support PoE, but check with your vendor to ensure you purchase a model that supports it if you need it. While more and more enterprise class APs do support PoE, some rare models still do not.

Mesh Networking Functions

Modern APs often provide a mesh networking function. The mesh function allows the AP (AP1) to act as a client to multiple other APs (AP2 and AP3 for example) and treat the individual associations with these other APs as ports across which it can bridge traffic for the STAs associated with it (AP1). When a client needs to reach a destination that is

reachable through AP2, but that client is associated with AP1, AP1 will bridge the packets across the association with AP2 on behalf of the client.

There is a limit to the number of associations these APs can make. For example, the older Motorola/Symbol AP-5181 AP can create up to three mesh associations with other APs. The AP-5181 calls these connections client bridges. At the same time, the device can act as a base bridge and accept income client bridge connections from other AP-5181 APs. With these capabilities, a somewhat dynamic mesh network can be built over time across which client traffic may be directed. All of the associations in the Motorola/Symbol APs are based on the SSID (called the ESSID in documentation, though this is not IEEE standard terminology). In other words, the mesh network is built dynamically based on the SSID and the other APs in client bridge mode, base bridge mode, or both are discovered through beacon scanning.

Most vendors today support mesh functions in their APs. These APs can build a mesh using one radio and provide client access with the other. For example, ten APs could build a mesh using 5 GHz radios and then provide client access with their 2.4 GHz radios. This method provides optimal performance as the AP does not have to switch a single radio from client servicing to mesh servicing.

Figure 4.19 shows a network implementation using APs that support a mesh networking mode. In this case MU1 is associated with AP1, and MU2 is associated with AP2. Since AP1 is a client bridge to AP2, and AP2 is a client bridge to AP3 while being a base bridge to AP1, both MU1 and MU2 can access the files on the file server. This is possible even though AP1 may not be connected to an Ethernet port. The association AP1 has with AP2 becomes the port across which it bridges network traffic destined for the file server.

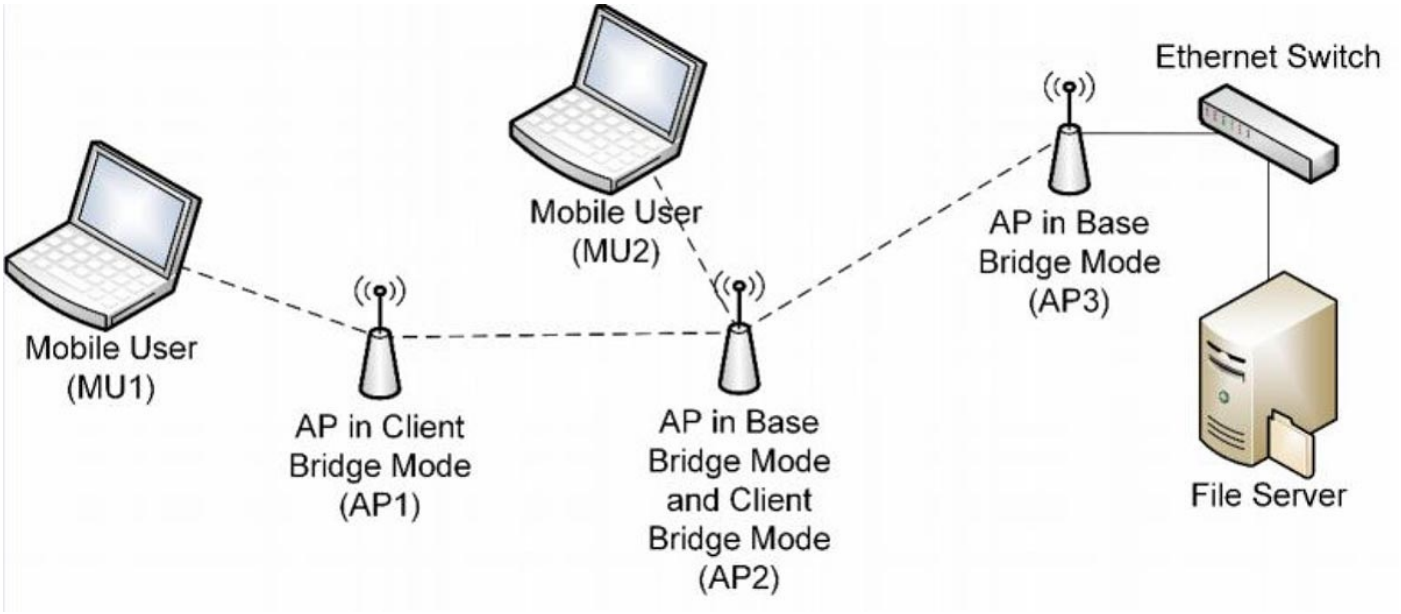


Figure 4.19: Mesh Networking Mode Implemented

Hotspot Support

Increasingly newer APs are coming equipped with hotspot support. This usually includes walled garden capabilities and may also include connectivity to online payment processing services if you are providing a for-pay hotspot. Having this support built in is also useful when you simply want to provide a “guest” network for visitors to your organization’s facilities. The Wi-Fi Alliance provides the Hotspot 2.0 (Wi-Fi Certified Passpoint)

certification for providing hotspot features. According to the Wi-Fi Alliance:

Wi-Fi CERTIFIED Passpoint™ launched in 2012 as an industry-wide solution to streamline network access in hotspots and eliminate the need for users to find and authenticate a network each time they connect. In Wi-Fi networks that do not support Passpoint, users must search for and choose a network, request the connection to the access point (AP) each time, and in many cases, must re-enter their authentication credentials. Passpoint automates that entire process, enabling a seamless connection between hotspot networks and mobile devices, all while delivering the highest WPA2™ security. Passpoint is enabling a more cellular-like experience when connecting to Wi-Fi networks.

Wi-Fi is a strategic imperative in today's mobile world, and is becoming increasingly crucial for mobile and fixed operators, as well as the retail and hospitality industry, as they invest in Wi-Fi to meet business challenges. In October 2014, new features were released that build on Passpoint's foundation of security and seamless connection to make the technology even more valuable for service providers, while opening up new opportunities for other sectors. New features include:

- **Online sign-up and immediate account provisioning:** Passpoint now enables a streamlined process to establish a new user account at the point of access. For service providers, this reduces barriers to account creation and usage. For users, this capability takes the complexity out of getting connected and enables in-pocket connection across a service provider's network of hotspots. Learn more about Certificate Authority Vendors.
- **Secure registration:** The process of establishing a new account or connecting a second device takes place securely. Devices are provisioned with the appropriate credentials and configuration for network access. Users can be confident they are connecting to their chosen provider's valid network, and their credentials are exchanged securely.
- **Operator policy:** Passpoint now includes the capability for service providers to distribute their specific subscriber policies, such as which networks to join and in what order of preference. This policy support enables providers to deliver the best user experience on Wi-Fi, while still easily maintaining the business requirements of Wi-Fi roaming agreements.

The end-user market is poised to embrace seamless Wi-Fi offerings. Research recently conducted among smartphone and tablet users in the United States and United Kingdom on behalf of Wi-Fi Alliance found that Wi-Fi services enabled by Passpoint have the potential to foster customer loyalty and drive measurable business value for both service providers and retailers.

Security Capabilities

APs support a large pool of common security capabilities. These include:

- MAC address filtering (a common item in vendor's lists of security features though it is not such)
- 802.1X port-based authentication

- 802.11i (TKIP/RC4 and CCMP/AES)
- SSH and SSH2 for management access
- HTTPS access to web-based management
- WPA/WPA2 (remember that WPA is now deprecated in the standard)
- SNMP v3 for secure SNMP management
- Various EAP types (some are secure some are not)
- Built-in firewalls
- Support for VPN tunnel endpoints and pass-through
- Content filtering

Your role as a WLAN administrator or engineer may include the selection of APs that support the security technologies required by your security policies. Today, these policies will likely specify that you cannot implement an AP that uses WEP for data encryption, and you must therefore select an AP that supports WPA-PSK at a minimum (if you must support older devices) or WPA2-PSK at a minimum to comply with modern standards. More likely, in an enterprise implementation, you will be implementing full CCMP/AES (WPA2) support from this point forward—until a newer and better security technology comes along. This last statement is not meant to indicate that WPA is automatically insecure, only that it will be someday and is already far less secure than WPA2 even with proper implementation.

Management Capabilities

APs will provide different methods for configuration and management of the devices. These methods will vary from vendor to vendor and from model to model within vendor's product lines. However, there are common methods utilized. These common methods include:

- Console (serial)
- Telnet
- SSH
- SNMP
- Custom software applications
- Web-based interfaces

Console or serial interfaces are usually only provided on enterprise class hardware. For example, Cisco, HP, and other enterprise devices are likely to come with console interfaces for configuring them. Linksys, Belkin, D-Link, and Netgear devices are less likely to come with such an interface. This should not be taken as a given. For example the NETGEAR WG302 AP (see Figure 4.20) supported a console port as well as most of the other common management interfaces mentioned in this section. Many vendors that were once known as only SOHO vendors are beginning to attempt to cross over into the enterprise market.

When using a console interface to configure an AP, you will usually connect a serial cable from your computer to the AP. You may also use a USB to serial converter such as the one seen in Figure 4.21. Once connected, you will use a terminal program such as PuTTY, in Windows, to connect to the device. Once connected, you will use the CLI (command line interface) provided by the vendor. Each vendor's CLI will be somewhat different, and sometimes they will be vastly different. This is one of the major arguments for using consistent hardware throughout your organization: you only have to learn one set of CLI commands rather than a varied set. The good news is that the CLI is usually only used at initial configuration or for device reload, and the other graphical interfaces are usually used for ongoing maintenance and configuration support.

Figure 4.20: Older NETGEAR WG302 AP Often Considered SOHO

Figure 4.21: A USB to Serial Converter

The telnet and SSH or SSH2 interfaces will be similar to the console management method in that the CLI will be utilized. The difference is that the CLI is being utilized across the network rather than through the console port and a serial cable. When using these management methods across the network, you should be careful to ensure that some form of encryption is in use. Otherwise, with telnet for example, the commands being transmitted from your machine to the AP are being sent in clear text that is easily readable in any common Ethernet packet analyzer.

SNMP is widely supported among WLAN devices. Due to security vulnerabilities in earlier versions, you should choose only devices that support SNMP v3, and eventually higher. SNMP provides for centralized mass configuration management. SNMP is a standardized technology so one centralized application can often manage multiple vendors' APs.

Custom software applications may come with the AP and are usually provided on a CD-ROM or from download sites when they do. These applications are usually designed to run on Windows clients since these clients are very popular in enterprises. The applications may provide first-time configuration only, or they may provide for ongoing configuration management. Due to the proprietary nature of these applications, they provide limited value to very large scale installations.

Finally, web-based configuration interfaces take advantage of built-in web server software in APs to allow for remote configuration through the Ethernet interface. While you may be able to enable web-based management through the WLAN interfaces, I do not recommend it. This means that an attacker can try to guess the password and then manage the AP across the WLAN. He or she will not even need to gain access to your physical network. For this reason, if you enable the web-based administration interface at all, it should only be enabled for the Ethernet port. Web-based management interfaces are provided on

nearly all APs whether they are built for enterprise or SOHO use.

Note: **In addition to the configuration features mentioned here, most WLAN-autonomous APs also allow you to save the configuration to a file that can be downloaded from the device to a disk. This allows you to quickly and easily reload the configuration at a later point. It also provides for quick changes from one configuration to another. Some APs also provide onboard storage of multiple configurations among which you can switch.**

Mounting Options

APs may be placed on flat surfaces or they may be mounted in many different ways. Mounting locations and methods include:

- Wall mount
- Ceiling mount
- Pole mount

When mounted on the wall, screws are usually fastened into the wall, and then the AP's mounting hardware is slipped onto the screws. The screws may be tightened further, and then the AP snapped into the mounting hardware. Alternatively, the AP may have the mounting hardware already attached, and the mounting is complete as soon as the AP is slipped onto the screws. With a ceiling mount the AP is usually attached to similar mounting hardware, but the fasteners must be passed through the tile or other ceiling material. Finally, the pole mount method usually includes a wrapping brace that passes around the pole and then fastens to the AP's mounting hardware. Figures 4.22, 4.23, and 4.23 show examples of these three mounting methods. While these examples show screen shots of the mounting instructions for the older Motorola/Symbol 5131 and Motorola/Symbol 5181 APs, most APs offer similar mounting instructions and capabilities.

Mounting an AP is more involved than just deciding among the wall, ceiling, pole, or flat surface mount options. You should actually determine where the AP needs to be placed (during survey and design), and then determine the mounting option available to you based on the location. In other words, the mounting method will usually be dictated by the location. The ultimate goal is to provide the proper coverage in the proper location, and this means that mounting methods are secondary.

Another factor to consider when choosing a mounting method is physical access for maintenance. Will you be able to access the reset button on the device, if needed? Will you be able to view the power and connectivity LEDs to determine operational status? These factors should be considered carefully. If you do not have access to the reset button or the power cord for power cycling, can you implement an AP that supports PoE for power cycling? While this will not provide convenient access to configuration resets (like the configuration reset button would), it will allow you to power cycle the device more easily.

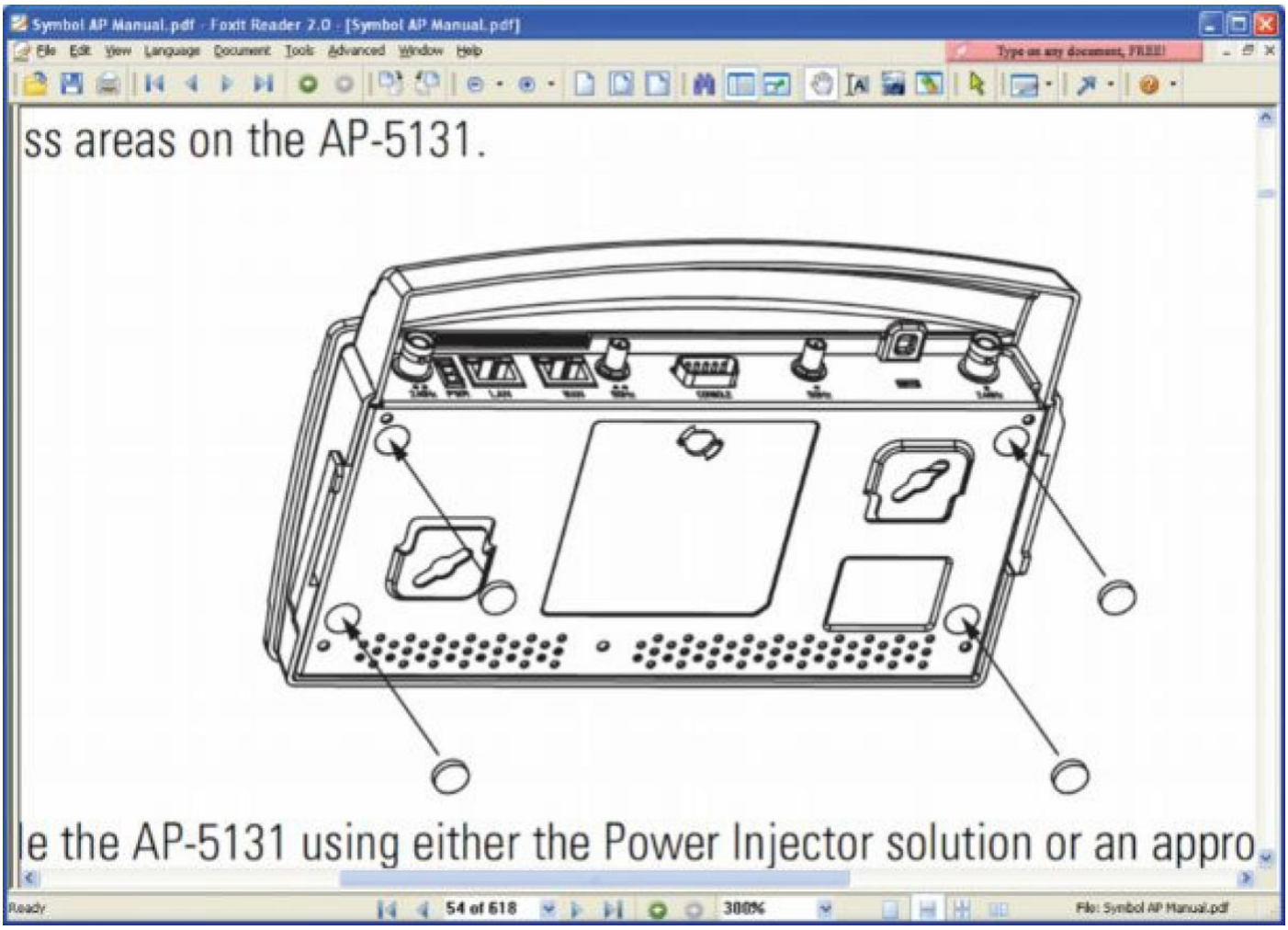


Figure 4.22: Wall Mount Slip over Holes and Flat Surface Shock Pads

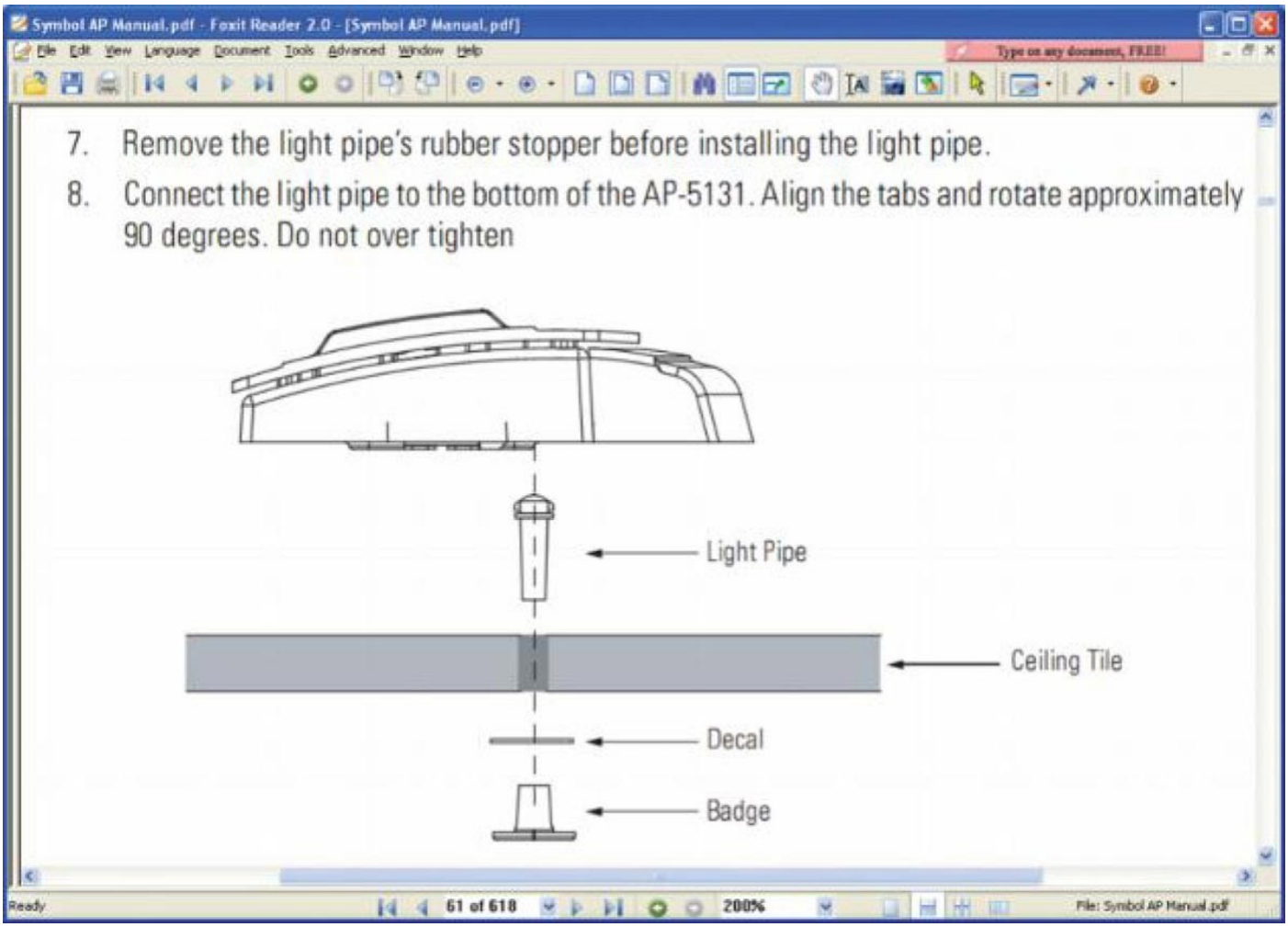


Figure 4.23: Ceiling Mount Pass-Through Fasteners for Tiles

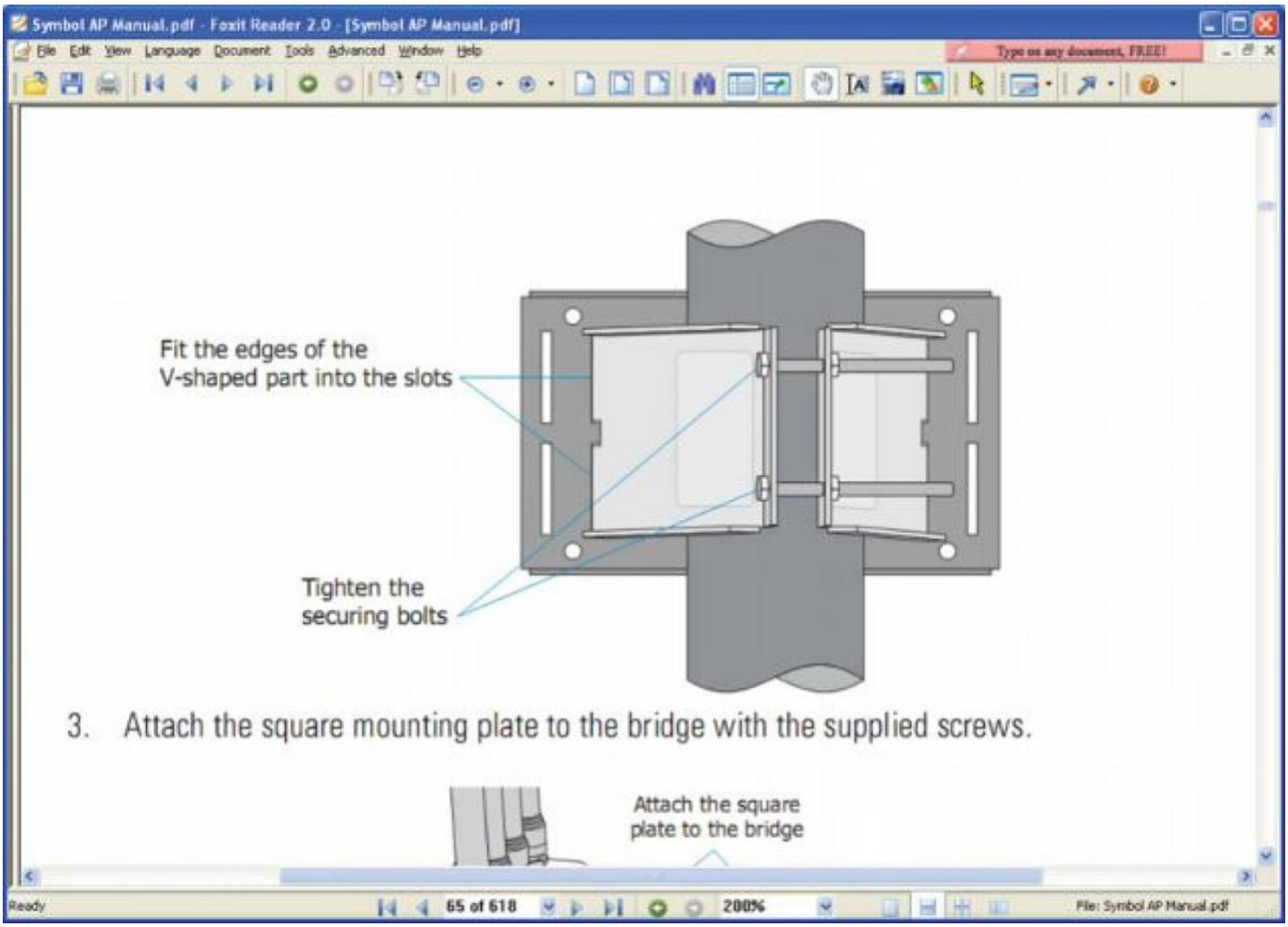


Figure 4.24: Pole Mount Fastening Option

When mounting APs and other WLAN devices outdoors, you will need to consider weather issues. For example, will the AP be protected from rain and wind damage? The National Electrical Manufacturers Association (NEMA) has established a set of standards for electrical equipment enclosures. These NEMA enclosures are available for mounting APs and other WLAN devices outdoors. The NEMA Standards Publication 205 defines the various enclosure standards and is available at www.nema.org.

AP Configuration Processes

Many new APs will come out of the box with the antennas detached, if they have removable antennas. If this is the case, you will need to first attach the antennas before the AP will be able to radiate the RF signal. Depending on the AP, it may be damaged if powered on without antennas attached. You will typically attach the antennas and then configure the AP before connecting it to the wired network if it is an autonomous AP.

As the last sentence suggested, you should configure the AP before connecting it to the actual wired LAN to which it will provide access. This helps to remove the potential for wired-side access before the AP is properly configured, and reduces the likelihood that you will provide an unsecure entry way into your LAN—though only for a short time—during the configuration window. Most APs come from the factory with little or no security set, so they can certainly provide a point of vulnerability by default. Some APs come with the radios turned off to avoid possible damage, as well.

After the AP is properly configured according to your security policies and configuration standards, you will need to connect the AP to the wired LAN via the Ethernet port. You may also need to connect the antennas if you did not connect them before configuration, or if you disconnected them during configuration for security reasons.

When the AP is a lightweight, it will come with no significant configuration and should be connected to the wired port to locate the controller and pull its configuration and or firmware from the controller.

Finally, you should test the AP to ensure that you can connect to it with a client configured for appropriate security and configuration settings that match the SSID transmitted from AP. If you are using an AP model for the first time, you may also want to perform some load testing to verify whether the AP works as advertised (in relation to throughput and concurrent connection) or not. You may need to adjust the number of installed APs according to real-world performance with some devices.

> **EXAM MOMENT:** Virtual LANs (VLANs) are commonly used in conjunction with different SSIDs to separate and identify different WLANs in a single AP. This allows the AP to service more than one WLAN.

In the end, access points come in many different shapes and sizes. One vendor may provide very different APs in form factor and capabilities. At the very least, they will often offer indoor and outdoor models and options for both internal and external antennas. APs usually support a common set of IEEE standards, security capabilities, and mounting options. Common management interfaces include console, telnet, and web-based interfaces, among others. Most APs that are used in enterprise installations today support SNMP for centralized management and may support custom software provided by the AP vendor. As a WLAN administrator, it is important that you understand these options and be able to choose among them effectively.

AP Spec Sheet

An AP spec sheet, like a client spec sheet, provides important information for decision makers and WLAN analysts. As an analyst, it provides you with information needed to understand the operational capabilities of the AP. In this section, I will describe the spec sheet for the WAP371 from Cisco, which is available at `bit.ly/1pkepb3`. This is a small business AP that supports 802.11ac and 802.11n in 5 GHz and 2.4 GHz, respectively. It is an excellent AP for lab exercises, as it is inexpensive and supports frame capture in 3x3:3 VHT mode. The packets can be downloaded to a computer for analysis in Wireshark or a commercial protocol analyzer, which is discussed more in the later section of this chapter titled Wireless Analysis Hardware and in-depth in Chapter 5.

A typical spec sheet has important sections including:

- Standards
- Ports
- Antennas
- Security

- QoS
- Management
- WLAN Capabilities and Data Rates
- Transmit Power
- Antenna Gain
- Receive Sensitivity
- Power Options

Vendors may reference these sections with different names, but the information they provide is key. The following sections describe this information.

Standards

This section lists the standards supported by the device. For example, it will indicate the 802.11 standards supported as well as other standards such as PoE (802.3af and 802.3at), 802.1X (port-based security), 802.1Q (VLANs), 802.11i (WPA and WPA2 security), 802.11e (QoS), and higher layer standards. The WAP371 in review lists the following supported standards:

- 802.11ac
- 802.11n
- 802.11g
- 802.11b
- 802.3af
- 802.3u
- 802.1X (security authentication)
- 802.1Q (VLAN)
- 802.1D (Spanning Tree)
- 802.11i (WPA2 security)
- 802.11e (wireless QoS)
- IPv4 (RFC 791)
- IPv6 (RFC 2460)

Ports

The Ports section will list the available wired ports on the device. For example, it will indicate whether the port supports 100 Mbps or 1 Gbps. Specialized ports, such as 4G interfaces, may also be listed. The WAP371 lists a LAN Gigabit Ethernet autosensing port. As an alternate example, the Aruba Networks RAP-155, which is a remote access point (RAP) with built-in switch ports, indicates that it includes a single 1 Gbps uplink port and four 1 Gbps LAN ports. Additionally, it indicates that two of the LAN ports are PoE capable as an option.

In modern, dual-band APs with 802.11ac 3x3:3 in 5 GHz and 802.11n 2x2:2 in 2.4 GHz (the specs of the WAP371), it is theoretically possible that the wired port could become a bottleneck. However, thanks to the WLAN overhead and the maximum throughput of around 350 Mbps (with 40 MHz channels) on the 802.11ac radio and around 80 Mbps (with 20 MHz channels) on the 802.11n radio, it is very unlikely that the 1 Gbps port will become a bottleneck. As new 4x4:4 chipsets are integrated into 802.11ac APs, and 3x3:3 chipsets are used in the 2.4 GHz band, the aggregate WLAN throughput could reach 600-650 Mbps. If a dual 5 GHz AP is implemented with 4x4:4 802.11ac, a 1 Gbps port will likely become a bottleneck in dense BSSs.

Antennas

The antennas section may simply indicate that internal antennas are used, or it may indicate external antennas and the connector types. This information is crucial should you determine through analysis that alternate antennas should be used to address coverage problems. Antennas should be selected based on vendor support, along with gain requirements and connector types. Some vendor spec sheets will provide antenna pattern charts. For example, Figure 4.25 shows the antenna pattern charts for the RAP-155 from Aruba Networks in the 2.4 GHz band. Recall that you learned about how to read these patterns in CWNA.

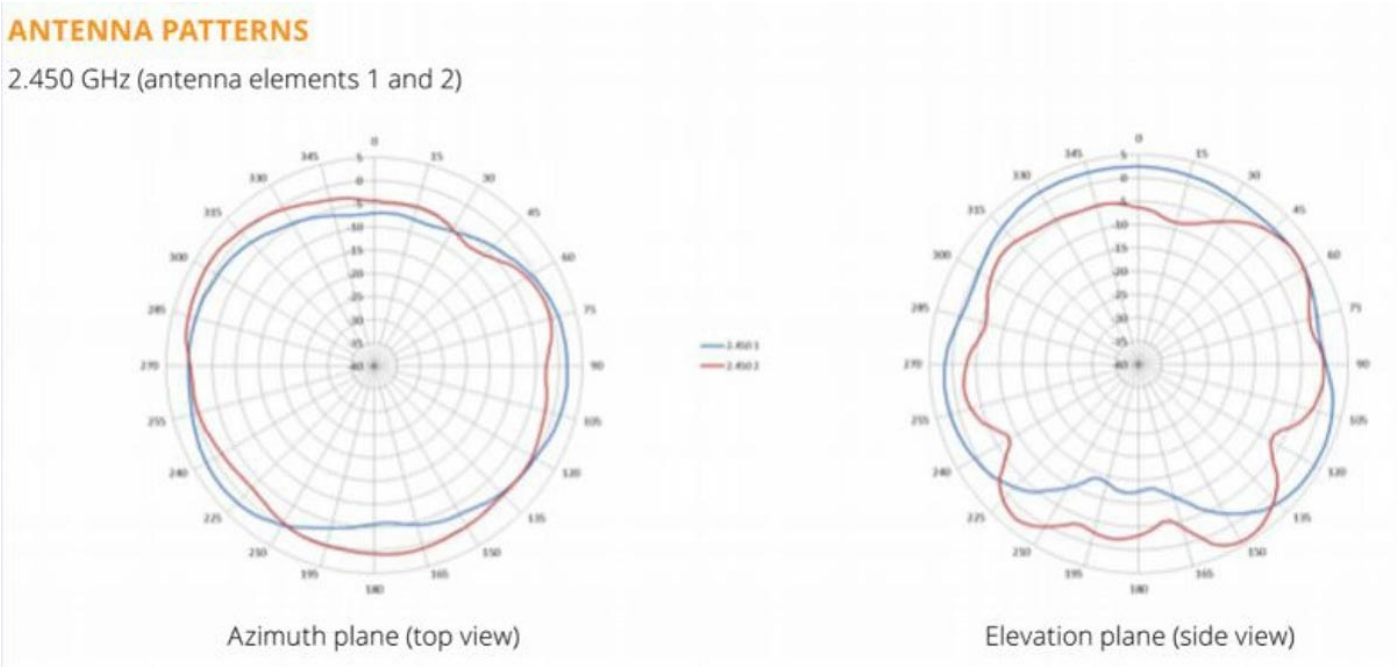


Figure 4.25: Antenna Pattern Chart in AP Spec Sheet

Antenna Gain

The antenna gain section will provide information on the gain of the default antennas or only antennas when they are integrated without external antenna support. Antenna gain is typically indicated in dBi (decibel isotropic). For example, the WAP371 provides 2 dBi of gain. Therefore, if transmitting at 17 dBm (50 mw), and the antenna gain is 2 dBi, the resulting equivalent isotropically radiated power (EIRP) is 80 mw. The WAP371 has a default output power of 17 dBm for 2.4 GHz with some variation depending on the data rate used and, therefore, has an EIRP of 80 mw by default. The exact details of the transmit power of the WAP371 are shown in the later section titled Transmit Power. Again, refer to CWNA for the RF math if you need to.

Security

The security section will indicate security features available. The WAP371 lists the following security features:

- WPA/WPA2 with Enterprise support
- ACL-based access control
- HTTPS for secure management
- Rogue AP detection

QoS

The QoS section will list the prioritization and queueing features available on the AP. The Cisco WAP371 lists WMM and client QoS. The RAP-155 lists no direct information about QoS (with the exception of airtime fairness, which some consider a QoS feature); however, when searching the Wi-Fi Alliance database for certifications for the RAP-155, the information in Figure 4.26 shows certified support for both WMM and WMM-Power Save. This fact reveals the importance of gathering information about devices from multiple sources.

For example, you can gather information from:

- Vendor websites
- Wi-Fi Alliance product finder
- FCC ID search

Wi-Fi CERTIFIED™ Interoperability Certificate

This certificate lists the features that have successfully completed Wi-Fi Alliance interoperability testing.
Learn more: www.wi-fi.org/certification/programs

Certification ID: WFA19814 **Page 1 of 2**

Date of Last Certification	May 20, 2013
Company	Hewlett Packard Enterprise
Product	Aruba Instant Access Point RAP-155
Model Number	RAP-155
Product Identifier(s)	
Category	Enterprise/Service Provider Access Point, Switch/Controller or Router
Hardware Version	Product: , Wi-Fi Component:
Firmware Version	Product: 6.2.1.0-3.3.0.0, Wi-Fi Component:
Operating System	Proprietary / Other: Unspecified
Frequency Band(s)	2.4 GHz, 5 GHz - Switchable

Summary of Certifications

CLASSIFICATION	PROGRAM
Connectivity	Wi-Fi CERTIFIED™ a, b, g, n
	WPA™ – Enterprise, Personal
	WPA2™ – Enterprise, Personal
Optimization	WMM®
	WMM®-Power Save

Figure 4.26: Aruba Networks RAP-155 AP Certificate

Note: **If you enjoy disassembling APs to explore the insides, consider using an FCC ID search instead of prying open the AP. The photos of the internals may give you all the information you need, and it will not void the manufacturer's warranty. For example, Figure 4.27 shows the inside of the WAP372 from the FCC site.**

Figure 4.27: Cisco WAP371 Internals

Management

The management section will typically provide information on management protocols available and other management features. The WAP371 lists the following in the management section:

- Management protocols: Web browser, Simple Network Management Protocol (SNMP) v3, Bonjour
- Remote management: Yes
- Event logging: Local, remote syslog, email alerts
- Network diagnostics: Logging and packet capture
- Web firmware upgrade: Firmware upgradable through web browser, imported/exported configuration file
- Dynamic Host Configuration Protocol (DHCP): DHCP client
- IPv6 host: Yes
- HTTP Redirect: Yes

WLAN Capabilities and Data Rates

The WLAN capabilities and data rates sections are formatted differently among vendors, but they will all provide information on the PHYs supported, the number of spatial streams, the data rates available, and the channel widths available. Figure 4.28 shows these sections for the WAP371 AP.

These sections may also list the supported channels in each frequency band and the number of non-overlapping channels. For example, the WAP371 lists three non-overlapping channels in 2.4 GHz (at 20 MHz) and 21 non-overlapping channels in 5 GHz (at 20 MHz). It lists nine 40 MHz channels and five 80 MHz channels.

Wireless	
Frequency	Dual concurrent radios (2.4 and 5 GHz)
Radio and modulation type	Dual radio, orthogonal frequency division multiplexing (OFDM)
WLAN	802.11n/ac 3x3 multiple-input multiple-output (MIMO) with 3 spatial streams at 5 GHz 2x2 MIMO with 2 spatial streams at 2.4 GHz 20-, 40-, and 80-MHz channels for 802.11ac 20- and 40-MHz for 802.11n PHY data rate up to 1.6 Gbps 802.11 dynamic frequency selection (DFS)
Data rates supported	802.11a/b/g: • 54, 48, 36, 24, 18, 12, 9, 6, 11, 5.5, 2, and 1 Mbps • 802.11n: 6.5 to 450 Mbps ◦ 20-MHz bandwidth: MCS 0-15 for supported data rates ◦ 40-MHz bandwidth: MCS 0-15 for supported data rates • 802.11ac: 6.5 to 1300 Mbps ◦ 20-MHz bandwidth: MCS 0-9 for supported data rates ◦ 40-MHz bandwidth: MCS 0-9 for supported data rates ◦ 80-MHz bandwidth: MCS 0-9 for supported data rates

Figure 4.28: Wireless Capabilities Section

Transmit Power

The transmit power section will provide the output power levels for the different PHYs at different data rates. Figure 4.29 shows this section for the Cisco WAP371 AP spec sheet. Notice that the default output power levels vary depending on the PHY and data rate.

The Aruba RAP-155 simply lists the maximum output power per radio chain as 18 dBm (64 mw) in both 2.4 GHz and 5 GHz; however, it further states that the output power will be limited as needed to comply with regulatory requirements.

Receive Sensitivity

The receive sensitivity section is very important as it informs you of the signal strength required to achieve particular MCS or data rates. Figure 4.30 shows the Receiver Sensitivity section for the WAP371 AP, and Figure 4.31 shows this section for the RAP-155 AP.

Power Options

The final section discussed here is the input power options section. This portion of the

spec sheet will inform you of the methods available for powering the device. For example, the Cisco WAP371 lists the options of an 802.3at Ethernet switch, a Cisco power injector (still PoE) or an AC adapter.

> **EXAM MOMENT:** Understanding how to read a spec sheet and apply it to troubleshooting scenarios is very important for the CWAP exam candidate and for day-to-day support of WLANs.

Transmitted output power	2.4 GHz • 802.11b: 17.0 +/- 1.5 dBm @ CH6, all rates • 802.11g: 17.0 +/- 1.5 dBm @ CH6, 6 Mbps • 802.11g: 15.0 +/- 1.5 dBm @ CH6, 54 Mbps • 802.11n(HT20): 17.0 +/- 1.5 dBm @ CH6, MCS0 • 802.11n(HT20): 14.0 +/- 1.5 dBm @ CH6, MCS15 • 802.11n(HT40): 12.0 +/- 1.5 dBm @ CH6, all rates 5 GHz UNII-1 (5150 to 5250 MHz) • 802.11a: 10 +/- 1.5 dBm @ all rates • 802.11ac(HT20): 10 +/- 1.5 dBm @ all rates • 802.11ac(HT40): 11 +/- 1.5 dBm @ all rates • 802.11ac(HT80): 11 +/- 1.5 dBm @ all rates 5 GHz UNII-2 (5250 to 5350 MHz)/UNII-2 Extended (5470 to 5725 MHz) • 802.11a: 16.0 +/- 1.5 dBm @ 6 Mbps • 802.11a: 15.0 +/- 1.5 dBm @ 54 Mbps • 802.11ac(HT20): 16.0 +/- 1.5 dBm @ MCS0 • 802.11ac(HT20): 13.0 +/- 1.5 dBm @ MCS9 • 802.11ac(HT40): 18.0 +/- 1.5 dBm @ MCS0 • 802.11ac(HT40): 13.0 +/- 1.5 dBm @ MCS9 802.11ac(HT80): 13.0 +/- 1.5 dBm @ all rates 5 GHz UNII-3 (5725 to 5850 MHz) • 802.11a: 18.0 +/- 1.5 dBm @ 6 Mbps • 802.11a: 15.0 +/- 1.5 dBm @ 54 Mbps • 802.11ac(HT20): 18.0 +/- 1.5 dBm @ MCS0 • 802.11ac(HT20): 13.0 +/- 1.5 dBm @ MCS9 • 802.11ac(HT40): 18.0 +/- 1.5 dBm @ MCS0 • 802.11ac(HT40): 13.0 +/- 1.5 dBm @ MCS9 • 802.11ac(HT80): 18.0 +/- 1.5 dBm @ MCS0 • 802.11ac(HT80): 13.0 +/- 1.5 dBm @ MCS9

Figure 4.29: Cisco WAP371 Transmitted Output Power Section

Receiver sensitivity	2.4 GHz • 802.11b: -86 dBm @ 11 Mbps • 802.11g: -75 dBm @ 54 Mbps • 802.11n(HT20): -69 dBm @ MCS15 • 802.11n(HT40): -66 dBm @ MCS15 5 GHz • 802.11a: -79 dBm @ 54 Mbps • 802.11ac(HT20): -62 dBm @ MCS9 • 802.11ac(HT40): -59 dBm @ MCS9 • 802.11ac(HT80): -57 dBm @ MCS9

Figure 4.30: Cisco WAP371 Receiver Sensitivity Section

RF PERFORMANCE TABLE		
	Maximum transmit power (dBm) per transmit chain	Receiver sensitivity (dBm) per receive chain
802.11b 2.4 GHz		
1 Mbps	18.0	-92.0
2 Mbps	18.0	-92.0
5.5 Mbps	18.0	-90.0
11 Mbps	18.0	-88.0
802.11g 2.4 GHz and 802.11a 5 GHz		
6 Mbps	18.0	-88.0
54 Mbps	16.0	-75.0
802.11n HT20 2.4 GHz and 5 GHz		
MCS0/8/16	18.0	-88.0
MCS7/15/23	14.0	-71.0
802.11n HT40 2.4 GHz and 5 GHz		
MCS0/8/16	18.0	-85.0
MCS7/15/23	14.0	-68.0

Figure 4.31: Aruba Networks RAP-155 Receiver Sensitivity Table

WLAN Controllers and Managers

The legacy edge architecture where WLAN APs were placed at the network edge and configured individually was fine for smaller networks; however, as larger and larger WLANs were implemented it became apparent that configuring each AP was no longer feasible. Vendors rushed to create their own solutions to this enterprise network dilemma. The result was the creation of WLAN switches, which are now known as WLAN controllers. For this reason, I will use the term WLAN controller to refer to the features and capabilities that are commonly found in these devices.

A WLAN controller contains all or part of the functionality of one or more virtual APs. At first glance, a WLAN controller may look like any other switch when it is configured to have the capabilities of a regular LAN switch with additional support for WLAN control. Other WLAN controllers, like the Cisco small business 2504 controller pictured in Figure 4.32, have only a limited number of ports (usually two), and they appear very different from standard Ethernet switches. Such controllers are intended to connect to a small number of APs (four for the 2504) or to connect to APs through other standard Ethernet switches.

When implementing a WLAN controller, each Ethernet port connects to an AP from the same vendor that produced the controller, or each Ethernet port connects to another switch that connects to multiple Ethernet ports for the support of more APs. For example, the Cisco 2504 controller provides only four Ethernet ports, and yet the controller can manage up to 75 APs and up to 1000 client STAs. Obviously, with three Ethernet ports for the APs and the other for connectivity to the wired network, there must be a layered switching architecture to accommodate 75 total APs. Indeed, you would connect one or more LAN switches to the Ethernet ports and then connect APs to the LAN switches or even other switches several routers away. It is for this reason, among others, that WLAN analysts

cannot *simply know* wireless networking—they must fully grasp it. Chapter 7 addresses wired networking issues that commonly cause problems in WLANs.

Figure 4.32: Cisco 2504 WLAN Controller

Of course, every WLAN vendor says their WLAN controller solution is the best on the market. To be certain, each solution has its benefits and drawbacks. As a WLAN administrator and troubleshooter, you must analyze the features offered and then choose the best solution for your implementation. This analysis usually means looking through the vendor literature thoroughly and sometimes requesting test equipment to work with during the analysis phase of your WLAN implementation project. Some vendors will provide the evaluation equipment free of charge, while others will come in and perform a demonstration of the equipment for you. The reality is that smaller organizations are less likely to get free sample devices and larger organizations are more likely to get them. If you are in a smaller organization, the product manuals, which are usually available for free download from the vendor websites, may suffice for your analysis.

When looking through the vendor literature, pay close attention to the IEEE standards that are supported as well as the proprietary ways in which the WLAN will be implemented. Larger vendors usually remain in business for long periods of time or are consumed by other vendors who continue to support their hardware. A perfect example of this is the Symbol hardware that is so common in WLANs. Symbol was acquired by Motorola, but Motorola continued to support and sell the Symbol WS2000 and WS5100 series WLAN switches among other devices for a period of time after acquisition, and you can still download support files for some of these devices. (Motorola has since been purchased by Zebra Technologies.)The point is this: if you go with a vendor who implements heavy proprietary technologies, and their devices simply cannot operate in an IEEE standard fashion (from a management perspective) you may be forced to replace all the equipment at a later—and possibly earlier than expected—date, if support is lost.

Many WLAN controllers include built-in site survey capabilities that are either assisted or automated in nature. The assisted site surveys will require that you walk around within the facility, after a pool of APs have been installed, with a compatible client that can send signal information back to the controller through the APs. The automated site surveys will simply configure the WLAN according to guidelines you can generally manage centrally at the WLAN controller. Today, this is often called Radio Resource Management (RRM), though RRM is often used in conjunction with manual site surveys. The automated method usually requires more over-engineering (placing more APs than are absolutely

needed), and the manual method usually requires less; however, many controllers support both.

WLAN Controller Common Features

Since many of the features of WLAN controllers were already covered in the AP section, I will only list the common features here. Remember, a WLAN controller usually centralizes the “AP” processing into the controller and away from the AP itself. For this reason, WLAN controllers often implement the features that are traditionally found in thick or autonomous APs. The following features are common, and some may require additional licensing:

- PoE injection into the Ethernet ports (may only be supported on a subset of the ports)
- Built-in firewall capabilities
- Port filtering and MAC address filtering
- Standards-based and proprietary WLAN security technologies such as WPA, WPA2, EAP and IEEE 802.11i
- VPN tunneling
- Common management interfaces (web, telnet, CLI, SSH, console, etc.)
- Configuration file management
- Activity monitoring and logging
- Built-in RADIUS servers for EAP authentication types
- Redundant WLAN access ports for greater uptimes and easier maintenance
- Rate limiting for the various managed WLANs; this feature is very convenient for setting up two WLANs in the same area – one for VoWLAN (no rate limits) and the other for data (rate limited)
- Hotspot support including IP redirect to map connections to a specific “starting” page
- RBAC (role-based access control) or identity-driven management (IDM) to provide different levels of access to different users depending on RADIUS settings
- Voice prioritization for VoWLAN
- CAPWAP compatibility
- Wireless client roaming management and assistance
- QoS including IEEE 802.1p and IEEE 802.11e
- Internal DHCP server
- Built-in Wireless Intrusion Detection System (WIDS) or Wireless Intrusion Prevention System (WIPS)

For more information on any of the features listed here, or features not listed, be sure to visit the various vendor websites listed below and download the product manuals for their WLAN switches. These manuals will go into the details of how each vendor implements the WLAN differently and help you understand the general use of WLAN switches in modern wireless networks. Consider visiting the following websites at a minimum:

- Cisco: www.cisco.com
- Aruba Networks: www.arubanetworks.com
- Meru Networks: www.merunetworks.com

WLAN Controller Configuration Process

The configuration process will vary depending on the controller vendor you choose; however, the process is generally similar when considered from a less detailed level. The process usually looks something like this:

1. Perform the initial controller configuration
2. Configure WLANs in the controller
3. Connect APs to the controller
4. Ensure APs are properly enabled and configured

The first step is to perform the initial controller configuration. This usually includes specifying which port will be used for WLAN AP connectivity and which port will be used for WAN uplinks (may be a LAN link if it is only used locally and not connecting to the Internet for a branch office deployment). If the WLAN controller contains multiple ports for connections to APs or wired devices, you may configure the proper use of each port.

Next, you will need to determine if you are going to support one virtual WLAN or multiple virtual WLANs. Some controllers will support multiple WLANs with one AP and others will require multiple APs to support multiple WLANs, though this latter scenario is rare today in enterprise hardware. You will need to determine the security settings and other configuration options for each WLAN, or allow the controller to automatically select some or all of these features. You may also need to specify VLANs for the separation of the different logical WLANs that run on the same physical APs and controllers.

Now you are ready to connect the APs and have them detected by the WLAN controller. Some systems will support autonomous APs as well, but they must be converted to behave as thin APs. This may be an automatic process of the WLAN controller, or you may have to manually perform some configuration changes. The APs will find the controller using DNS, DHCP, or stored information in the cache of the AP. Once located, the APs will negotiate with the controller to receive configuration settings and firmware updates.

Finally, ensure that the APs are working properly and that you have the needed WLAN access in the needed locations. First, this will involve inspection through the WLAN controller's management interface. Make sure everything "looks" right in the controller. Second, use a laptop or some other WLAN client device to connect to the WLAN or

WLANs in the various locations to ensure that the network is functioning as you need it to function.

Note: **Remember, each vendor's installation procedure will be different. Check with the vendors to see how their installation procedures fit into the above generic installation process. You will usually find that they simply require specific, and often different, steps within each of these four phases.**

Wireless Analysis Hardware

Chapters 5 and 6 go into detail about the Wireless Analysis hardware used by WLAN analysts; however, a brief overview is in order in this chapter on WLAN hardware, as well. The two primary hardware components are spectrum analyzers and protocol analyzers.

Spectrum Analysis Hardware

To perform spectrum analysis, two basic options are available:

- Laptop spectrum analysis adapters
- Integrated AP spectrum analysis

Laptop spectrum analysis adapters are either PC Cards or USB adapters. Figure 4.33 shows the popular Metageek spectrum adapter, which is USB-based. This adapter is used in many ways today, including:

- With the Metageek Chanalyzer software
- Integrated support in protocol analyzer software
- Integrated support in site survey software

Figure 4.33: Metageek DBx Adapter

When integrated into protocol analyzer and site survey software, the adapter is often rebranded with the software vendor's logo, but it is the same adapter.

This adapter supports both 2.4 GHz and 5 GHz spectrum analysis. Figure 4.34 shows the Metageek Chanalyzer software interface.

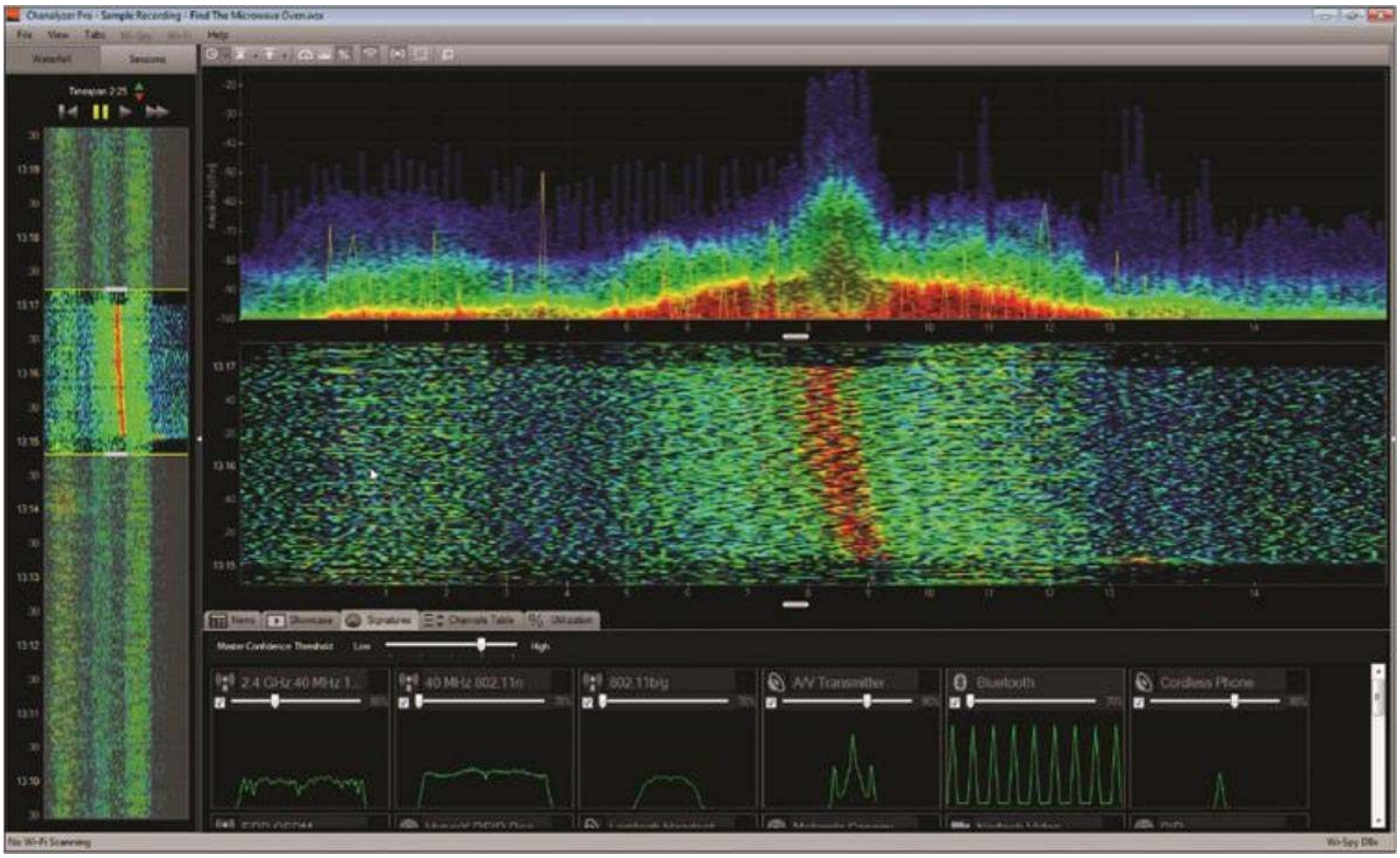


Figure 4.34: Chanalyzer Spectrum Analysis

Protocol Analysis Hardware

Protocol analysis hardware is typically a laptop computer and a device that can be used to capture the 802.11 frames. Alternatively, frames can be captured by the AP and passed to the protocol analyzer using remote packet capture (RPCAP), or stored in memory in the AP and downloaded as a packet capture file.

The challenging part, in Windows, is acquiring an adapter that supports the frame capture. You can easily capture Layer 3–7 using any adapter, but capturing Layer 2 frames will require the use of an adapter that is compatible with the protocol analysis software. Protocol analyzer vendors provide lists of such hardware.

Far more adapters can work for packet capture on Linux distributions. For example, Kali Linux is a popular penetration testing distribution that includes Wireshark and many 802.11 adapter drivers in the distribution. Simply acquiring an inexpensive adapter supported by the distribution allows you to capture frames.

The WAP371 Cisco AP referenced earlier in this chapter includes frame capture and is an excellent choice if you require only the capture of 3x3:3 streams in 5 GHz. More details on spectrum analysis and protocol analysis hardware and software are provided in chapters 5 and 6.

Wired Hardware

Wired hardware is important to the WLAN analyst, as the wireless users are ultimately

communicating with and across the wired LAN. In many cases, users think there is a problem with the WLAN, but the problem actually exists in the wired network—either in a device or server/service. This section provides a brief overview of these wired devices and services.

Ethernet Switches

The primary functions of switches in a WLAN implementation are fourfold. First, they provide access to the network, which is of course essential. Second, they configure and support the VLAN settings for the BSSs served by the APs. Third, many vendors' switches provide power to the APs using a PoE. Finally, the fourth function is QoS implementation. While the APs may be trusted to specify QoS settings, it can also be performed at the switch as the frames enter the network.

Several switches are available for use in WLAN networks; however, you will likely want to select a switch that offers at least three features:

- Power over Ethernet (PoE) for the powering of the APs
- At least 100 Mbps data rates or older WLANS and 1 Gbps for newer WLANs
- Sufficient ports for your needs

The vast majority of enterprise switches offer configurable QoS support, as well. However, if you purchase the newer switches being sold at retail stores, keep in mind that many of them are not configurable. The phrase "unmanaged switch" is often used to indicate the positive element of this inability to configure the switch. The point of the marketing is that you don't have to manage it—you simply install it and it works. Yes, it does work. It works in the way it's configured to work from the factory, and you have no way of telling it to work any differently. In most business networks you will want to avoid these unmanaged switches.

Figure 4.35 shows the Cisco 3550 switch series, which offers all of the features mentioned previously and more features, as well. The Cisco 3550 was a common switch used to provide both network access and WLAN operations and is still a great choice for building a learning lab as they can be acquired at low prices. This particular switch has been discontinued and can no longer be purchased new from Cisco. The Cisco 3750 series of switches is the recommended replacement; however, the feature set is close enough so that you can use a 3550 switch for learning in the lab and still be able to properly configure a 3750 in production environments. You are likely to continue encountering 3550 switches in production environments for a few years.

Figure 4.35: Cisco 3550 Switch

The 2950 switch, shown in Figure 4.36, is another example of a useful switch for WLAN networks. The 2950 is considered a fixed configuration switch because it does not support add-on modules. The phrase “fixed configuration” used in Cisco’s literature should not be taken to mean the same thing as unmanaged. Cisco 2950 switches run the IOS and are fully manageable from the CLI or through various GUI tools provided by Cisco. The 2950 series of switches is also discontinued and replaced with the 2960; however, they too are still excellent as a lab switch.

Figure 4.36: Cisco 2950 Switch

The Cisco switches presented here are for illustration purposes only. HP, Aruba Networks, Juniper Networks®, Dell™, and others make excellent switches, as well.

Common tasks required to configure switches for use in VoIP networks include:

- Configuring VLANs for WLAN operations
- Configuring the switch ports for access

- Configuring QoS settings

The following commands represent typical operations on a Cisco 2950 switch:

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface fastethernet0/4
Switch(config-if)#switchport mode access
Switch(config-if)#?
  cdp               Global CDP configuration subcommands
  channel-group     Etherchannel/port bundling configuration
  channel-protocol  Select the channel protocol (LACP, PAgP)
  description       Interface specific description
  duplex            Configure duplex operation.
  exit              Exit from interface configuration mode
  mac-address       Manually set interface MAC address
  mls               mls interface commands
  no                Negate a command or set its defaults
  shutdown          Shutdown the selected interface
  spanning-tree     Spanning Tree Subsystem
  speed             Configure speed operation.
  storm-control     storm configuration
  switchport        Set switching mode characteristics
  tx-ring-limit     Configure PA level transmit ring limit
Switch(config-if)#cdp enable
Switch(config-if)#mls ?
  qos  qos command keyword
Switch(config-if)#mls qos trust ?
  cos     cos keyword
  device  trusted device class
  dscp    dscp keyword
  <cr>
Switch(config-if)#mls qos trust device cisco-phone
Switch(config-if)#exit
```

So how does the switch work its magic? The first thing that you need to know is that a switch is a learning device. As data comes in and out of the switch, it notices the MAC address of the sending device as it transmits data through a particular port. Since the device sent data to the switch through that port, the switch knows that it can reach the device (or its MAC address) through that same port. This learning process is repeated

again and again, and it forms a database in memory that tracks the various MAC addresses and the ports through which they can be reached.

Now, when a frame comes into the switch destined for a known MAC address, the switch forwards that frame to the appropriate port. When a frame comes into the switch destined for an unknown MAC address, the switch floods the frame to all ports. In the end, a switch is effectively a multiport bridge. The traditional (and now obsolete) basic network bridge had two ports in most implementations. One port existed on one network, and the other port existed on another. Each port learned the MAC addresses on that side of the bridge, and the bridge only forwarded frames from one side to the other that were actually destined for a device on the other side. Switches implement the same basic functionality, only there are multiple “virtual bridges” within the switch. In fact, most switches state that they support the IEEE 802.1D standard, which is not a switching standard but is rather a bridging standard.

Just like routers, and all other computing devices, a switch is a computer.

IP Routers

The routers used for network services are sometimes also called integrated services routers (ISRs). As an example, Cisco has offered several router series over the years. Older Cisco equipment, including 1700 series, 2600 series, and 3600 series routers can still be used to implement and test WLAN labs. The newer 800, 1800, 2800, and 3800 series of routers can also be used for WLAN services. The 800 series is really only useful in routing WLAN packets on a network as no WLAN services can be managed on the router itself. The 1800 through 3800 series routers can perform additional operations like VoIP implementation with a call manager. Figure 4.37 shows the Cisco 2851 router with an IP phone and AIM-CUE card for Cisco Unity Express implementation showing the flexibility of an ISR.

Note: **One of my favorite Cisco routers is the 2801 ISR even though it is at its end-of-life (you can still acquire them used). This router can be used for just about any learning you need to do with modern Cisco exams and CWNP exams. You can implement security features, voice features, the Security Device Manager, Call Manager Express, and much more with this entry-level 2800 series device. It has four expansion slots, support for onboard PVDM modules, Compact Flash based memory (for IOS storage), and two built-in Fast Ethernet ports.**

Figure 4.37: Cisco 2851 Router with IP Phone and AIM-CUE Unity Express Card

The common tasks performed by Cisco routers in a WLAN network include:

- Performing IP routing
- Acting as a DHCP server or relay agent
- Filtering traffic based on destination ports and IP address ranges
- Implementing Layer 3 QoS

To help you understand what a router really is and does, consider that a router is nothing more than a computer. If you were to install two Network Interface Cards (NICs) in a single computer and then connect one NIC to one network and the other NIC to another network, your computer could be configured to route between the two networks. The Windows operating system has had routing capabilities in it since the early Windows NT days, and Linux systems have this capability, as well. In fact, there are a few routers on the market that actually run an embedded and scaled-down specialized version of the Linux operating system.

While most computers have hard drives, memory chips (RAM), and a processor, most routers have non-volatile random access memory (NVRAM), memory chips (RAM), and a processor or set of special processors. Computers use the hard drive to store permanent information that needs to be retained between boots, and routers use the NVRAM for this purpose. This difference allows the routers to boot quickly and, probably more important, reboot quickly. It also reduces moving parts that are common points of failure. In comparison to computers, network routers very rarely fail. Even a consumer-grade router, such as one from Linksys, will usually work for well over ten years; however, most

computers do well if they make it four or five years without minimally needing a hard drive replaced. Notice what it is that is most likely to fail: the hard drive. This problem is why the NVRAM is so beneficial.

A dedicated device has at least two major benefits. First, the processing will most likely be faster, since it is dedicated to the process of routing. Second, the up time will most likely be greater, since you will have to perform fewer upgrades and you will experience fewer hardware failures (remember, non-moving parts). On the first point the processing will not only be faster because the entire device is dedicated to routing, but also because the software is optimized for that purpose. With a regular PC running an operating system that supports routing, the operating system is most likely doing many unnecessary tasks unrelated to routing.

Routers, in most cases, route IP traffic. Where does the IP protocol operate in the OSI mode? It operates at Layer 3 or the Network layer. This tells you that a router is a Layer 3 device. Routers are most commonly used to connect switches, which are Layer 2 devices in most implementations, together to form larger networks than could be otherwise created. It is important to know that some routers can perform switching with added components and some switches can perform routing. However, for our purposes here, we'll treat the two as completely separate devices and ignore the customized modern routers and switches offered by today's vendors.

As I stated previously, routers perform their most important tasks at Layer 3. This layer is where the IP protocol operates, and in today's networks IP routing is the primary function of a Layer 3 router. It is very useful for you to understand how a router works its magic. It all begins at Layer 1 and it ends at Layer 1, as well. To understand this concept, consider Figure 4.38. The router in this figure has two interfaces, one on the address of 10.10.10.100 and the other on the address of 10.10.10.200. Using a subnet mask of 255.255.255.128, this means that IP addresses from 10.10.10.1-10.10.10.127 are on the 10.10.10.100 interface, and addresses from 10.10.10.128-10.10.10.254 are on the 10.10.10.200 interface. When the computer at 10.10.10.1 seeks to communicate with the computer at 10.10.10.201, it must do so through the router—its default gateway.

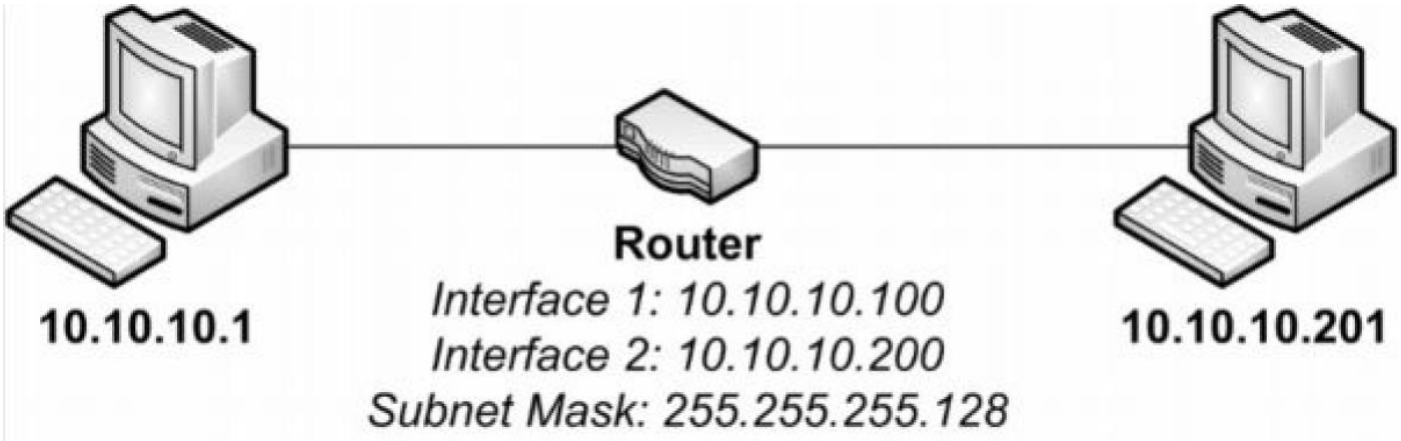


Figure 4.38: The Router at Work

The work of a router can be summarized as follows:

1. Receive incoming frames on each interface.
2. Extract the IP packet from the incoming frame.

3. Evaluate the IP header in order to determine the destination of the packet.
4. Look in the routing table to determine the best route to the destination.
5. Encapsulate the IP packet inside a new frame and transmit it on the interface that connects to the next step in the route.
6. Process the next received frame.

As you can see, the process is really quite simple. The router must remove the preamble, the MAC frame header, and the FCS from the Ethernet frame, which results in the original IP packet. This original IP packet will remain the same as it moves from source to destination as long as no dynamic tagging is used. The header of the IP packet contains the destination address as well as the source address. The router can use the destination address to determine the best way to reach the network on which that destination address exists. To do this task, it will use its routing table.

The router's routing table is a listing of known networks and the routes to those networks. The simplest routing table may look something like Table 4.1. Each entry will contain an IP address and a subnet mask. These two values are used to determine a destination network. The same IP address can be listed multiple times with different subnet masks and would result in different networks based on the configuration of the subnet masks. The Via column in the sample table represents the "way to the destination" network or host. For example, based on this routing table, if the router received an IP packet destined for 192.168.15.73, it would forward that packet on to 192.168.5.2. Now considering the subnet mask, we know that 192.168.15.73 is not on the same network as 192.168.5.2, but that node (which is another router) knows how to get to the destination address.

IP Address	Subnet Mask	Via
192.168.13.0	255.255.255.0	192.168.5.1
192.168.15.0	255.255.255.0	192.168.5.2
192.168.20.0	255.255.255.0	192.168.5.2

Table 4.1: Example of a simple routing table

These routing tables can be built manually or automatically. If they are built manually, they are said to be static routes, and if they are built automatically, they are said to be dynamic routes. Static routes are entered by an administrator who understands the structure of the network. The benefit of static routes is that they give you, the administrator, full control over the routing process. The problem with static routes is that they must be manually modified anytime the network changes. This task can become time consuming and burdensome.

This is where routing protocols come into the overall network picture. Don't get confused about the phrase routing protocol. A routing protocol is a protocol that discovers the

neighbor networks around a router and dynamically builds the routing table for IP to utilize in routing decisions. The key is to remember that a routing protocol does not perform routing. IP is in charge of the actual routing, but the routing protocol provides the information to IP so that it can make the best decision. There are many routing protocols, but the most popular are:

- BGP
- IS-IS
- OSPF
- IGRP
- EIGRP
- RIP

Routing protocols are often categorized as either interior or exterior. Of those listed, only the Border Gateway Protocol (BGP) is considered an exterior routing protocol. BGP is used for routing on the Internet and is a distance-vector routing protocol. Distance-vector protocols choose the best route based on how many hops or routers the packet will have to pass through in order to reach the destination.

IS-IS (Intermediate System to Intermediate System) is an interior routing protocol (interior routing protocols are used within local networks) and is a link-state protocol as opposed to a distance-vector protocol. Link-state protocols actually look at the state of a connection. For example, is the link up or down? Additionally, link-state protocols can usually measure the quality and the speed of the link to truly find the best route. For this reason, in enterprise networks, link-state protocols are often preferred over distance-vector protocols.

OSPF (Open Shortest Path First) is another link-state interior routing protocol. It borrows some of its features from IS-IS and is probably the most popular link-state protocol in use on modern networks.

Both IGRP (Interior Gateway Routing Protocol) and EIGRP (Enhanced IGRP) are distance-vector routing protocols that were developed by Cisco. Technically, EIGRP is a hybrid routing protocol as it takes the best from the link-state and distance-vector protocols and combines them. In a pure Cisco-routed environment supporting EIGRP, it is usually the best routing protocol to use. IGRP was created in the 1980s by Cisco to overcome some of the limitations of the RIP protocol, which was and is limited to having 16 hops in a route. This limitation affected the overall size of the network. Additionally, RIP supported only a single metric: hop count. IGRP added new metrics such as internetwork delay and load. This addition makes the route calculation similar to a link-state protocol. EIGRP is simply an enhanced version of IGRP that was created in the 1990s to improve efficiency. The biggest change is in the fact that EIGRP does not send out a periodic update to all neighboring routers of its routing table. It instead discovers neighbors and communicates with them directly, greatly improving network efficiency.

RIP, the Routing Information Protocol, is one of the oldest distance-vector routing protocols still in use today. RIP and RIPv2 are excellent solutions for small networks with two or three routers. The big problem with using them in larger networks is that they do

send periodic broadcasts to all neighboring routers, whether anything has changed in the routing tables or not. This design is not very efficient. Also, both versions are limited to 16 hops in a route. This number limits the size of the network to medium-sized organizations anyway. Those medium-sized organizations would be much better served by OSPF or EIGRP and should avoid RIP.

Servers and Services

The final components provided by the wired network are the servers and services. These include:

- *DNS servers:* used to resolve domain names to IP addresses and IP addresses to domain names; also used to locate services on the network.
- *DHCP servers:* used to provision the IP configuration for requesting devices including IP addresses, subnet masks, default gateways, DNS servers, domain names, and various options.
- *Identity servers:* used to store authentication information for users and devices on the network.
- *Certificate servers (public key infrastructure (PKI)):* used to issue and manage certificates, which are used for encryption and authentication purposes.
- *Monitoring servers:* used to log events and notify personnel of important issues and concerns.
- *Database servers*: used to store data for many other systems including identity servers, monitoring servers, and reporting servers.
- *Reporting servers*: used to generate reports that may be readable on multiple platforms such as Windows, Linux, Mac OS X, and web-based interfaces.
- *NTP servers:* used to centrally manage time synchronization by providing a location where all other devices can retrieve the correct time.

All of these servers and services play a key role in WLAN network operations. More details are provided on many of these servers and services in Chapter 7.

Chapter Summary

In this chapter, you learned about the important hardware in WLANs. This includes client devices, APs, controllers, analysis hardware, and wired network devices. With this information, you can better troubleshoot problems on the WLAN.

Review Questions

1. What does it mean to say that a client is dual-band?
    a. It supports both 802.11n and 802.11g.
    b. It operates in the 2.4 GHz and 5 GHz frequencies.
    c. It supports both USB and PC Card interfaces.
    d. It has two antennas.
2. Where can you find the FCC ID for a search at the FCC website?
    a. In vendor literature
    b. In the centralized FCC database
    c. On the device
    d. On the chipset
3. What adapter form factor is commonly used for both laptops and desktop and for protocol analysis?
    a. USB
    b. PCIe
    c. CF
    d. SD
4. What problem may occur that is common with PCI cards acting as WLAN adapters in desktop computers but is not likely to happen with USB adapters?
    a. The antennas are behind the computer, under the desk, and against a wall.
    b. The client drivers are not supported in the operating system.
    c. The Windows supplicant cannot use it.
    d. The software does not support WPA2.
5. What must occur to use an AP as a lightweight AP when it ships as an autonomous AP in most cases?
    a. Firmware change
    b. IP address change
    c. MAC address change
    d. Nothing
6. When an AP is implemented to connect to networks, in what operational mode is it functioning?
    a. Bridge
    b. Root

c. Repeater

d. Announcer

7. What is a major drawback introduced when using an AP as a repeater?

a. Reduction in coverage area

b. Reduced CCI

c. Reduced throughput

d. Reduced output power

8. Which one of the following PHY devices will be unable to connect to an 802.11ac radio?

a. HT

b. OFDM

c. ERP

d. VHT

9. While MAC filtering in APs provides little in the way of security, for what can it be used?

a. Management purposes

b. Filtering out unwanted PHYs

c. Filtering out unwanted IPs

d. Filtering out unauthorized Ethernet devices on the wired side

10. What advantage is provided by APs with variable output power settings?

a. Security enhancement

b. Cell sizing capabilities

c. Reduction in human health threats

d. Gaining access to power levels beyond regulatory constraints

11. When implementing 802.11ac APs, what minimum Ethernet speed should be provided?

a. 10 Mbps

b. 100 Mbps

c. 1 Gbps

d. 10 Gbps

12. When troubleshooting problems that may involve AP stability issues, what advantage may be provided by PoE?

a. More syslog data

b. Better frame captures

c. Restarting APs

d. Increasing power to APs

13. What Wi-Fi Alliance certification provides support specifically for hotspots?

    a. Passpoint

    b. WPA2

    c. WMM

    d. GuestSpot 2.0

14. When using Web-based administration to administer APs and controllers, what protocol should be used?

    a. HTTPS

    b. FTPS

    c. sFTP

    d. SSH

15. What part of an AP spec sheet can help you understand the coverage provided by the AP when included in the sheet?

    a. Ports

    b. Security

    c. Antenna patterns

    d. Standards

16. If a device spec sheet does not reference some of the information you want to know about the device, what other source might be helpful?

    a. Wi-Fi Alliance product finder

    b. Other vendor spec sheets

    c. Other vendor FAQs

    d. RFCs

17. Instead of opening a device to see the internal components and voiding the warranty, how can you view the internal components of an AP?

    a. Wi-Fi Alliance product finder

    b. Spec sheet

    c. Antenna pattern charts

    d. FCC ID search

18. When a device reports 3x3:3 MIMO, what does this indicate?

a. The device can use three spatial streams concurrently.

b. The device has three antennas but may not support three spatial streams.

c. The device has three antennas but may not have three radios.

d. The device has three radios but may not have three antennas.

19. When a device lists a transmit power of 17 dBm, what does this equal in mw?

a. 50

b. 60

c. 100

d. 1000

20. Why is the receiver sensitivity chart important in WLAN analysis?

a. It helps you determine the output power of the AP.

b. It allows you to determine the signal strength required for a given data rate or MCS.

c. It allows you to determine the best antenna.

d. It helps you understand the modulation used for noisy environments.

21. Given that a WLAN controller has eight Ethernet ports, how many APs can it support?

a. 4

b. 8

c. 16

d. Unknown – the number of APs is a factor of licensing and processing capabilities

22. What form factor is the most commonly used for spectrum analysis hardware used with laptops today?

a. PCIe

b. Mini-PCIe

c. USB

d. SD

23. In addition to a supported 802.11 adapter, what device could be used to capture 802.11 frames for analysis?

a. AP

b. Ethernet switch

c. IP router

d. Firewall

24. What is a common service provided by Ethernet switches to WLAN APs?
    a. IP routing
    b. Layer 3 QoS
    c. Call management
    d. PoE
25. What is a common service provided by IP routers to WLAN APs and attached STAs?
    a. DNS resolution
    b. DHCP relay
    c. VLAN management
    d. Direct server service access

Review Question Answers

1. **B** is correct. A dual-band adapter works in both 2.4 GHz and 5 GHz. It can support either ERP/HT in 2.4 GHz or OFDM/HT/VHT in 5 GHz, but not both at the same time. A dual-band AP can support both at the same time because it has two radios.
2. **C** is correct. The FCC ID is listed on the device. It may be on a visible label outside the case, or you may have to disassemble the device to see it internally.
3. **A** is correct. USB adapters are the only ones commonly used across all three listed scenarios: desktops, laptops, and protocol analysis.
4. **A** is correct. Because PCI cards are inserted into the motherboard, and the antennas then protrude out the backside of the computer. The antennas often end up under the desk and against a wall, which can diminish link quality.
5. **A** is correct. A firmware change is typically required to use an autonomous AP as a lightweight AP when it supports this conversion.
6. **A** is correct. In bridge mode, the AP is used to connect two networks. In root mode, it acts as a standard BSS AP. In repeater mode, it acts as a client to another AP and as an AP to clients.
7. **C** is correct. When using an AP as a repeater, network throughput is greatly reduced as clients connected through the repeater causing all frames to be transmitted twice.
8. **C** is correct. The ERP PHY operates only in 2.4 GHz and 802.11ac operates only in 5 GHz, so an ERP PHY device could not connect to an 802.11ac radio.
9. **A** is correct. MAC filtering can be used for management purposes to control the devices that can even try to connect from a basic perspective; however, even this becomes unmanageable in larger networks.
10. **B** is correct. Variable output power allows for cell sizing. To increase the size of the cell, increase the output power within reason. To reduce the size of the cell, reduce the output power. Remember, however, that the cell should be designed to accommodate the clients. Too much output power can result in a link mismatch that can cause problems.
11. **C** is correct. Due to the potential for throughput in excess of 100 Mbps, 1 Gbps Ethernet connections should be used.
12. **C** is correct. When PoE is provided through a managed switch (and not an unmanaged switch or PoE injector), the WLAN analyst can cycle the AP by stopping and starting power provisioning on the attached port.
13. **A** is correct. Passpoint provides for hotspot support.
14. **A** is correct. HTTPS should be used so that all traffic is encrypted. Without this, HTTP sends traffic with clear text information that could cause data leakage.
15. **C** is correct. Antenna patterns are not always provided, but when they are they can

help you understand the likely coverage provided by the AP.

16. **A** is correct. In addition to the spec sheet, you can learn more from the Wi-Fi Alliance, FCC ID searches, and chipset manufacturers.
17. **D** is correct. Performing an FCC ID search allows you to see the internals of a device without opening it and possibly voiding the manufacturer's warranty.
18. **A** is correct. The 3x3:3 nomenclature indicates three transmit chains, three receive chains, and three spatial streams in that order.
19. **A** is correct. 17 dBm is 50 mw. Remember the rules of 10s and 3s from CWNA studies. 0 dBm equals 1 mw. Therefore, 10 dBm equals 10 mw, 20 dBm equals 100 mw, and 17 dBm equals 50 mw.
20. **B** is correct. Receiver sensitivity information tells you the signal strength required to achieve a given data rate or MCS. Therefore, to design or repair a network to achieve such a data rate, you should learn the device receive sensitivities on your network and design around them.
21. **D** is correct. A WLAN controller can have one port and still support dozens of APs. The number of APs supported is not a factor of the number of ports, but of the licenses and processing power of the controller.
22. **C** is correct. USB is now the most common form factor for spectrum analyzer hardware.
23. **A** is correct. Many APs now have protocol capture capabilities built into them.
24. **D** is correct. Switches provide PoE, Layer 2 QoS, VLAN management and standard Ethernet connectivity to WLAN APs.
25. **B** is correct. Routers provide IP routing, security, DHCP relay, DHCP server, and other functions to WLAN APs and attached STAs.

Chapter 5:

Protocol Analysis

Objectives

3.4 Describe and implement WLAN analysis hardware for protocol analysis and spectrum analysis.

4.1 Describe the common functionality and features of protocol analyzers.

4.2 Demonstrate the ability to install, configure and use a protocol analyzer to capture and analyze WLAN traffic.

4.3 Demonstrate the ability to use a protocol analyzer to capture the appropriate wired traffic related to WLAN operations.

A protocol analyzer is a primary tool for the WLAN analyst. It is used to evaluate wireles network performance, operations and problems. On the wired side, it is used to locate sources of configuration errors, throughput delays, and communication problems. Without a protocol analyzer and sufficient knowledge to use it, the WLAN analyst would be hindered significantly.

This chapter provides discussion of WLAN-specific protocol analyzers, and protocol analyzers in general. It explores the hardware required to perform analysis, essential software, and the processes used to capture and analyze traffic. The first step is understanding the hardware and software required to perform analysis.

WLAN Analysis Hardware and Software

A protocol analyzer allows you to capture and analyze network traffic. It can be as simple as a tool used to view individual frames and packets with decodes, or as complex as those WLAN-specific tools that offer expert modules for performance analysis, troubleshooting, and security compliance monitoring.

WLAN analysis begins with acquiring the right hardware and software to do the job. Many options exist, but they all come down to a threefold combination:

1. The operating system
2. The software
3. The hardware

First, you must determine the operating system on which the protocol analyzer will run. Today, for most people it is either Windows, MAC OS X, or Linux. Then you to choose software that works on your operating system. However, in addition to the software, you must have specific capture hardware that works with that software on that operating system. The three work together.

For example, Savvius OmniPeek® wireless protocol analyzer software works on Windows, but it may be able to run on a virtual machine in the MAC OS X or Linux platforms. Wireshark works on Windows, but it is harder to find adapters that work with it for analysis, particularly three stream adapters supporting 802.11n or 802.11ac. But if you run Wireshark on Linux, it may be easier to perform protocol captures. The MAC OS X operating system can perform protocol captures natively and then you can open the captures in virtual machines. As you can see, the options are many and nuanced.

In the next two subsections, you will explore the hardware and software for protocol analysis, and learn tips for using them on various operating systems.

Protocol Analysis Hardware

Protocol analyzers fall into three primary categories:

- Mobile

- Infrastructure
- Distributed

Figure 5.1 illustrates these three analyzer types.

Mobile analyzers are laptop-based (or desktop-based when viewing and analyzing captures from other sources) and require a combination of software for capturing network data and hardware that can pass the data to the software. In some cases, internal WLAN adapters can be used to capture the traffic. In others USB-based adapters will be used. It is far more common to use USB-based adapters today because the WLAN analyst can choose an adapter that meets his or her needs.

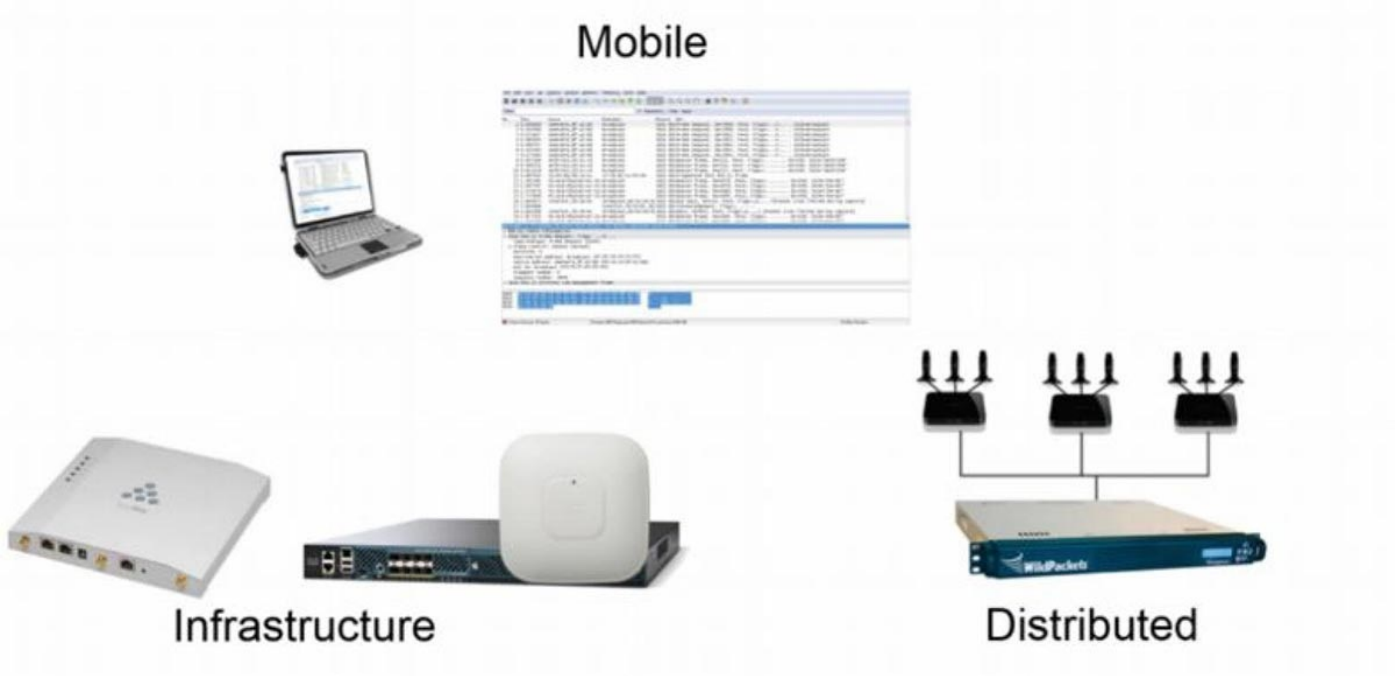


Figure 5.1: Three Types of Protocol Analyzers

When selecting hardware for mobile analysis, the following must be considered:

- **Support in the software and operating system:** the adapter must be supported by both the operating system and the capture software. It is important to remember that you can capture WLAN frames and higher-layer packets with a separate software program from the analysis software. So, if the analysis software you prefer to use does not support a given adapter, performing external capture may be an option. If you want to view live statistics and analysis dashboards in the protocol analyzer, a supported adapter must be used.
- **PHY and MAC support:** The adapter must support the physical and MAC layers you want to analyze. For example, you cannot perform proper 802.11ac analysis with an 802.11n adapter.
- **Number of streams:** At the time of this writing, three-stream transmissions are the highest common denominator in most implementations; however, in 2016 and later, we will see four-stream transmissions. As new technology emerges, having a capture solution that supports the number of streams and the PHY/MAC layers is key to seeing the whole WLAN story.
- **Hardware interface:** The last piece of the puzzle is the hardware interface. This is

typically either USB or integrated. For example, MacBook Pro laptops include 802.11ac 3x3:3 adapters internally that can capture 802.11ac traffic. Windows-based systems may include internal adapters that can capture as well. Many analysts choose to use USB adapters for the flexibility and control of options they provide.

Infrastructure analysis depends on the APs to capture the WLAN frames, and then they are either made available from the AP or controller to your WLAN analysis software. Capturing the newest frame types on your WLAN is easier with an AP simply because the only frame types that can successfully traverse your WLAN are those supported by your AP. However, capturing at the AP does not always reveal the information you need to properly analyze WLAN problems. I will explain capture location selection in more detail later in this chapter. For now, know that infrastructure analysis is not a complete solution, but it can be very useful in addition to mobile analysis. In fact, you may find that the majority of the time, the information gathered from infrastructure analysis is sufficient for the scenario.

Distributed analysis uses multiple sensors (capture devices) distributed throughout the organization's WLAN coverage area. These sensors can be APs, laptops with the software installed, or dedicated devices used to capture the information. Distributed analysis makes roaming analysis easier and gives a better picture of the overall WLAN activity in your environment.

Now that I have briefly described the three primary analysis hardware options, consider the following scenario. You want to capture and analyze within AirMagnet Wi-Fi Analyzer Pro, which is a WLAN-specific protocol analyzer. You will use a laptop running Windows 8.1 to perform the capture and analysis. You want to capture 3x3:3 802.11ac frames for some scenarios, but simply capturing beacons is sufficient for some compliance analysis as well. Let us walk through this scenario and see how you would build out a protocol analysis solution, from a hardware perspective, that meets your needs.

The first step is to explore the supported adapters or capture hardware that may work for AirMagnet Wi-Fi Analyzer Pro in a 3x3:3 capture scenario. A visit to the Fluke Networks® website reveals the information in Figure 5.2. This is a partial screen capture of the driver download section of the MyAirMagnet web portal. The information shows that the only adapter supporting 802.11ac 3x3:3 capture is the Express Card adapter sold by Fluke Networks. This adapter works very well, but it requires two things: the purchase of the adapter and a laptop with an Express Card slot. Given that such laptops are less common today, this introduces a challenge. If you do not have such a laptop, you will be forced to purchase one just to capture the 802.11ac frames you desire.

File	Format	Description
AirMagnet 802.11ac 3x3 Express Card Adapter Driver	EXE	Driver software for the AirMagnet 802.11ac 3x3 Express Card Adapter for Windows 7, 8, and 8.1 64-bit.
AirMagnet Multi-Adapter Kit Drivers	EXE	Read-me documents and software package for Proxim 8494 802.11a/b/g/n USB adapters as part of the WiFi Analyzer and Survey multi-adapter kit. Driver supported for 32-bit (Windows XP, Vista, Window 7, Window 8 only for Proxim USB) and 64-bit OS (Windows 7, Window 8 only for Proxim USB) Window 8.1 64-bit for Survey PRO/Express/Planner Only
802.11a/b/g/n USB adapter drivers	EXE	Software Package for the following adapters: - Proxim 8494 802.11a/b/g/n USB adapter - Ubiquiti SR-71 USB - D-Link Xtreme N Dual Band (DWA-160) H/W ver. A1 and A2 - Netgear RangeMax Dual Band WNDA3100v1 Wireless-N USB 2.0 Adapter Driver supported for 32-bit (Windows XP, Vista, Windows 7, Windows 8 Only for Proxim USB) and 64-bit OS (Windows 7 only, Window 8 only for Proxim USB) Window 8.1 64-bit for Survey PRO/Express/Planner Only

Figure 5.2: Adapter Information for AirMagnet Wi-Fi Analyzer Pro

The information may compel you to use a different software analyzer, or to capture using different software and only analyze the captures using Wi-Fi Analyzer Pro. For example, if you have a MacBook Pro® laptop, you could capture the frames using its capabilities and then open the capture in a virtual machine running Wi-Fi Analyzer Pro. However, if you are required to stick with the scenario and capture and analyze in the software, you will have to acquire a laptop with an Express Card slot and also purchase the Express Card adapter from Fluke Networks. The Express Card adapter is shown in Figure 5.3.

Figure 5.3: Fluke Networks Express Card 802.11ac Capture Adapter

Alternatively, you could get an inexpensive AP that can capture the 802.11 frames desired for Wi-Fi Analyzer Pro. The Cisco WAP371, discussed in the last chapter (and again later in this chapter), is a good example of one of these APs. However, this introduces new problems in mobility. The AP will have to be taken to the capture location and powered. Three options really exist for this:

1. **Use wall outlet power at the location:** with this option, you can simply connect the laptop to the Ethernet port of the AP and begin capturing frames. The downside is that your mobility is degraded as you must now take the laptop, AP and power cable with you to the location.

2. **Use a PoE injector at the location:** with this option, you are doing the same thing as option 1, but using a PoE injector to power the AP. The downside is the same, though. When an Ethernet port is available, you could connect the AP to the Ethernet port and go back to your work area to connect to it and perform the

capture.

3. **Use available PoE drops at the location:** this option is the best, when available. Power the AP at the location and then go back to your work area to connect to it and perform the capture. You do not have to physically take the laptop on location, but you are capturing at that location.

As you can see, choosing a protocol capture solution is not a simple matter of just buying software and starting to capture. You must have the right combination of hardware, software, and operating system.

Protocol Analysis Software

Selecting the protocol analysis software is an important step. Your requirements will drive the software selection. The following are common possible requirements of the WLAN analyst:

- Capture the latest frames traversing the WLAN.
- Capture at multiple locations.
- Provide accurate decodes of the 802.11 frames.
- Provide dashboards on performance, errors, and compliance.
- Provide troubleshooting experts.
- Provide reporting capabilities.
- Operate on the appropriate operating system.

As with the hardware selection process, the software selection is more complex than it may appear. If all you want to do is look at frame decodes, Wireshark is free and will likely meet your needs (as long as you can capture the proper frames). To be clear, the range of protocol analysis software features is large, and it is best to evaluate different solutions before making a decision. The primary software solutions for laptop-based analysis include:

- Wireshark
- Savvius OmniPeek
- Fluke Networks Wi-Fi Analyzer Pro
- TamoSoft Commview for Wi-Fi

Other software vendors exist, and many AP vendors include some level of frame analysis in their APs and controllers, but these four are the most commonly used applications by today’s WLAN professionals.

AirMagnet Wi-Fi Analyzer Pro lists the following benefits at the time of writing:

- Real-time accurate, independent, and reliable analysis of 802.11a/b/g/n and ac wireless networks, including 3 X 3 802.11ac wireless network analysis without missing any traffic

- Highly-portable wireless network analyzer that travels to the source of the wireless network troubleshooting problems enabling faster and accurate fault-finding without any AP downtime
- Dedicated Wi-Fi network monitoring and troubleshooting software solution guaranteeing any wireless network fault detection as compared to “time-slicing monitoring functionality” built inside the wireless network infrastructure
- Reduce IT costs, simplify workload and minimize user complaints by obtaining instant answers to ANY wireless network connectivity, Wi-Fi signal strength, wireless network performance, roaming, interference* and wireless network security issues using the AirWISE intelligence engine
- Unique active toolset to isolate and troubleshoot Wi-Fi connectivity and monitor wireless network performance issues
- Strengthen your wireless network security by monitoring, detecting, and eliminating any wireless network threats and vulnerabilities
- Auditor-ready Wi-Fi Security compliance reporting for multiple verticals including wireless PCI compliance, SOX, ISO, and many more
- Troubleshoot BYOD induced performance and monitor wireless network security issues

OmniPeek lists the following benefits at the time of writing:

- Analyze and troubleshoot local traffic
- Analyze and troubleshoot traffic captured by OmniPeek Software probes at remote locations—across the hall, across campus, or across the country
- Quickly view lists of top talkers, top protocols, and other at-a-glance statistics
- View a Peer Map that graphically represents all conversations between nodes on the network
- Gain unprecedented visibility into networks and applications
- Accelerate Mean-Time-To Resolution (MTTR)
- Discover and close network security gaps
- Maximize ROI on existing networks and applications
- Increase IT efficiency and responsiveness
- Reduce costs associated with network downtime and service degradation
- Reduce IT labor costs
- Increase end user productivity

CommView for WiFi lists the following benefits at the time of writing:

- Scan the air for Wi-Fi stations and access points
- Capture 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac WLAN traffic

- Specify WEP or WPA keys to decrypt encrypted packets
- View detailed per-node and per-channel statistics.
- View detailed IP connections statistics: IP addresses, ports, sessions, etc.
- Reconstruct TCP sessions
- Configure alarms that can notify you about important events, such as suspicious packets, high-bandwidth utilization, unknown addresses, rogue access points, etc.
- View protocol “pie” charts
- Monitor bandwidth utilization
- Browse captured and decoded packets in real time
- Search for strings or hex data in captured packet contents
- Log individual or all packets to files
- Load and view capture files offline
- Import and export packets in Sniffer®, EtherPeek™, AiroPeek™, Observer®, NetMon, Tcpdump, hex, and text formats
- Export any IP address to SmartWhois for quick, easy IP lookup
- Capture data from multiple channels simultaneously using several USB adapters
- Capture A-MPDU and A-MSDU packets
- Simulate access points

A quick review of the benefits of each tool reveals that, while the language may be different, the three primary contenders for your protocol analysis purchase all offer the same primary features. They typically differentiate in the areas of troubleshooting expert modules, reporting, and support for adapters.

A key factor in the selection process is the list of supported adapters. CommView for WiFi has traditionally supported more adapters and provides simpler reporting functions. OmniPeek and Wi-Fi Analyzer Pro support fewer adapters and provide more complex “experts” and reporting functions. Figure 5.4 shows a partial list of the 802.11ac adapters supported by CommView for WiFi. Consider that, at the time of this writing, OmniPeek and AirMagnet support only 1–2 802.11ac adapters.

802.11ac Adapters

Adapter	802.11 Bands	Form Factor	Supported OS	Limitations or Comments	Sensitivity on a 1-5 scale
Belkin F9L1109 v1	2.4 GHz/5 GHz	USB	Windows 7 or higher	Recommended See tech. notes	4
Buffalo AC866 (WI-U2-866D)	2.4 GHz/5 GHz	USB	Windows 7 or higher	See tech. notes	4
D-Link DWA-180 rev A1	2.4 GHz/5 GHz	USB	Windows 7 or higher	See tech. notes	4
D-Link DWA-182 rev A1	2.4 GHz/5 GHz	USB	Windows 7 or higher	See tech. notes	4
D-Link DWA-182 rev C1	2.4 GHz/5 GHz	USB	Windows 7 or higher	Recommended See tech. notes	5
Edimax EW-7822UAC BEST	2.4 GHz/5 GHz	USB	Windows 7 or higher	Recommended See tech. notes	5
EnGenius EUB1200AC	2.4 GHz/5 GHz	USB	Windows 7 or higher	See tech. notes	3
Intel AC 7260	2.4 GHz/5 GHz	Integrated	Windows 7 or higher	Recommended See tech. notes	Not rated *
Intel AC 7265	2.4 GHz/5 GHz	Integrated	Windows 7 or higher	Recommended See tech. notes	Not rated *
Linksys WUSB6300 BEST	2.4 GHz/5 GHz	USB	Windows 7 or higher	Recommended See tech. notes	4
NETGEAR A6200	2.4 GHz/5 GHz	USB	Windows 7 or higher	See tech. notes	4
Proxim ORiNOCO 9100 BEST	2.4 GHz/5 GHz	USB	Windows 7 or higher	Recommended See tech. notes	5
Qualcomm Atheros 61x4 and 988x	2.4 GHz/5 GHz	Integrated	Windows 7 or higher	Recommended	Not rated *
TP-LINK Archer T4U	2.4 GHz/5 GHz	USB	Windows 7 or higher	See tech. notes	4
TRENDnet TEW-805UB	2.4 GHz/5 GHz	USB	Windows 7 or higher	See tech. notes	3
ZyXEL AC240 BEST	2.4 GHz/5 GHz	USB	Windows 7 or higher	Recommended See tech. notes	5

Figure 5.4: Supported 802.11ac Adapters with CommView for WiFi

EXAM MOMENT: When selecting an adapter for capture, it must support the number of spatial streams and the PHY/MAC layers you wish to capture. If it does not, you will be able to capture some information (such as beacon frames), but not the detailed information needed for analysis.

Protocol Analysis

Performing actual protocol analysis involves selecting the right physical and logical location, capturing traffic to a capture file or memory, and using the protocol analyzer tools to analyze the traffic. This section provides the knowledge required to perform these actions on a WLAN. First, you will explore common features of protocol analyzers—those that are in all protocol analyzers including Wireshark. Then you will explore the basic installation and configuration processes, and finally you will learn to capture and analyze the traffic.

Common Features

All protocol analyzers supporting WLAN capture and analysis share at least four common features:

- Frame capture
- Frame decoding
- Highlighting or Filtering
- Expert Analysis

The following subsections provide explanations of these features.

Frame Capture

The fundamental capability of a protocol analyzer is frame capture (or packet capture). I use the term frame capture because, if a solution cannot capture the frames but only the higher-layer packets, it is not a true WLAN protocol analyzer and provides little value for direct WLAN analysis. All of the expert analysis features of protocol analyzers depend on frame capture. If frames cannot be captured, the analyzer is helpless to provide information.

Frame capture can be performed in two ways. The first is non-promiscuous, which means that only the frame to and from the capturing device can be seen. This mode provides value in some lab scenarios, but it provides little value in troubleshooting real-world problems.

The second is promiscuous mode, which means that all frames are captured regardless of the source and destination. This mode provides a complete (or as complete as possible from the location of the analyzer) picture of the WLAN activity. Promiscuous mode is also called monitor mode, but monitor mode indicates that the lower-layer frames are passed up to the decoder and may apply in non-promiscuous mode as well. Therefore, an adapter that supports promiscuous mode and monitor mode on your operating system and with your analyzer is needed to perform 802.11 frame capture.

WLAN protocol analyzers can capture on a single channel or on all supported channels of the adapter (you control this in configuration). When they capture on all supported channels, you will lose information, but get an overall picture of WLAN activity at the capture location.

Multiple channel capture is sometimes called channel scanning as it scans a channel, moves to the next, performs another scan, moves to the next and so on. This capture method builds excellent information for expert dashboards, which are provided in Wi-Fi Analyzer Pro, OmniPeek and CommView for WiFi.

When scanning your network and you know which channels are in use, you should scan only on active channels. For example, do not scan channels 2–5 and 7–10 if you are using only channels 1, 6, and 11 in your networks. This will give you more information about the used channels and avoid wasting time on unused channels. However, periodic scans of unused channels can also help you locate rogue devices or new neighbor devices that may operate on those channels.

Most WLAN protocol analyzers will allow you to specify

Note: **the scan time for channels. When they allow this, you may consider scanning for only 100–200 ms on unused channels and for longer times on used channels. This configuration can give you the best of both worlds.**

Frame capture options are usually configurable within the protocol analyzer. Figure 5.5 shows an example of the capture options frequently available. These include:

- Capture name
- Capturing to disk or memory
- Size of the capture
- Packet truncating (also called packet slicing)
- Channel to capture
- Adapter to use for capture
- Filters at capture time

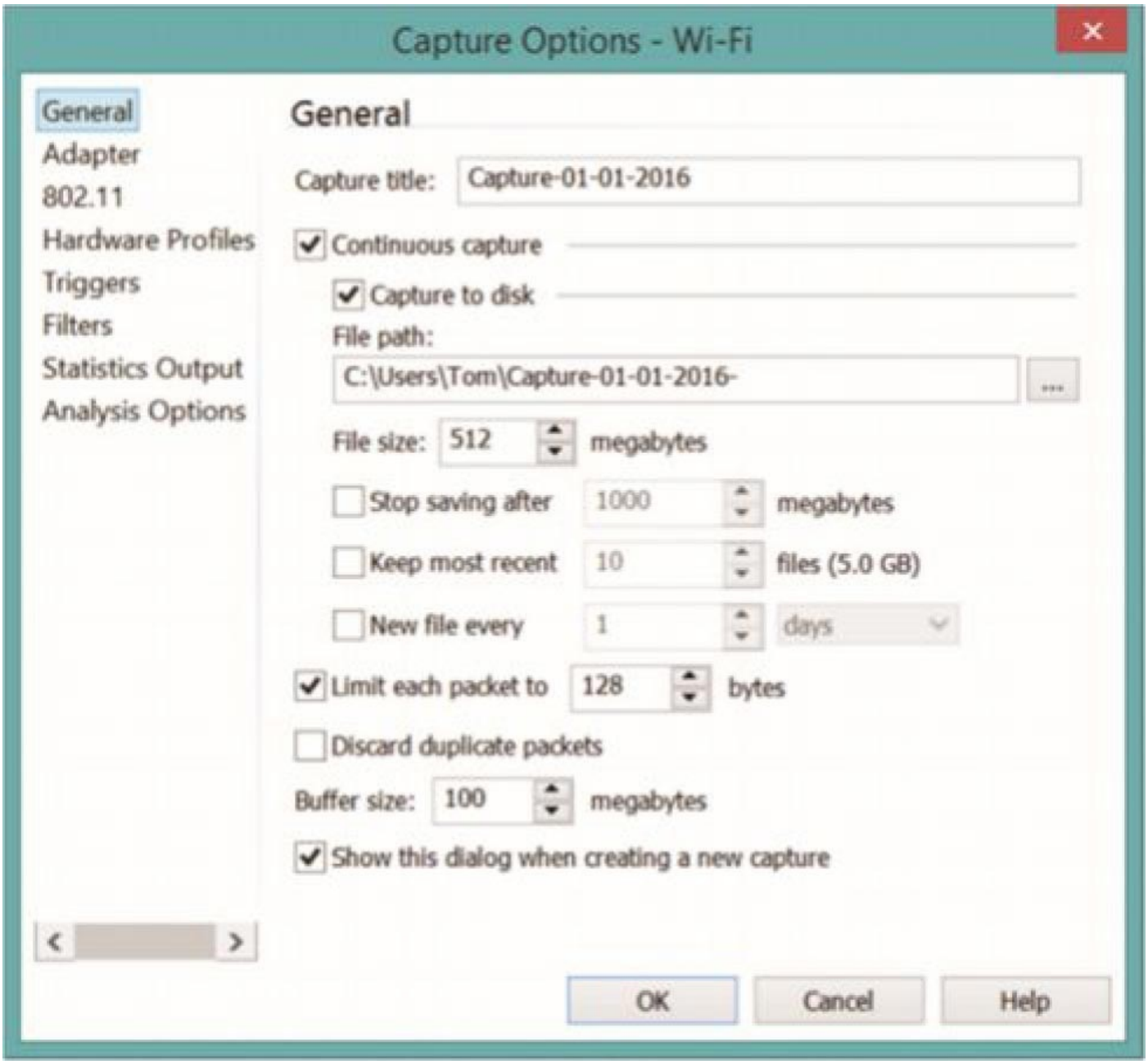


Figure 5.5: Capture Options in OmniPeek

Frame Decoding

Frame decoding is the process of converting the bits received into meaningful and explanatory information for presentation. That is, the protocol analyzer will not simply show you the binary bits, but it will decode them and provide you with explanations for them. All protocol analyzers perform decodes, but some are better than others at accurately decoding.

It is important to update protocol analyzers periodically to accommodate for changes in the PHY/MAC of 802.11. For example, a protocol analyzer designed to capture and decode 802.11n frames will not understand the newer 802.11ac frames, even if you capture them from some other source. Always update your protocol analyzer tools when you update to newer PHY/MAC layers in your network.

When a protocol analyzer decodes WLAN frames, it typically does three things for you:

- Provide a decode panel that displays the frame information in an organized hierarchical manner.

- Provide a hex view of the frame data.
- Provide an ASCII view of the frame data.

When looking at unencrypted frames, the ASCII view can show the actual HTTP requests and other plain text information. Given that most enterprise WLANs use encryption, most WLAN analysts spend more time in the decode panel viewing the organized information about the frames.

If WPA-Personal or WPA2-Personal are in use, most analyzers allow you to enter the PSK so that you can decrypt the traffic. It is important that you have permission to do so. Always check the privacy policies of an organization before decrypting traffic, even if you know the PSK.

Highlighting and Filtering

Protocol analyzers also support highlighting or colorization and filtering. The highlighting feature allows you to define colors for packets or frames matching particular criteria. It allows those frames to stand out as you browse through the captured frames.

Filtering can be performed during capture or in the display. When performed during capture, the capture file is smaller, but if you later desire to see other frames or packets, they will not be available in the capture. When performed in the display, all of the frames are there, but you are focusing on those you wish to see. If your computer can capture at a fast enough rate, it is often best to capture everything on the channel being monitored and then to filter in the display.

If you feel the capture will be too large, consider truncating the frames in the capture (packet truncating or packet slicing). Figure 5.5 shows this option in OmniPeek where you can “Limit each packet to” a specific size. This means you get all the frame headers, but the actual data payload is not captured. Given that most enterprise WLANs use WPA2-Enterprise encryption, truncating the captured frames will not likely be problematic because you will not be able to see the contents beyond the headers anyways.

Expert Analysis

Expert analysis, a generic term I am using here as each vendor uses their own terminology, takes the captured frames and the radio tap header information to provide you with summary information in dashboards and reports. These views can greatly reduce the time it takes to locate and resolve problems. Figure 5.6 shows the default Wi-Fi Analyzer Pro dashboard with the quick information it provides.

In the example dashboard in Figure 5.6, the following information is provided:

- **Channel Utilization:** reveals how busy a given channel is compared with its capacity. That is, how much of the airtime is consumed based on the captured information. Useful for quickly evaluating capacity handling.
- **Top Talkers:** provides the MAC addresses of the STAs with the most frame transmissions on the wireless network. May be helpful in locating users transmitting unauthorized data or using throughput intensive applications.
- **Most Utilized SSIDs:** displays the SSIDs that have the highest utilization rate and

can be used to determine if clients are roaming to better APs or sticking to those in a congested area.

- **Active Device Count:** tracks the number of communicating devices and displays them in the AP, STA, and ad-hoc categories.
- **Top APs Based on Active Associations:** lists the APs having the most active number of client STAs and can be useful in locating overloaded APs.
- **AP Security Settings:** reveals the APs that are encrypted (WEP), securely encrypted (WPA2), and transitionally secured (WPA). Also lists Open APs. Excellent for quick evaluations of security compliance.

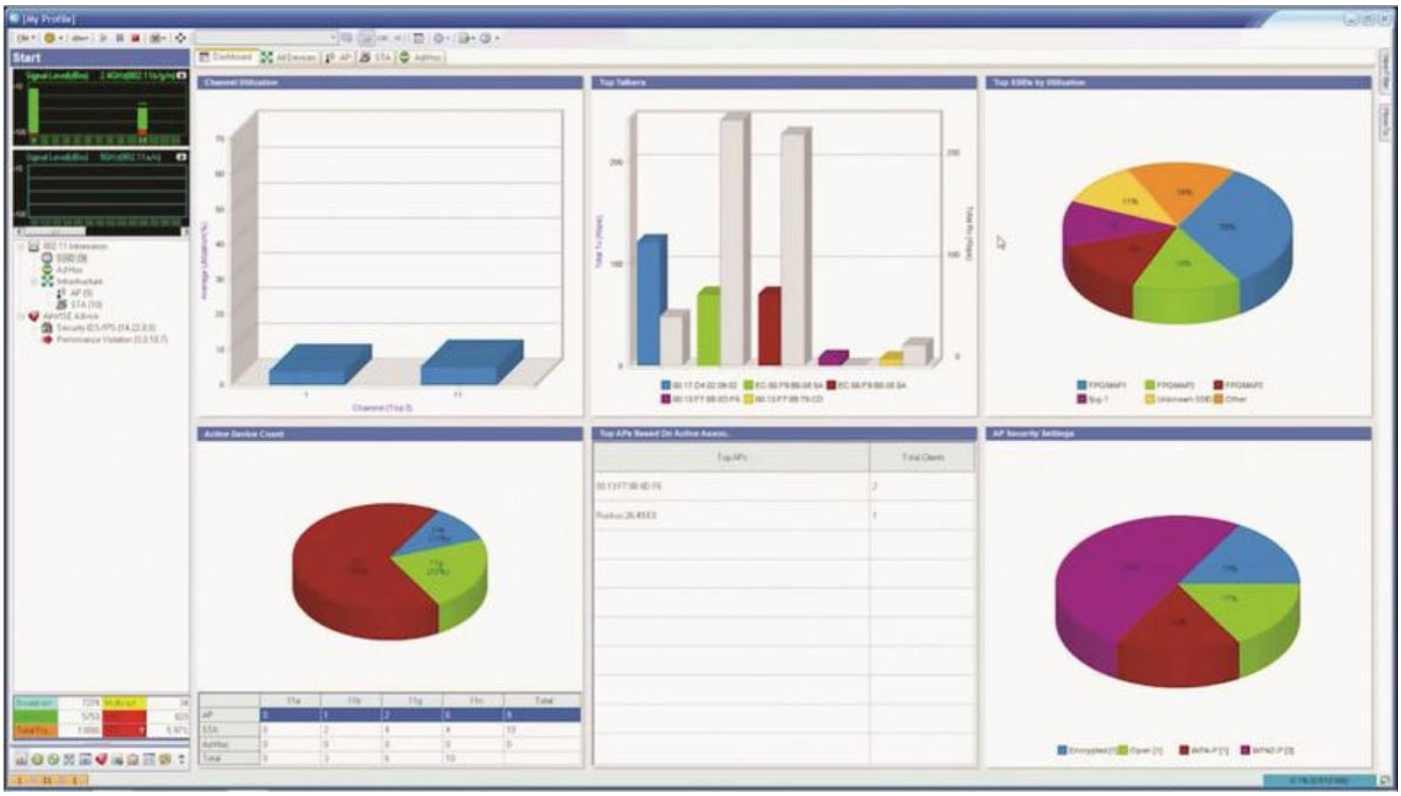


Figure 5.6: AirMagnet Wi-Fi Analyzer Pro Dashboard

As you can see, the dashboard alone provides very useful information. OmniPeek and CommView for WiFi also provide reports on similar information. All of these views and tools fall into the expert analysis category as they go beyond simple frame decoding. Figure 5.7 shows an example dashboard display from OmniPeek. Figure 5.8 shows an example dashboard from CommView for WiFi.

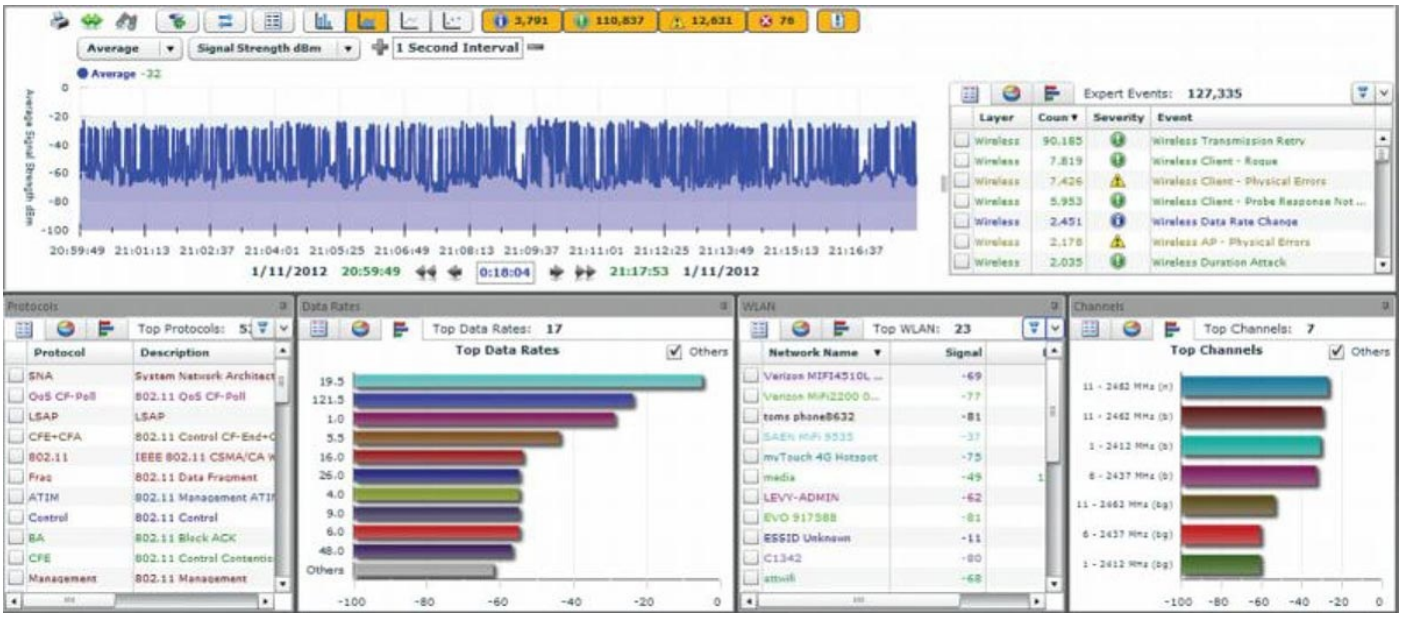


Figure 5.7: OmniPeek Dashboard Display

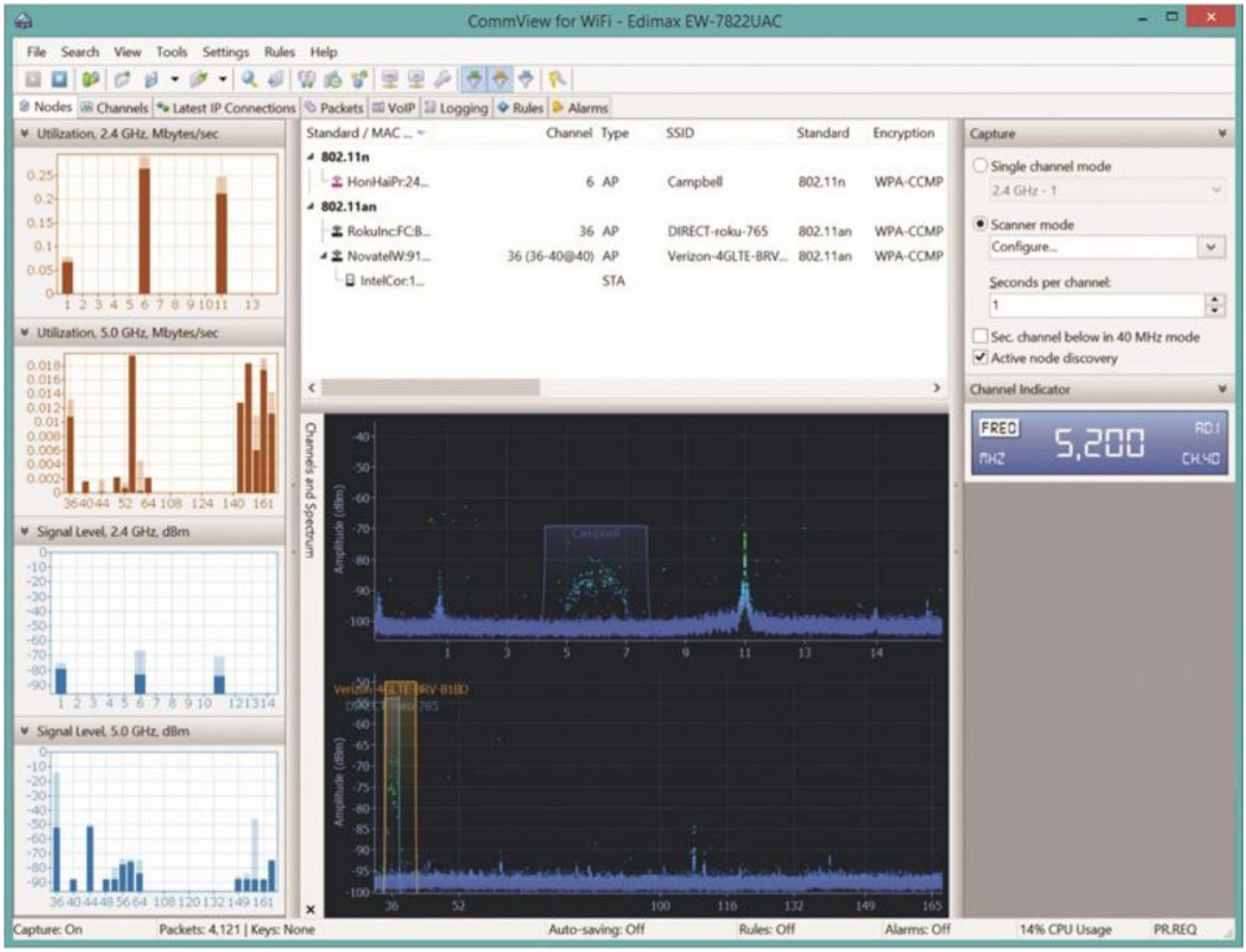


Figure 5.8: CommView for WiFi Dashboard

Installing and Configuring

Installing a WLAN protocol analyzer involves downloading the installation sources from the vendor website and then launching the installation. It is not a complicated process, but

licensing can be somewhat tricky. Licensing can either be simply serial number based or it can require a license file. When using a serial number, enter the number and allow the software to verify the license online. When using a license file, the software may be installed while offline; however, you typically have to go online within a short period of time to activate the software.

Some protocol analyzers require that the software be tied to either a machine or a WLAN adapter. When tied to the machine, typically, the internal Ethernet MAC address is used (or possibly the internal Wi-Fi adapter MAC address). When tied to an adapter, the MAC address of a capture adapter is used. The latter option allows you to install the software on multiple computers and use it as long as that single adapter is inserted into the USB port of the individual computers.

With all WLAN protocol analyzers, the first configuration step—or some might say the last installation step—is the installation of the appropriate device drivers. CommView for WiFI makes this process very easy in that it detects supported adapters and enables a dual-driver feature. When you launch the software it will enable the drivers needed for capture. When you exit the software, it returns the drivers to the state needed for OS connectivity. The other protocol analyzers require that you install the proper drivers (usually available from the vendor website) before launching the software.

After installation, on first launch, you should configure the protocol analyzer for your needs. Figure 5.9 shows the basic configuration interface for CommView for WiFi.

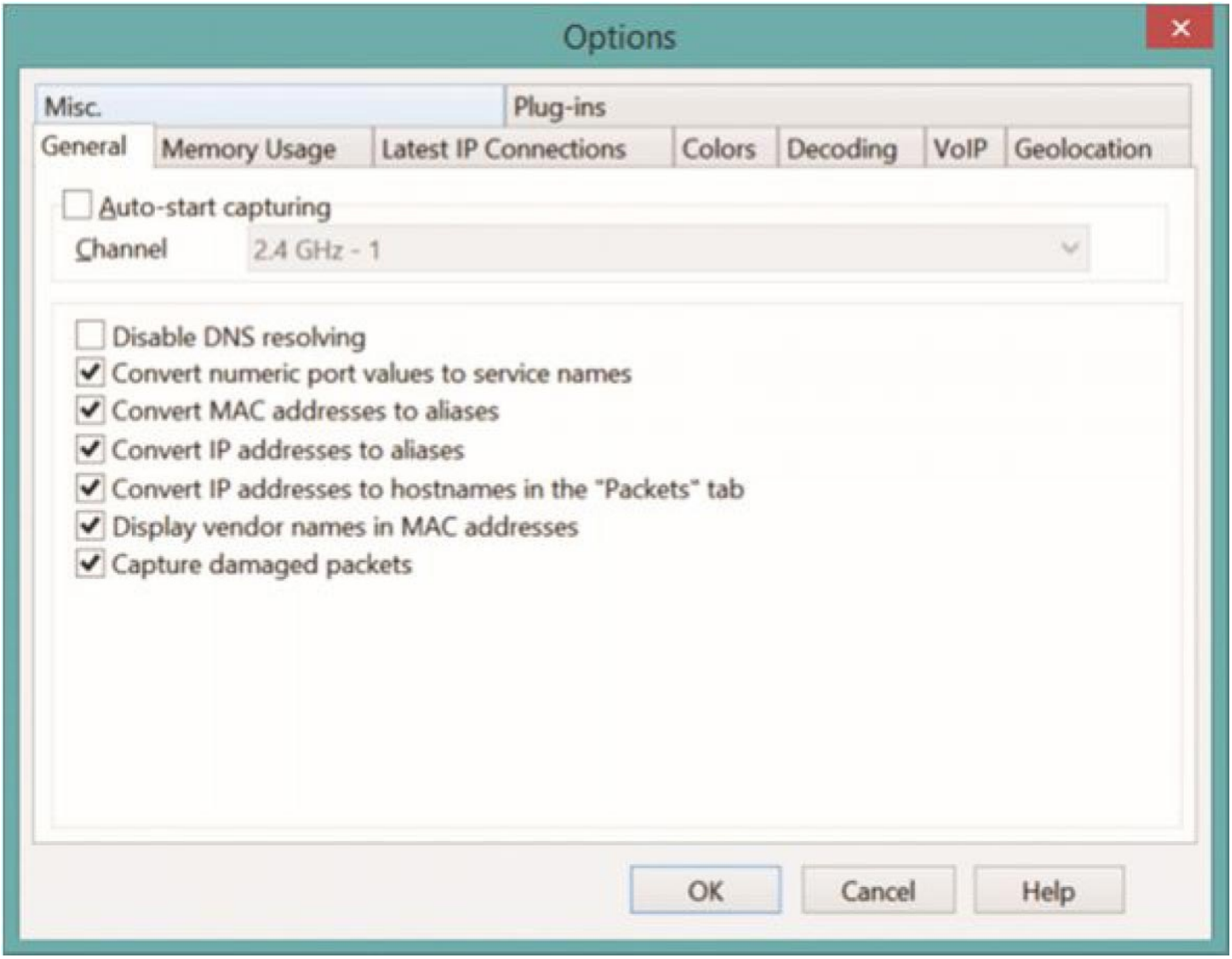


Figure 5.9: CommView for WiFi Configuration Options

Typical options reflect those available in Figure 5.9, but may be named differently in various applications. For example, Figure 5.10 shows the options windows in OmniPeek. As you can see similar named configuration pages are available. However, each protocol analyzer will also have its own unique configuration options. I will address the common configuration options here.

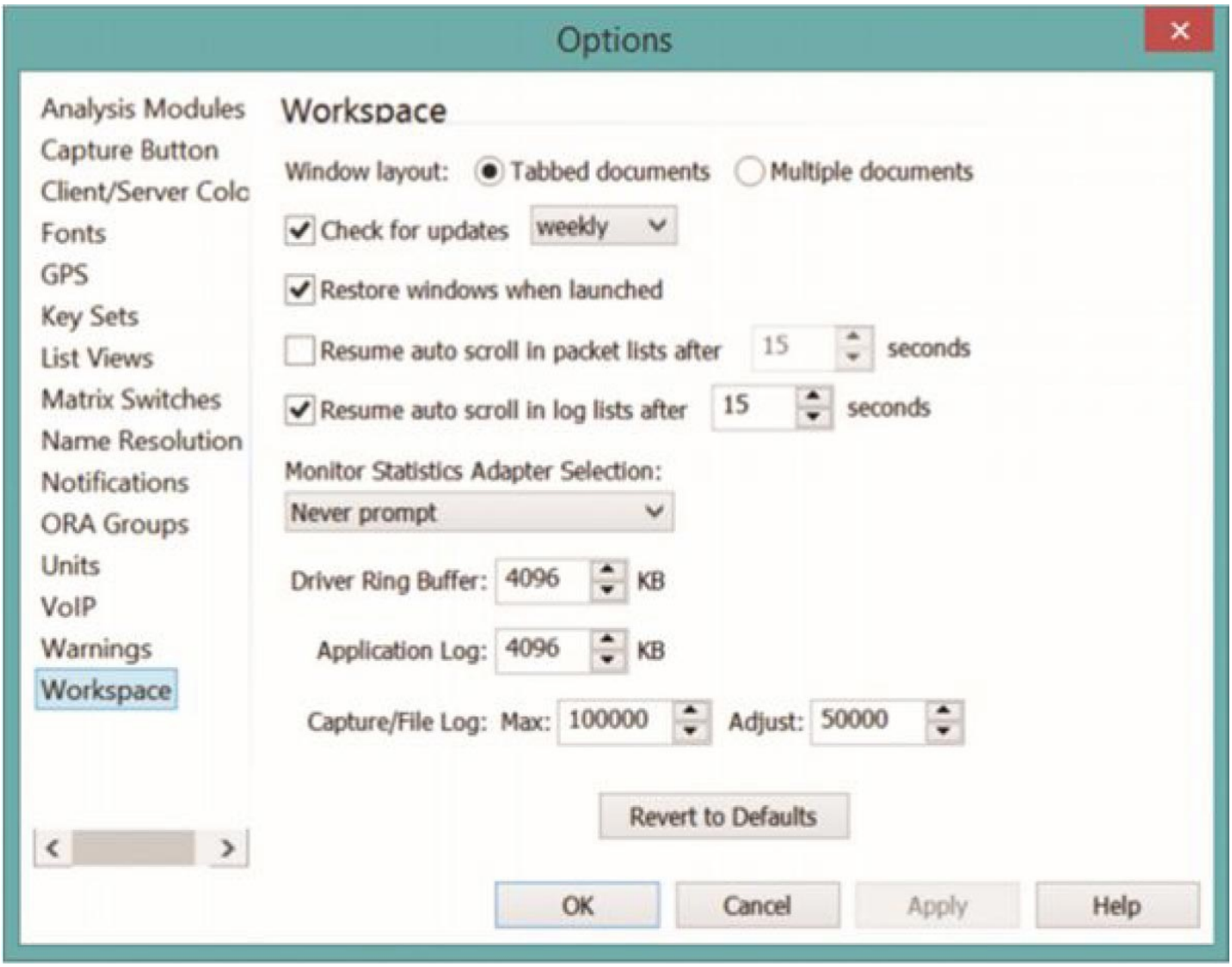


Figure 5.10: OmniPeek Options Window

Configuration options typically include default settings for automatic operations. For example, when the analyzer starts, you may want it to immediately begin either capturing or monitoring. In capture mode, packets are captured and saved either to memory or to disk. In monitor mode, packets are analyzed and discarded while historical statistics are maintained.

Log and buffer configurations are also important. The buffer is used to store the packets/frames as they are captured. It is limited to the size of RAM in the computer and must be written to disk if is exceeds available space.

Name resolution options are available for IP packets. When enabled and Layer 2 encryption is not used or when it is and the encryption key is entered, the analyzer can show DNS names instead of just IP addresses. This can be more meaningful to the analyst.

GPS options are useful in that, when enabled and a GPS module is in the computer, the software can track the GPS location at which a particular packet was captured. This is useful in both protocol and spectrum analyzers.

Of course, most analyzers allow you to customize the interface, including color options, font options, and workspaces. Figure 5.10 shows the font configuration dialog for OmniPeek. Font configuration is important in preventing eye fatigue if you spend hours working with a tool like a protocol analyzer.

The final options will be related to decoding. Figure 5.12 shows the Decoding tab in the CommView for WiFi Options dialog. You can configure the following important options related to decoding in most WLAN protocol analyzers:

- **Node expansion options for the decode window:** either start with all nodes expanded or specify the nodes to expand.
- **Signal level display:** options often include dBm or percentage.
- **Display type:** options include ASCII, Hexadecimal, HTML, and others.
- **Options to include or exclude:** may optionally include/exclude packet numbers, images, and more.

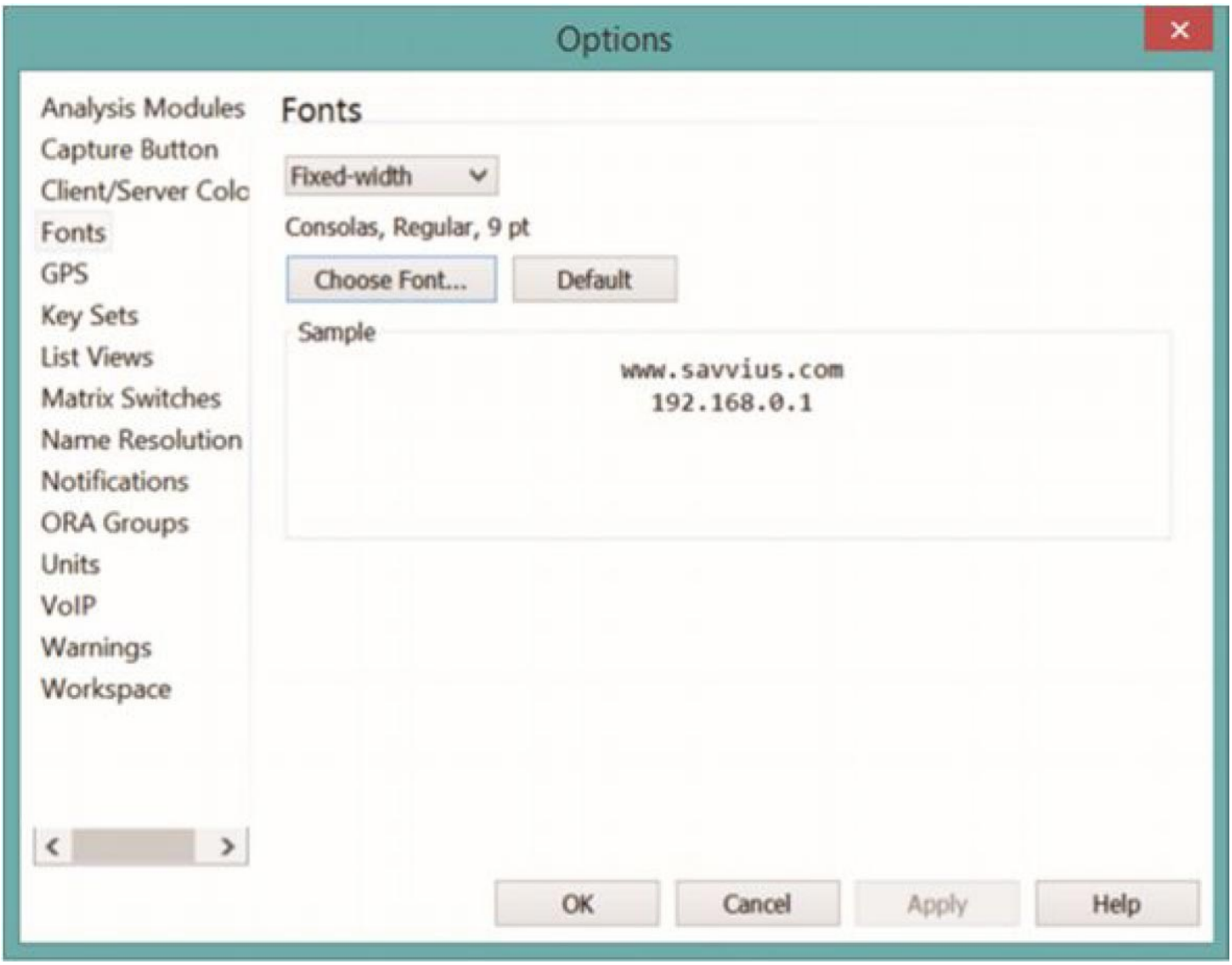


Figure 5.11: Font Configuration in OmniPeek

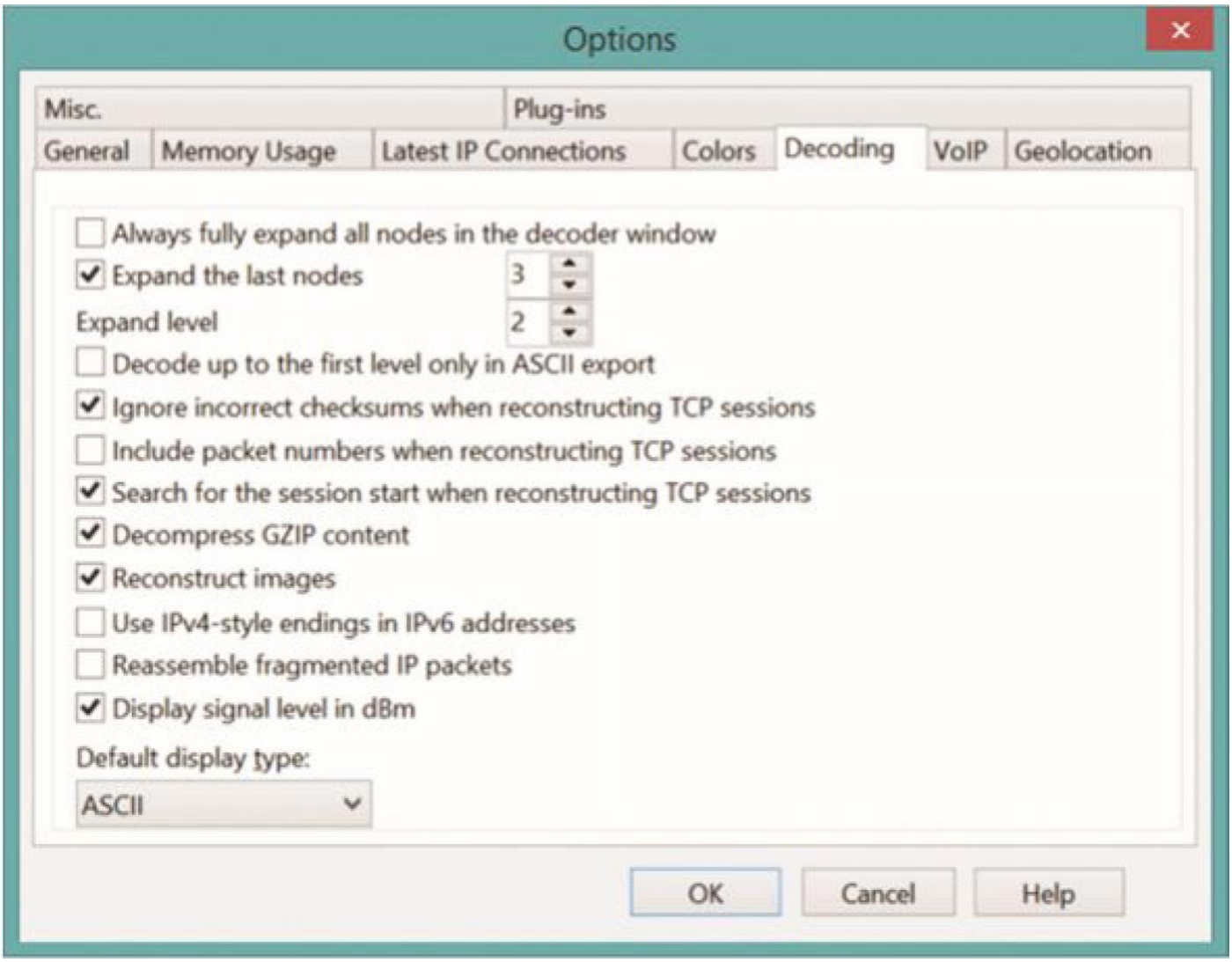


Figure 5.12: Decoding Options in CommView for WiFi

Additional common configuration settings of interest include:

- Profiles
  - User- or purpose-specific configuration settings that can be adapted and switched between for different types of analysis (e.g., wired vs. wireless, application-specific analysis, VOIP, TCP, etc.).
    - Configuration preferences
    - Channel scan settings
    - Display and Capture Filters and Macros
    - Coloring rules
- Capture Settings
  - Depending upon the capture type and purpose, analyzers can be configured to capture to a buffer or to a disk. Analyzers are able to save capture files in specified sizes (512 MB for example), with certain rules, or with event triggers.
- Name Resolution
  - There are different ways to “name” the devices on your network. Every

protocol analyzer offers a way to configure the device naming.

- Virtual or Physical address (e.g., 192.168.2.138)
- Hex MAC address (e.g., 00:14:C2:27:98:3B)
- Vendor OUI MAC address (e.g., Aruba Networks:00:f2:14)
- Configured Alias (e.g., William Wallace's iPad)

Capturing WLAN Traffic

When the installation and configuration process is complete, you can begin capturing WLAN traffic. The first and most important decision is the physical location for capture. Generally speaking, it is best to capture near the problem. For example, if a specific user is experiencing problems, you should capture at that user location. If several users in a BSS are experiencing problems, you should capture near the AP.

An interesting scenario often occurs when capturing WLAN frames. The protocol analyzer may report a lower signal strength than the AP, and yet you are capturing at the AP. The reason can simply be propagation, but it is more likely the quality of the receiver in the AP. Enterprise APs are typically designed with better quality components that results in better receiver sensitivity, that in turn results in better data rates or signal quality in the AP than in the client STA. It may not be about the actual signal but the signal processing abilities of the devices. This is an important piece of information.

To answer the question "where do you place the sniffer?" you should ask and answer several other questions:

- What packets do you want to capture?
  - A BSS or ESS?
  - A specific client station?
  - A specific AP?
  - A mobile station?
- Which physical areas will provide the best (least corruption) perspective of the packets (either from a device or from multiple devices in a conversation)?
- Are you looking for a specific conversation and both sides of that conversation?
- Are you performing a network baseline, or troubleshooting a network-wide problem?
- Is the analyzer designed to be part of an infrastructure or is it a mobile platform?
  - Where and how to mount distributed analyzers will depend entirely on your deployment needs and the selected product's capabilities. Consult vendor documentation for specifics. Most vendors recommend a monitor mode overlay solution in the range of 1:4 (1 AP to 4 monitor mode APs) or 1:6.
- Generally, an analyzer is placed near the AP or the client station experiencing a

problem:

- Placing the analyzer near an AP provides a view of the BSS from the AP's perspective (radio differences aside) and provides a more reliable trace of the AP's transmitted traffic.
- Placing the analyzer near a client station provides a view of the wireless medium from the client's perspective.

When you are analyzing a moving client, you should move along with the client. If that device will roam between APs, you should plot a similar course if you can. Identify the APs in the roaming path and know the operating channel for those APs. Use multiple adapters simultaneously to capture both channels- or to troubleshoot some roaming issues, set the adapter on a static scan of the "roam to" channel.

While monitoring or capturing frames, some analysis applications report traditional RF metrics, like signal strength, noise, and SNR. Most 802.11 NICs are not truly capable of gathering these metrics at the RF level. Instead, the product vendors rely on the Wi-Fi metrics that are reported by the card. In addition, the vendors also include some information from RF registers reported by the NIC, but this information is not comprehensive. For that reason, we are often left with helpful, but not quite accurate, RF reports. Figure 5.13 shows such metrics.

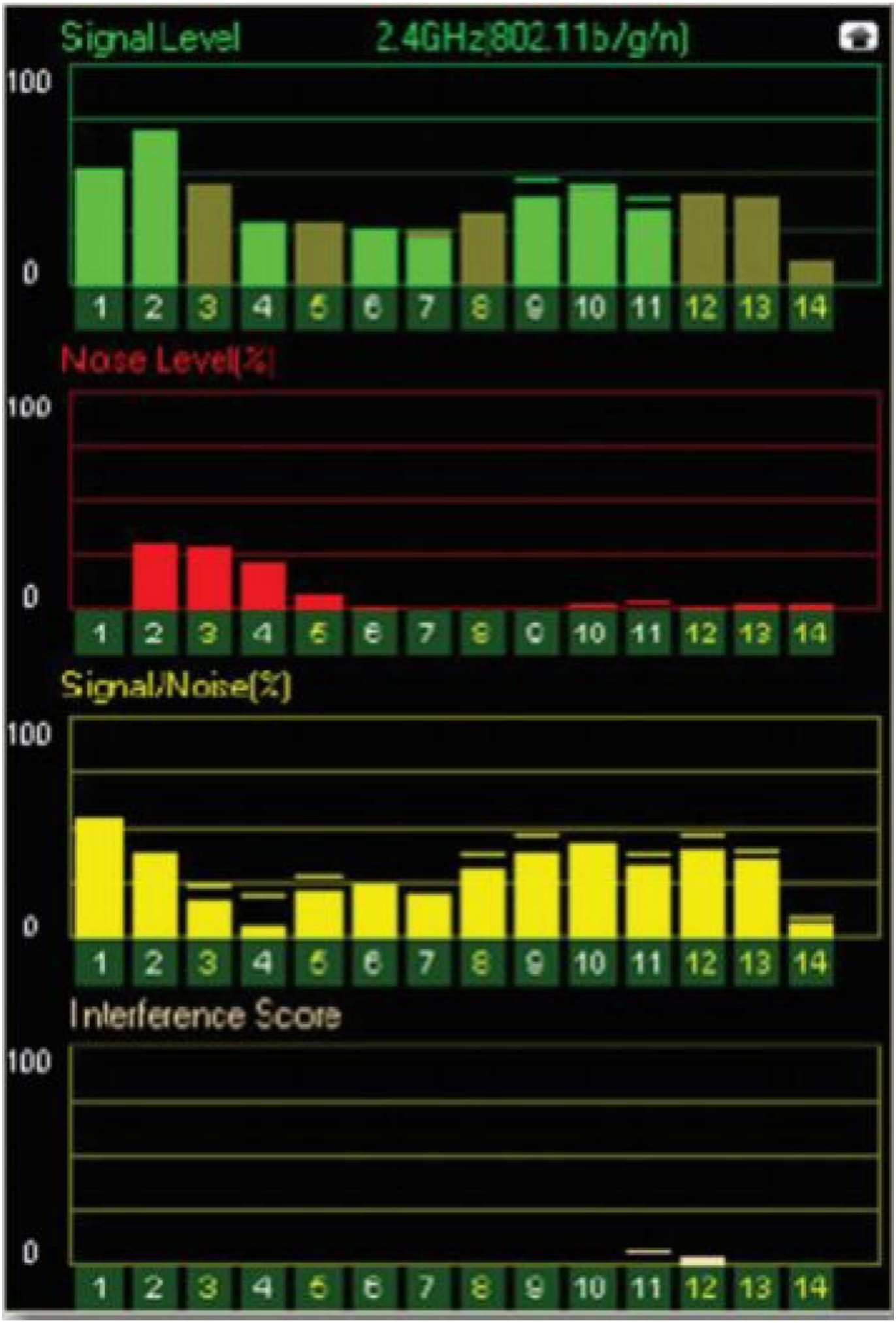

Signal Level
2.4GHz(802.11b/g/n)
100
0
1 2 3 4 5 6 7 8 9 10 11 12 13 14
Nose Level(%)
100
0
1 2 3 4 5 6 7 8 9 10 11 12 13 14
Signal/Noise(%)
100
0
1 2 3 4 5 6 7 8 9 10 11 12 13 14
Interference Score
100
0
1 2 3 4 5 6 7 8 9 10 11 12 13 14

Figure 5.13: Signal Metrics in a Protocol Analyzer

Most analyzers support filtering the traffic during the capture. This allows you to limit the overall size of the capture file as you are only capturing traffic you desire. Capture filters occur while the data is being captured by the wireless NIC. If the data does not match the filter requirements, those frames will be dropped and cannot be recaptured. Capture filters are the best way to limit the trace files to only those frames that are necessary. This keeps the capture file size down.

It is often recommended that capture filters be used sparingly. If certain frame types are omitted during capture, you may find that important information was lost and cannot be obtained after the fact. Unless you are certain of the traffic types that are necessary (or not) for analysis after capture, you should use display filters. Display filters are more flexible than capture filters and allow you to modify the visible frames as needed.

Some analysis tools have much more flexible (and potentially more complex) filter features, allowing for completely custom filter configurations. This can be handy when manually investigating large trace files (which are more common in wired traces).

Radio information is also available during capture. Every protocol analyzer provides information about the received packets that may not actually be a part of the packet. It adds information that is not contained in the transmitted frame. The added information tells the analyst about the frame as it was received by the radio. This information includes details like received signal strength (may be a dBm value or a %), the channel on which this frame was received (this may not match the channel on which it was transmitted), data rate, noise level, packet number, machine timestamps, and flags. Most of these fields are self-explanatory, but the flags are specific frame attributes that are differentiated by the analyzer, such as whether it is a fragment, whether it uses long or short GI, whether it is an aggregated frame, and many others.

Each analyzer uses its own name for this additional info. Wireshark calls it the “Radiotap Header,” whereas Wildpackets calls it “Packet Info.” The important thing to understand is that this information is populated from the PLCP header, or more commonly, from the radio driver. It may not be a part of the transmitted frame.

After capturing the frames, you can begin analysis of the individual frames and decodes, and you can use the different views of the analyzer to troubleshoot problem scenarios.

Analyzing WLAN Traffic

The first step to effective analysis is understanding the information provided in frame decode. Nearly all protocol analyzers provide a basic collection of information and each analyzer describes and provides this information in slightly different ways.

In protocol analyzer software, the two display features that create a lot of confusion are *time* and *device identification* displays. We want to highlight them here simply to add clarity.

The time characteristics can be the most confusing because every analysis software uses its own definitions and default settings for time displays. At a basic level, there are three

time characteristics that you should know:

- *Arrival Time*—This is the time that is assigned to a packet after it is processed by the host system. This timestamp is dependent upon the system clock of the computer, and designates when the packet was captured.
- *Delta Time*—Delta measurements are used for comparison between one point and another, and in protocol analyzers, often reference the elapsed time between consecutive packets.
- *Relative Time*—Relative time measurements compare one time with another designated time, such as the first packet. Relative measurements often use the first packet in the list, though they can also use an arbitrary reference time (such as the 15th packet), as designated by the user.

These definitions are often good baselines for time displays. However, when in doubt consult your application's user guide to know for sure. Other time fields may be used, and they can all be helpful when doing protocol analysis.

Device Identification is another common challenge in protocol analysis because there are a number of ways to identify network nodes.

- *Virtual or Physical Addresses*—You may be able to identify a station by the MAC address or IP address. In some situations, a captured packet (L3) will be encrypted, so only a MAC address is visible to the analyzer.
- *Address 1-4*—In a WLAN frame, there are four possible address fields, but all four will not be present in every case. They identify the transmitter address, receiver address, source address, destination address, and BSSID. If your analysis software uses Address numbers to identify a specific field, ensure that you can correctly interpret them.
- *Source, Destination, BSSID*—Instead of using numbered address fields and requiring the analyst to manually interpret the meaning of those fields, many analyzers will directly identify the source and destination addresses as well as the BSSID. In wireless analysis, there is a crucial distinction between a transmitter address and a source address. The former is wireless. The latter may be wired or wireless. The same applies to receiver and destination addresses.
- *Aliases*—Most analysis applications allow you to specify a recognizable name for a device to make it easier to recognize in the packet list. For example, you might label Johnny Appleseed's iPad as such, making it easier to identify that specific device instead of looking at a MAC address.

Understanding the differences in labels can make a massive difference in your interpretation of a set of packets.

In order to simplify analysis and make it easier to locate target frames, colorization and filtering can be used. Colorization changes the colors used in the frames/packets list so that particular frame types stand out to you. Filtering is used to remove particular frames/packets from the list or show only specified frames/packets. Each protocol analyzer offers its own filtering options. This chapter will explore the options in

Wireshark, as it can decode and process packets captures by other analyzers and its filtering engine is among the most powerful once you have the capture file. Wireshark is also freely available for download.

Figure 5.14 shows a capture file loaded in Wireshark with colorization enabled. Figure 5.15 shows the colorization rules interface used to implement it. Colorization is performed in Wireshark using filters. First identify the filter that matches the traffic you wish to specially color and then create the colorization rule. I find it easiest to use the expression builder available at the end of the filter field toolbar to formulate the filter. Then copy-and-paste it into the colorization rules dialog. Exercise 5 steps you through this process.

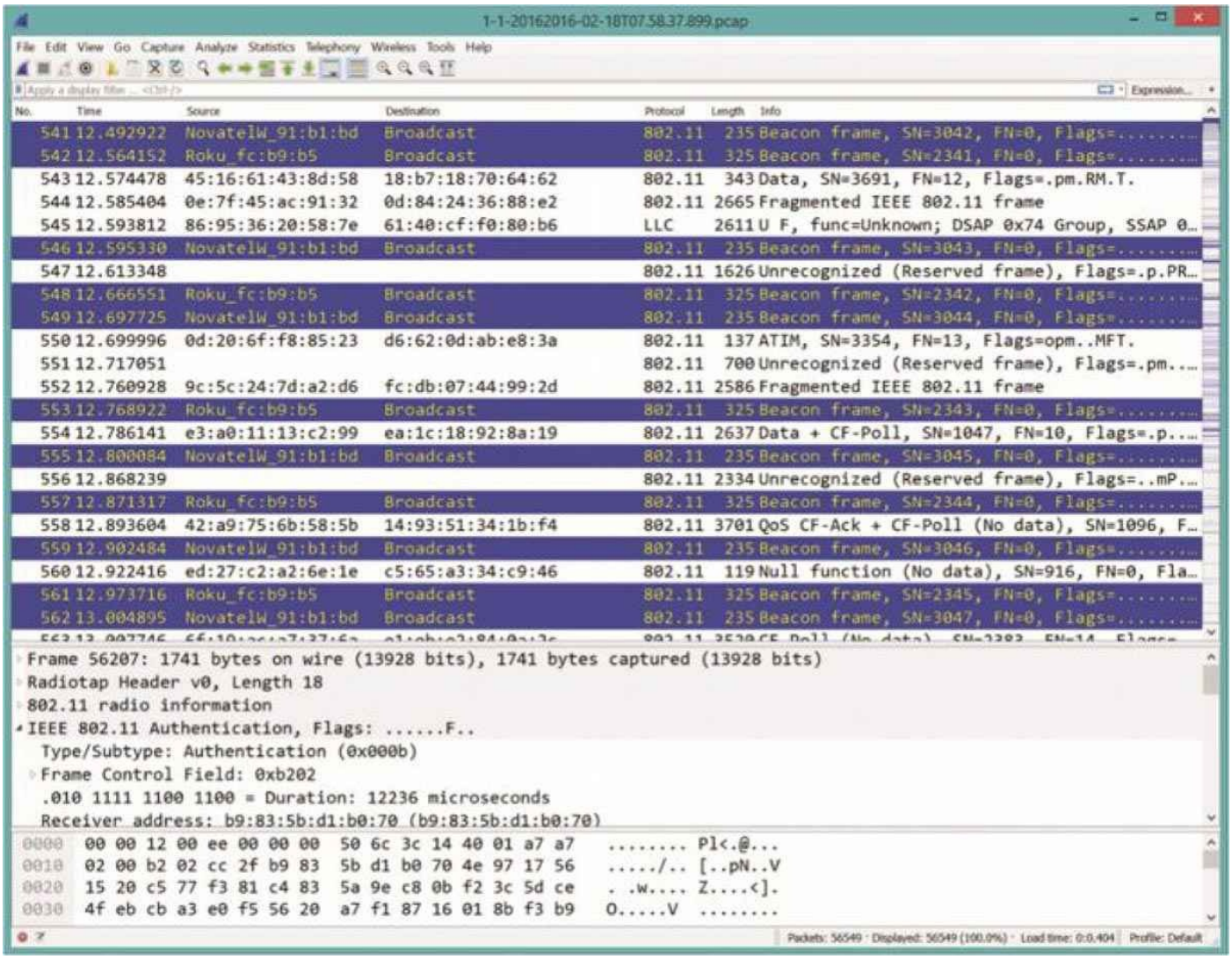


Figure 5.14: Colorized Capture File in Wireshark

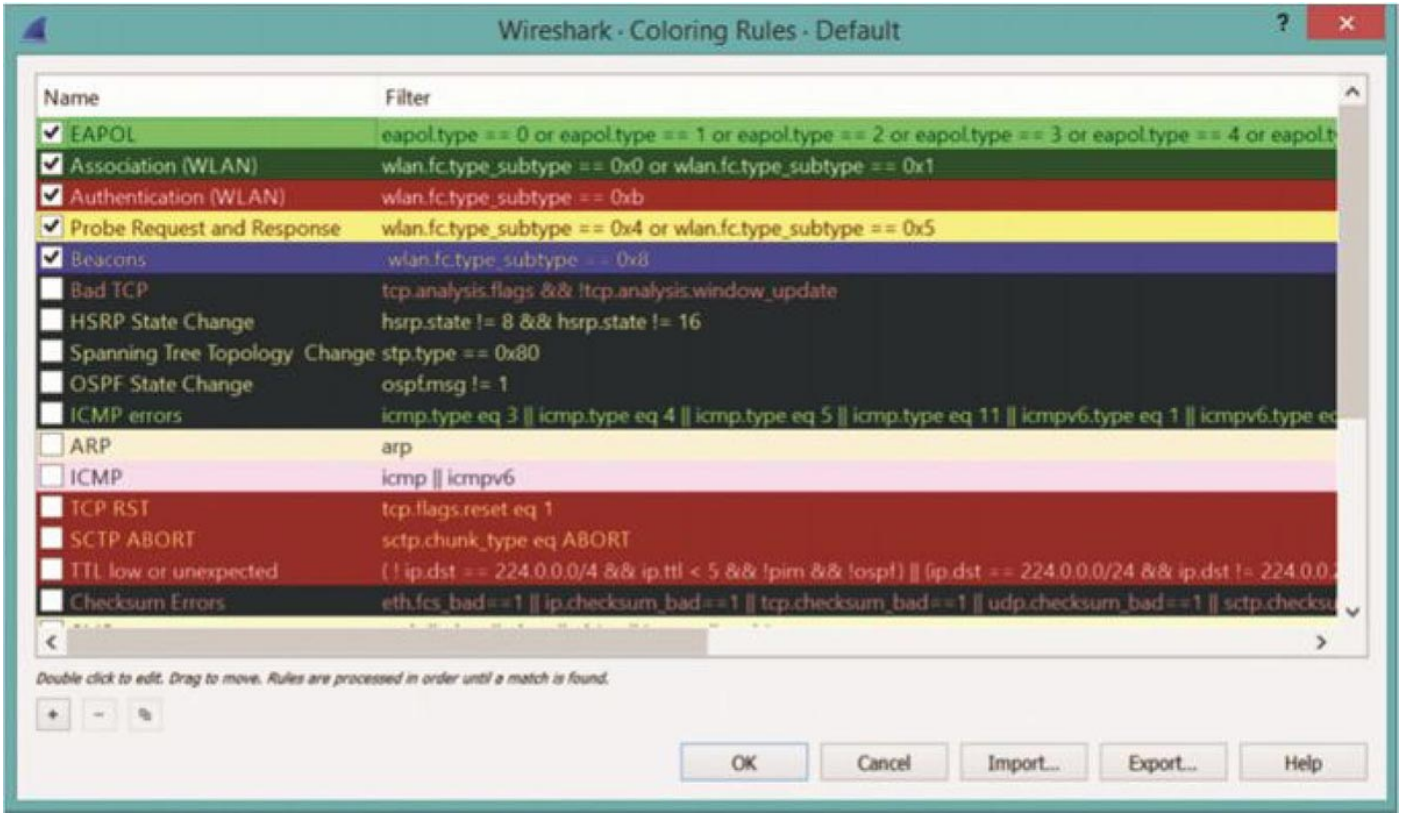


Figure 5.15: Colorization Rules Interface

Note: **Most WLAN protocol analyzers will allow you to specify the scan time for channels. When they allow this, you may consider scanning for only 100–200 ms on unused channels and for longer times on used channels. This configuration can give you the best of both worlds.**

Exercise 5

In this exercise, you will create a coloring rule that applies a special color to Null Data frames in WireShark. If you wish to perform this exercise, you will need to have Wireshark installed and a capture file that includes Null Data frames; otherwise, you can simple read along with the exercise and optionally watch the demonstration video for this exercise by searching for "CWNPTV colorizing null data frames" at YouTube.com.

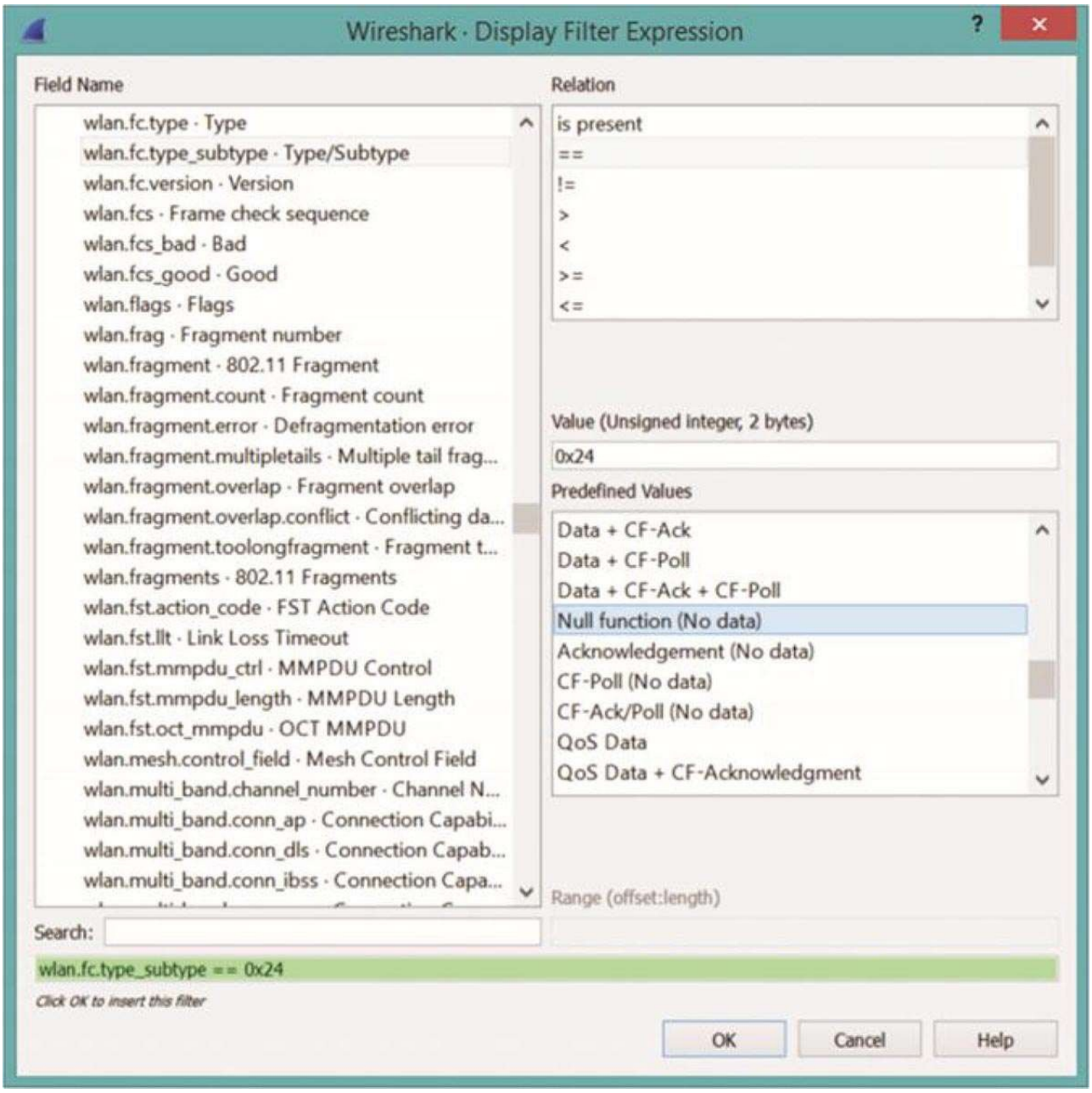
1. Launch Wireshark and open the capture file containing the null data frames.
2. In the Wireshark filter toolbar, click the Expression button in the upper-right corner.

Graphic 5.1

3. In the Wireshark Display Filter Expression dialog, scroll down in the Field Name box until you see IEEE 802.11 – IEEE 802.11 wireless LAN and then expand this

node by clicking the + to its left.

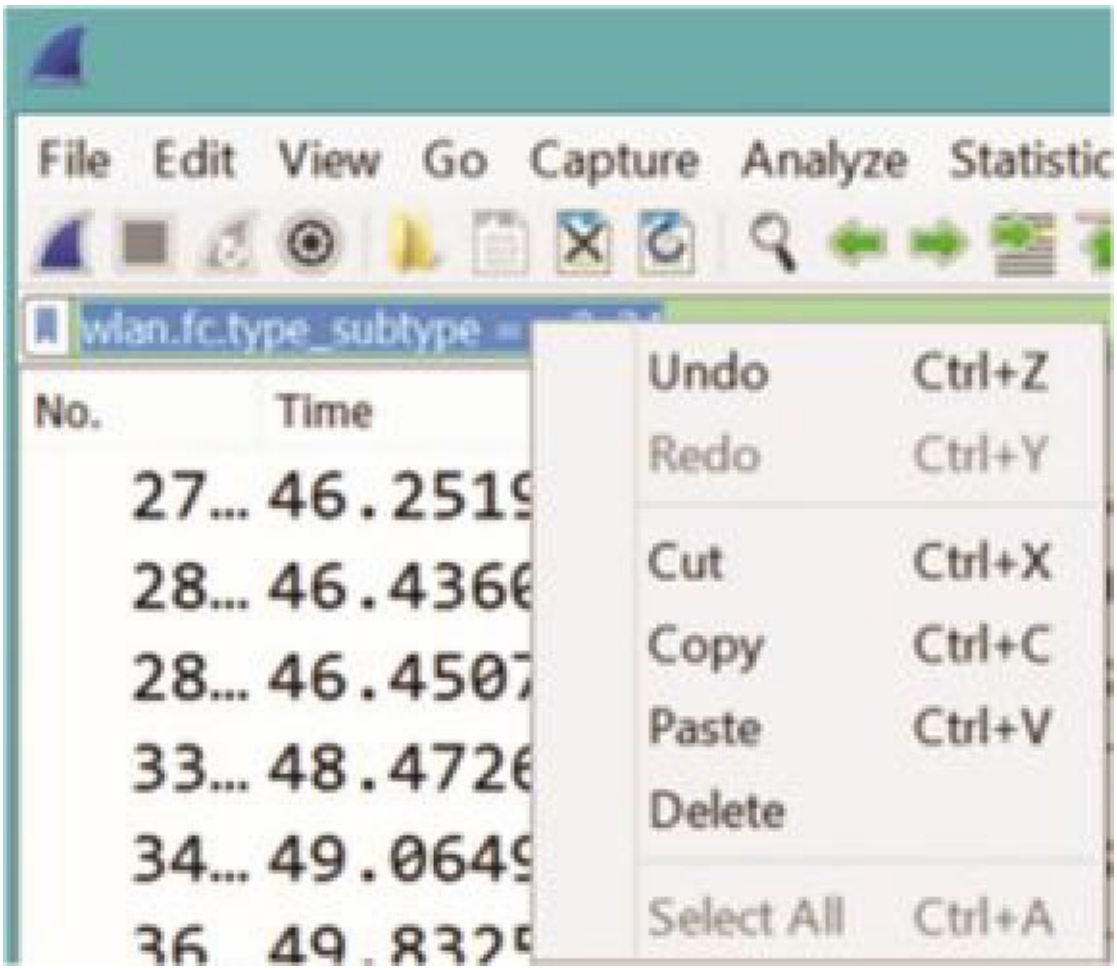
4. Within the node, scroll down until you see the wlan.fc.type_subtype – Type/Subtype entry and click this entry to select it.
5. Now, in the Relation box choose == to indicate “is equal to.”
6. Finally in the Predefined Values box, scroll down and select the Null function (No data) entry. The dialog should now look similar to the one in Graphic 5.2.



Graphic 5.2

7. Click OK to add the filter to the open capture file. Click the arrow to the right of the filter field to apply it to the capture. The capture should now display only Null Data frames.

8. Because the goal is to apply this filter as a colorization rule, click in the filter field, select the entire filter (`wlan.fc.type_subtype = = 0x24`) and right-click and select Copy.



Graphic 5.3

9. Click View > Coloring Rules in the menu to open the Coloring Rules dialog. This dialog box is used to create coloring rules and set the foreground and background colors for each rule. The rule is based on a filter.

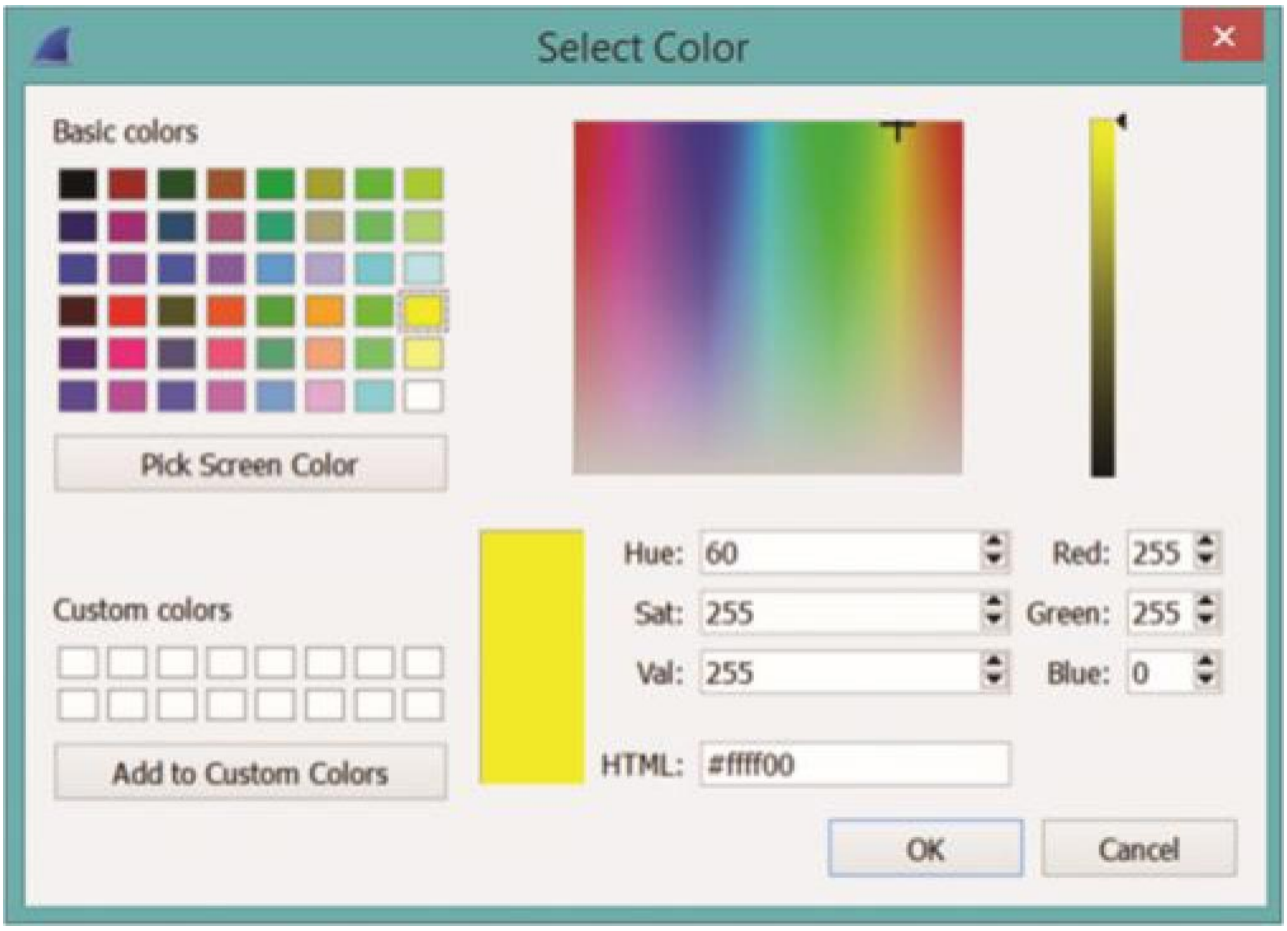
10. In the Coloring Rules dialog, click the + button in the lower left to add a new rule. The new rule is added with a default name and an empty filter field.

Graphic 5.4

11. If not already active, click in the filter field for the new rule and press CTRL+V to paste the filter into the rule filter column.

12. Double-click the Name field and type the name Null Data Frames to identify the rule well. Be sure to always select meaningful rule names as these are stored permanently in your Wireshark installation. Also, notice that you can click the Export button to export rules so that you can import them into another installation of Wireshark or in the event of a required reinstallation.

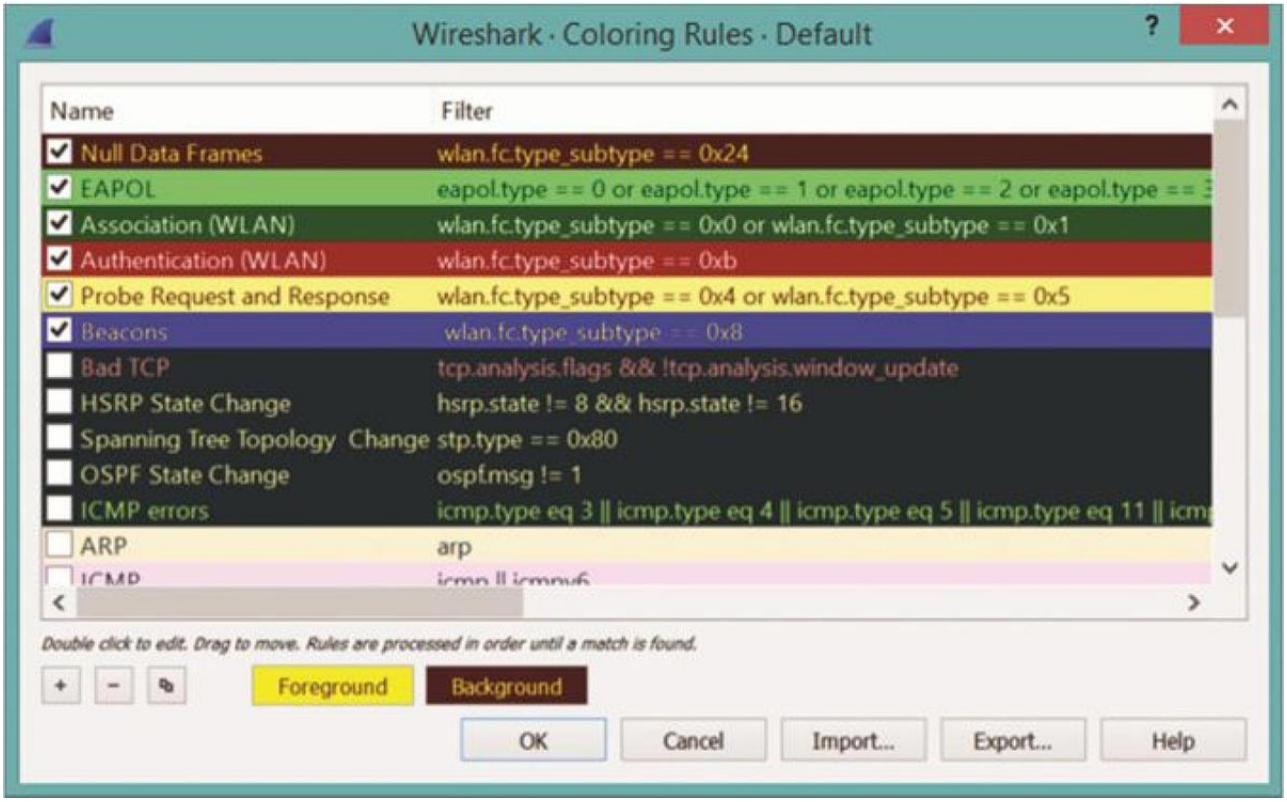
13. Click on the new rule to select it and then click the Foreground color in the bottom of the dialog to select the desired color.



Graphic 5.5

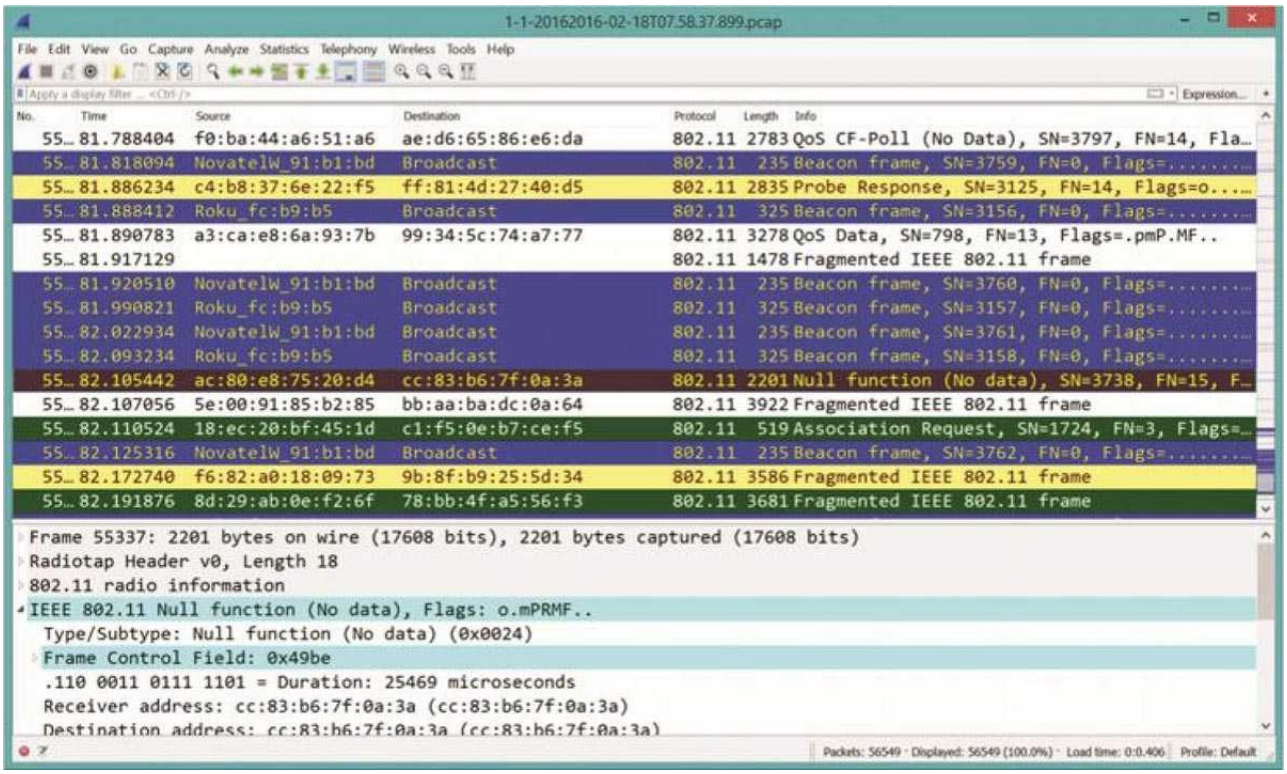
14. After selecting the foreground color, click the Background color to select the desired color for it. Be sure to select foreground and background colors that provide contrast and are readable.

15. When completed, the Coloring Rules dialog should look similar to the one in Graphic 5.6.



Graphic 5.6

16. Click OK to save the coloring rule changes.
17. Delete the filter from the filter field in the standard Wireshark display and press Enter to remove the filter.
18. In some cases, you will need to click View > Colorize Packet List to remove colorization and then click View > Colorize Packet List again to enable the new rule properly. Graphic 5.7 shows the capture with the rule applied and a Null Data Frame in view.



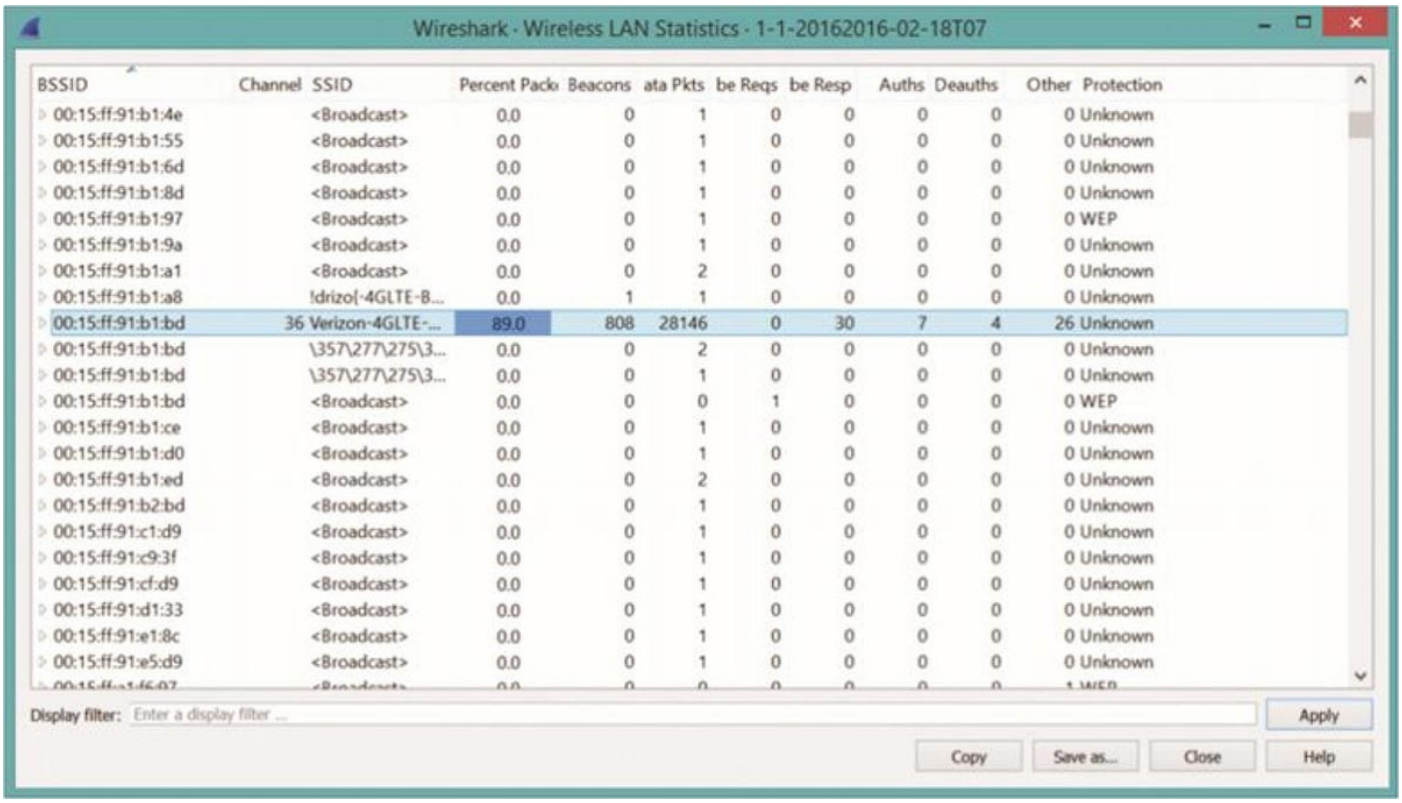
Graphic 5.7

Wireshark filters are very powerful and can be used to locate packets/frames of interest to the analyst. The Expression Builder makes it much easier to build these filters, but over time you may collect filters that you find useful. Table 5.1 lists several filters related to WLAN analysis that may be useful.

Description	Filter
Authentication Frames	wlan.fc.type_subtype == 0xb
Association Frames	wlan.fc.type_subtype == 0x0 or wlan.fc.type_subtype == 0x1
Probe Request and Response Frames	wlan.fc.type_subtype == 0x4 or wlan.fc.type_subtype == 0x5
Beacon Frames	wlan.fc.type_subtype == 0x8
EAPoL Frames	eapol.type == 0 or eapol.type == 1 or eapol.type == 2 or eapol.type == 3 or eapol.type == 4 or eapol.type == 5 or eapol.type == 6
Null Data Frames	wlan.fc.type_subtype == 0x24
802.11ac Frames at 80 MHz	wlan_radio.11ac.bandwidth == 4
2.4 GHz Frames	radiotap.channel.flags.2ghz == 1
5 GHz Frames	radiotap.channel.flags.5ghz == 1
Data Rates Less than 11 (replace with any Mbps number)	radiotap.datarate < 11
Data Rates Greater than 11 (replace with any Mbps Number)	radiotap.datarate > 11
Frame Retransmissions	wlan.analysis.retransmission

Table 5.1: Useful Wireshark Filters

Wireshark, like WLAN-specific analyzers, does offer some experts as well. Figure 5.16 shows statistics for WLAN traffic in a capture file. Wireshark also provides an I/O graph showing packets-per-second overtime as shown in Figure 5.17.



BSSID	Channel	SSID	Percent Packo	Beacons	ata Pkts	be Reqs	be Resp	Auths	Deauths	Other	Protection
00:15:ff:91:b1:4e		<Broadcast>	0.0	0	1	0	0	0	0	0	Unknown
00:15:ff:91:b1:55		<Broadcast>	0.0	0	1	0	0	0	0	0	Unknown
00:15:ff:91:b1:6d		<Broadcast>	0.0	0	1	0	0	0	0	0	Unknown
00:15:ff:91:b1:8d		<Broadcast>	0.0	0	1	0	0	0	0	0	Unknown
00:15:ff:91:b1:97		<Broadcast>	0.0	0	1	0	0	0	0	0	WEP
00:15:ff:91:b1:9a		<Broadcast>	0.0	0	1	0	0	0	0	0	Unknown
00:15:ff:91:b1:a1		<Broadcast>	0.0	0	2	0	0	0	0	0	Unknown
00:15:ff:91:b1:a8		!drizo(-4GLTE-B...	0.0	1	1	0	0	0	0	0	Unknown
00:15:ff:91:b1:bd	36	Verizon-4GLTE-...	89.0	808	28146	0	30	7	4	26	Unknown
00:15:ff:91:b1:bd		\357\277\275\3...	0.0	0	2	0	0	0	0	0	Unknown
00:15:ff:91:b1:bd		\357\277\275\3...	0.0	0	1	0	0	0	0	0	Unknown
00:15:ff:91:b1:bd		<Broadcast>	0.0	0	0	1	0	0	0	0	WEP
00:15:ff:91:b1:ce		<Broadcast>	0.0	0	1	0	0	0	0	0	Unknown
00:15:ff:91:b1:d0		<Broadcast>	0.0	0	1	0	0	0	0	0	Unknown
00:15:ff:91:b1:ed		<Broadcast>	0.0	0	2	0	0	0	0	0	Unknown
00:15:ff:91:b2:bd		<Broadcast>	0.0	0	1	0	0	0	0	0	Unknown
00:15:ff:91:c1:d9		<Broadcast>	0.0	0	1	0	0	0	0	0	Unknown
00:15:ff:91:c9:3f		<Broadcast>	0.0	0	1	0	0	0	0	0	Unknown
00:15:ff:91:cf:d9		<Broadcast>	0.0	0	1	0	0	0	0	0	Unknown
00:15:ff:91:d1:33		<Broadcast>	0.0	0	1	0	0	0	0	0	Unknown
00:15:ff:91:e1:8c		<Broadcast>	0.0	0	1	0	0	0	0	0	Unknown
00:15:ff:91:e5:d9		<Broadcast>	0.0	0	1	0	0	0	0	0	Unknown

Figure 5.16: Wireshark WLAN Statistics

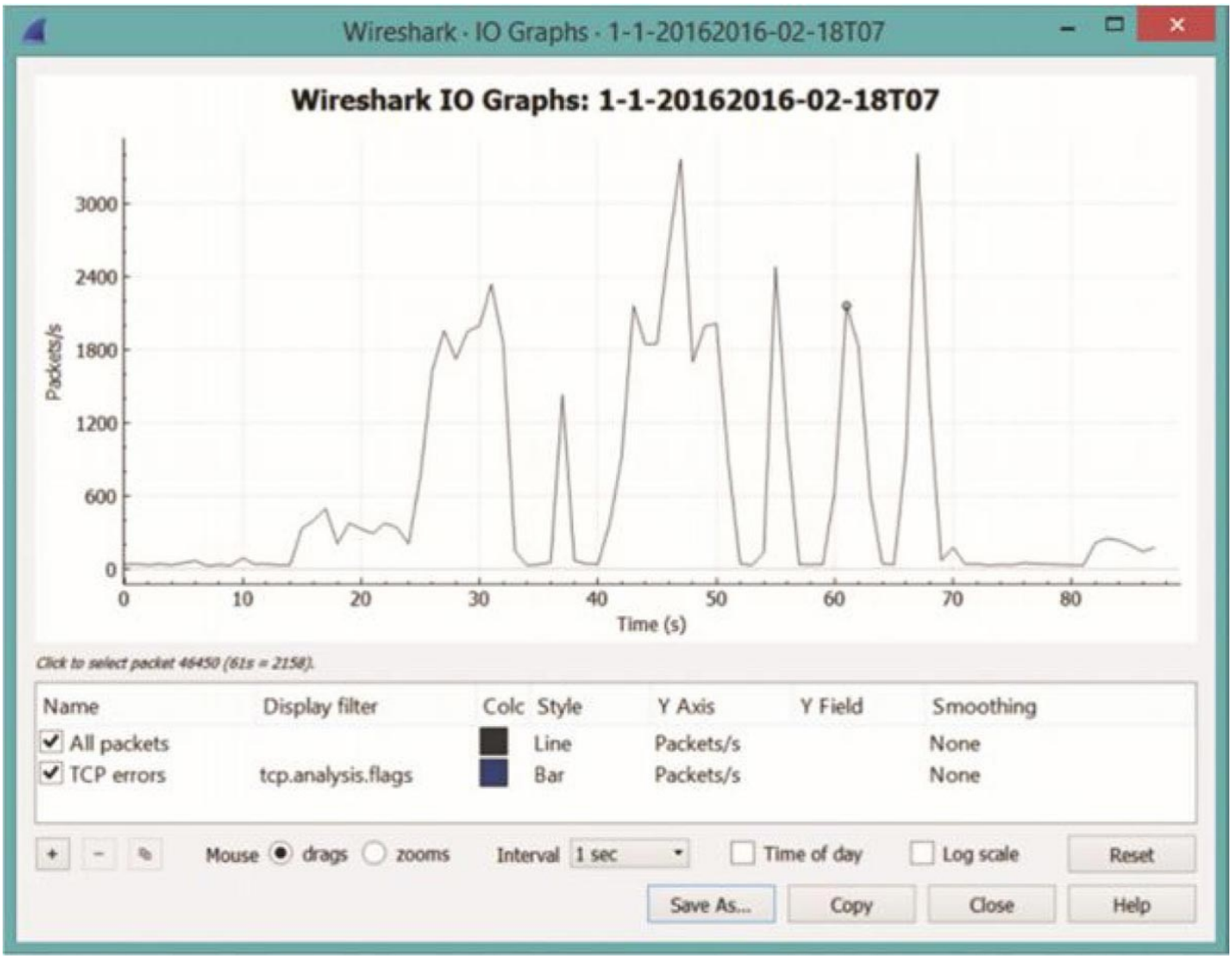
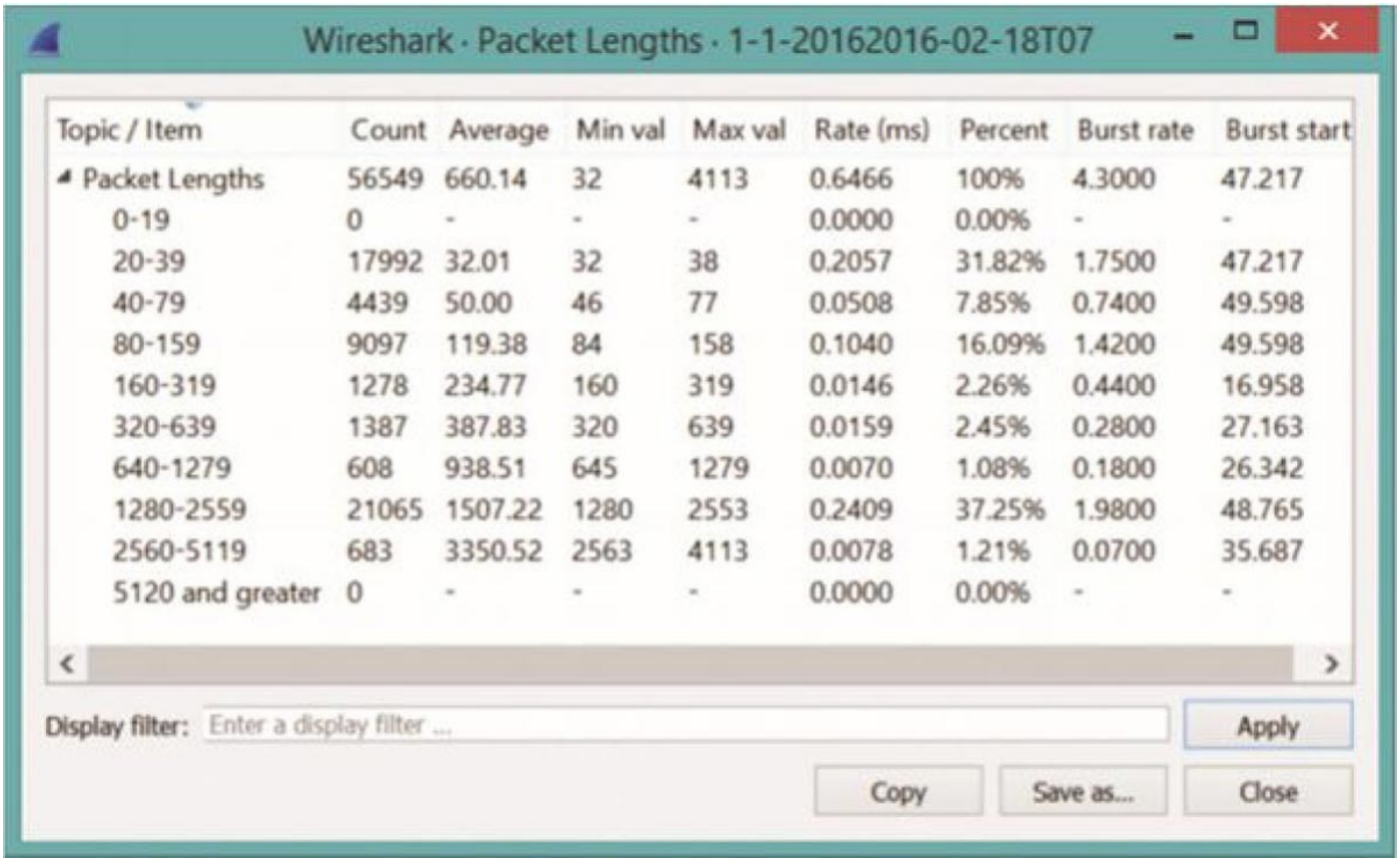


Figure 5.17: Wireshark I/O Graph

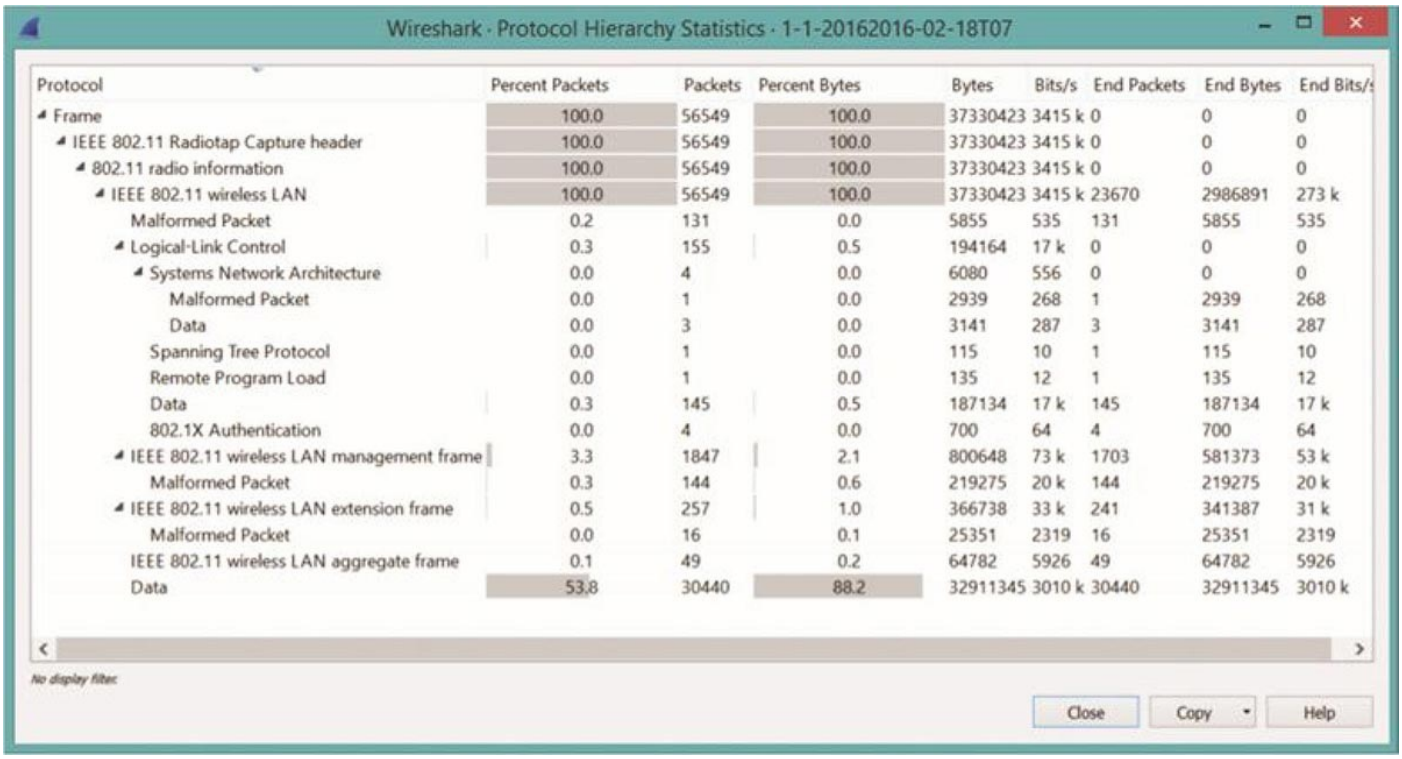
The packet lengths dialog allows you to see the packets sent at various size ranges, the average size of packets within those ranges and the percent of total packets made up of the ranges. For example, in Figure 5.18, packets ranging from 1280–2559 bytes with an average of 1507.22 bytes made up 37.25% of frames in the captured communications.



Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
Packet Lengths	56549	660.14	32	4113	0.6466	100%	4.3000	47.217
0-19	0	-	-	-	0.0000	0.00%	-	-
20-39	17992	32.01	32	38	0.2057	31.82%	1.7500	47.217
40-79	4439	50.00	46	77	0.0508	7.85%	0.7400	49.598
80-159	9097	119.38	84	158	0.1040	16.09%	1.4200	49.598
160-319	1278	234.77	160	319	0.0146	2.26%	0.4400	16.958
320-639	1387	387.83	320	639	0.0159	2.45%	0.2800	27.163
640-1279	608	938.51	645	1279	0.0070	1.08%	0.1800	26.342
1280-2559	21065	1507.22	1280	2553	0.2409	37.25%	1.9800	48.765
2560-5119	683	3350.52	2563	4113	0.0078	1.21%	0.0700	35.687
5120 and greater	0	-	-	-	0.0000	0.00%	-	-

Figure 5.18: Wireshark Packet Lengths Dialog

The final dialog I will mention from Wireshark is the Protocol Hierarchy Statistics dialog. This dialog, shown in Figure 5.19, allows you to see the percentage of frames used for management, as opposed to data transfer. In Figure 5.19, 53.8 percent of the packets are data packets, however these data packets comprise 88.2 percent of the total bytes in the capture. Therefore, out of 37,330,423 bytes transmitted, 32,911,345 were used to move data through the network. This information can be useful when analyzing throughput issues.



Wireshark · Protocol Hierarchy Statistics · 1-1-20162016-02-18T07

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	56549	100.0	37330423	3415 k	0	0	0
IEEE 802.11 Radiotap Capture header	100.0	56549	100.0	37330423	3415 k	0	0	0
802.11 radio information	100.0	56549	100.0	37330423	3415 k	0	0	0
IEEE 802.11 wireless LAN	100.0	56549	100.0	37330423	3415 k	23670	2986891	273 k
Malformed Packet	0.2	131	0.0	5855	535	131	5855	535
Logical-Link Control	0.3	155	0.5	194164	17 k	0	0	0
Systems Network Architecture	0.0	4	0.0	6080	556	0	0	0
Malformed Packet	0.0	1	0.0	2939	268	1	2939	268
Data	0.0	3	0.0	3141	287	3	3141	287
Spanning Tree Protocol	0.0	1	0.0	115	10	1	115	10
Remote Program Load	0.0	1	0.0	135	12	1	135	12
Data	0.3	145	0.5	187134	17 k	145	187134	17 k
802.1X Authentication	0.0	4	0.0	700	64	4	700	64
IEEE 802.11 wireless LAN management frame	3.3	1847	2.1	800648	73 k	1703	581373	53 k
Malformed Packet	0.3	144	0.6	219275	20 k	144	219275	20 k
IEEE 802.11 wireless LAN extension frame	0.5	257	1.0	366738	33 k	241	341387	31 k
Malformed Packet	0.0	16	0.1	25351	2319	16	25351	2319
IEEE 802.11 wireless LAN aggregate frame	0.1	49	0.2	64782	5926	49	64782	5926
Data	53.8	30440	88.2	32911345	3010 k	30440	32911345	3010 k

No display filter

Close Copy Help

Figure 5.19: Wireshark Protocol Hierarchy Statistics

Applied Analysis

When a WLAN problem is reported and you are called on-site to troubleshoot it, an initial scan of network health is a good place to start. Two of the initial metrics to assess are utilization and frame errors.

Frame errors can be measured either by looking at CRC errors or the Retry count. These values are not the same. The CRC calculation is performed by the radio driver of the analysis machine so that the software knows whether or not to trust a certain frame. Your machine may calculate a CRC error, but this does not necessarily mean that the frame's intended recipient also calculated a CRC error. To get a better gauge of actual errors, look for frame retries, which are an indication that the first attempt at the frame transmission failed.

When it comes to network utilization, some analyzers have more capabilities than others. Only a few are capable of reporting channel utilization by airtime, but they are all capable of breaking down the traffic on a channel to investigate what types of traffic are using the airtime. Basic channel utilization can be very helpful because it tells you how much of your channel's capacity is being used by your network. This identifies source problems like congestion or interference.

As you look at network utilization with more granularity, you can pinpoint other problems such as too much overhead (high number of management and/or control frames) or channel congestion caused by low data rates. Figure 5.20 shows a network utilization graph in OmniPeek. You can see an increase in utilization occur in about the middle of the graph and then it tapers off throughput. This was an intentional large file transfer initiated at that point.

By understanding the expected and desired behavior on your network you can draw

conclusions about acceptability of the displayed values. This requires that you have measured your network when it is operating normally to understand typical baselines. Some statistics have predictable ranges of acceptable values. There are no absolute “right” measurements in many cases. Each network is different, and application performance is the key criteria.

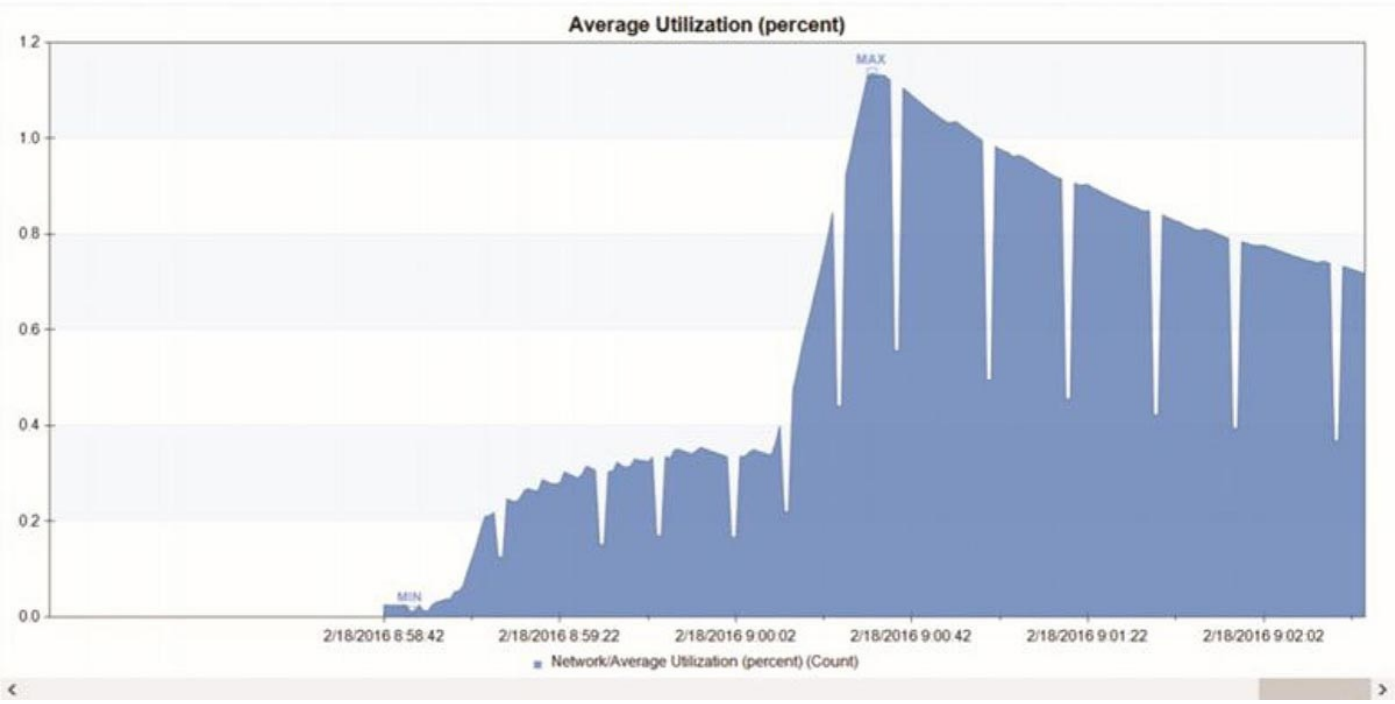


Figure 5.20: OmniPeek Network Utilization Graph

Capacity analysis is an important periodic action the WLAN analyst should take. The goal is to ensure continued performance of the WLAN and sufficient capacity for current user needs. Look for the following issues to measure WLAN performance related to capacity:

- **CCI and ACI:** A quick channel scan can identify the nearby APs and their operating channels. High AP counts per channel may warrant a new survey or redesign, or disabling selected radios.
- **Retries and CRCs:** Retries are the best indicator to measure congestion, though fairly accurate CRC measurements can be gained very near the AP.
- **Load Planning:** Evaluate the client load per AP. If you see this growing over time, you can predict when more APs or newer PHY/MACs will be required to accommodate the load.
- **Protocol Overhead:** Evaluate protection mechanisms (RTS/CTS), data rates used, fragmentation, contention, and retries to measure the impact of overhead on network performance.

Channel performance is another important consideration. WLAN analyzers are capable of breaking down statistics for each channel or node. Deeper inspection of these metrics is key to isolating network-wide or device-specific problems. Some problems are easily identified by looking at:

- Channel utilization
- Retry count

- Usage breakdown by frame types (how many frames/bytes of each frame subtype)
    - These metrics can tell you how much management or control overhead exists on the network
- Usage breakdown by data rate (how many frames/bytes at each data rate)
    - These metrics can help identify the impact that lower data rates may have on your network's overall capacity

Channel utilization conversations often lead us down the path of wireless contention domains and WLAN design. When channel performance problems are detected, an RF site survey is often a necessary step in the resolution process. Figure 5.21 shows a channel view in Wi-Fi Analyzer Pro.

Figure 5.21: Channel Utilization in Wi-Fi Analyzer Pro

Various statistics are made available by WLAN protocol analyzers. Figure 5.22 shows the WLAN Statistics tab in OmniPeek. This tab reveals the current signal strength, total bytes and retry packets. All of these are very important statistics for analysis.

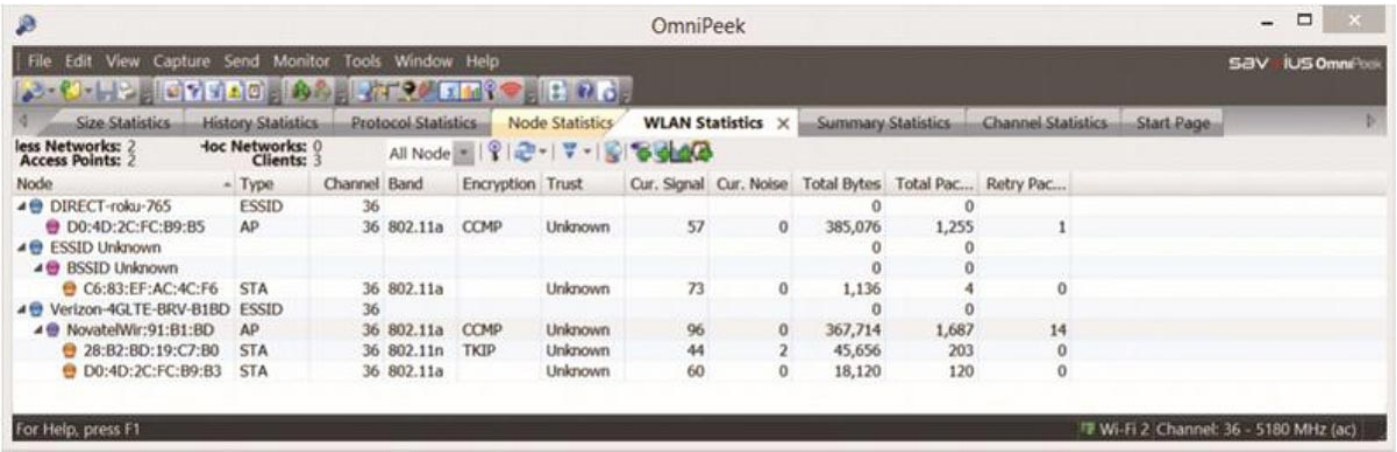


Figure 5.22: WLAN Statistics

Packet size distribution is also an important measurement. It informs the analyst of the kinds of traffic on the WLAN. When most of the traffic is very large, this indicates heavy use of either streaming video or file transfers of some sort. When most of it is smaller traffic, it probably indicates applications like VoIP and Web browsing. Figure 5.23 shows the Packet Size Distribution graph from OmniPeek.

Figure 5.24 shows the screen in CommView for WiFi. This screen provides information about the selected channel. Provided information includes:

- Signal levels for the top 10 nodes

- Packets per second in the channel
- Megabytes per second in the channel
- Data rates used
- Retry percentage (not in view in Figure 5.24, but available when scrolling down in the lower right panel)
- Percentage breakdown for management, control and data frames
- CRC error tracking

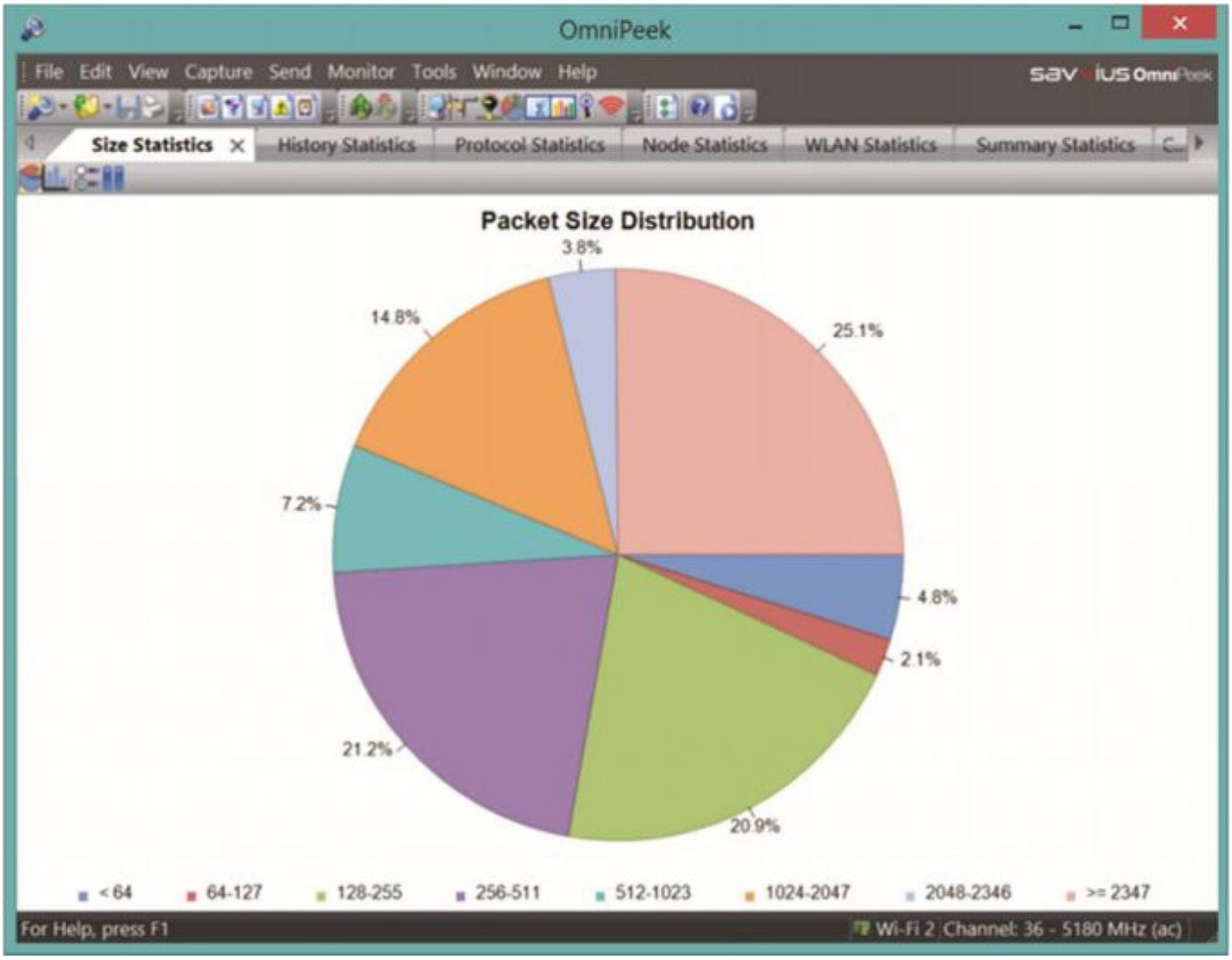


Figure 5.23: Packet Size Distribution

With this information, you can get a clear picture of the health of the channel. When you see very low data rates used for data frames, it is an indication of signal strength problems, interference issues or low data rate PHY devices. When you see high retry percentage rates (certainly above 10%), it may indicate CCI, ACI, non-Wi-Fi interference, or hidden node problems. Higher percentages of control frames may indicate use of protection mechanisms like RTS/CTS. The point is that viewing a screen like that in Figure 5.24 periodically at various locations on your network can reveal potential problems and help you to proactively solve them.

As you can see from the information in this section, WLAN protocol analyzers are powerful tools for troubleshooting and analysis in today's WLANs. Choosing the right

tool is a factor of features, adapter capabilities, and OS support and budget constraints. When you select a protocol analyzer, dive in and learn its specific features that are beyond the scope of this material. Here in this text, I want to ensure you understand the common features and capabilities of protocol analyzers and are able to utilize them for your troubleshooting processes.

However, WLAN protocol analysis alone is not sufficient in our modern networks. Wired analysis is also key to understanding the entire network environment. The next brief section of this chapter introduces wired analysis. Many excellent references are available for more detail on wired networking analysis including the in-depth Wireshark Network Analysis, Second Edition by Laura Chappell, and Practical Packet Analysis by Chris Sanders. In addition to this CWAP Official Study Guide, these three books provide a complete library of information on protocol analysis for wired and wireless networks.

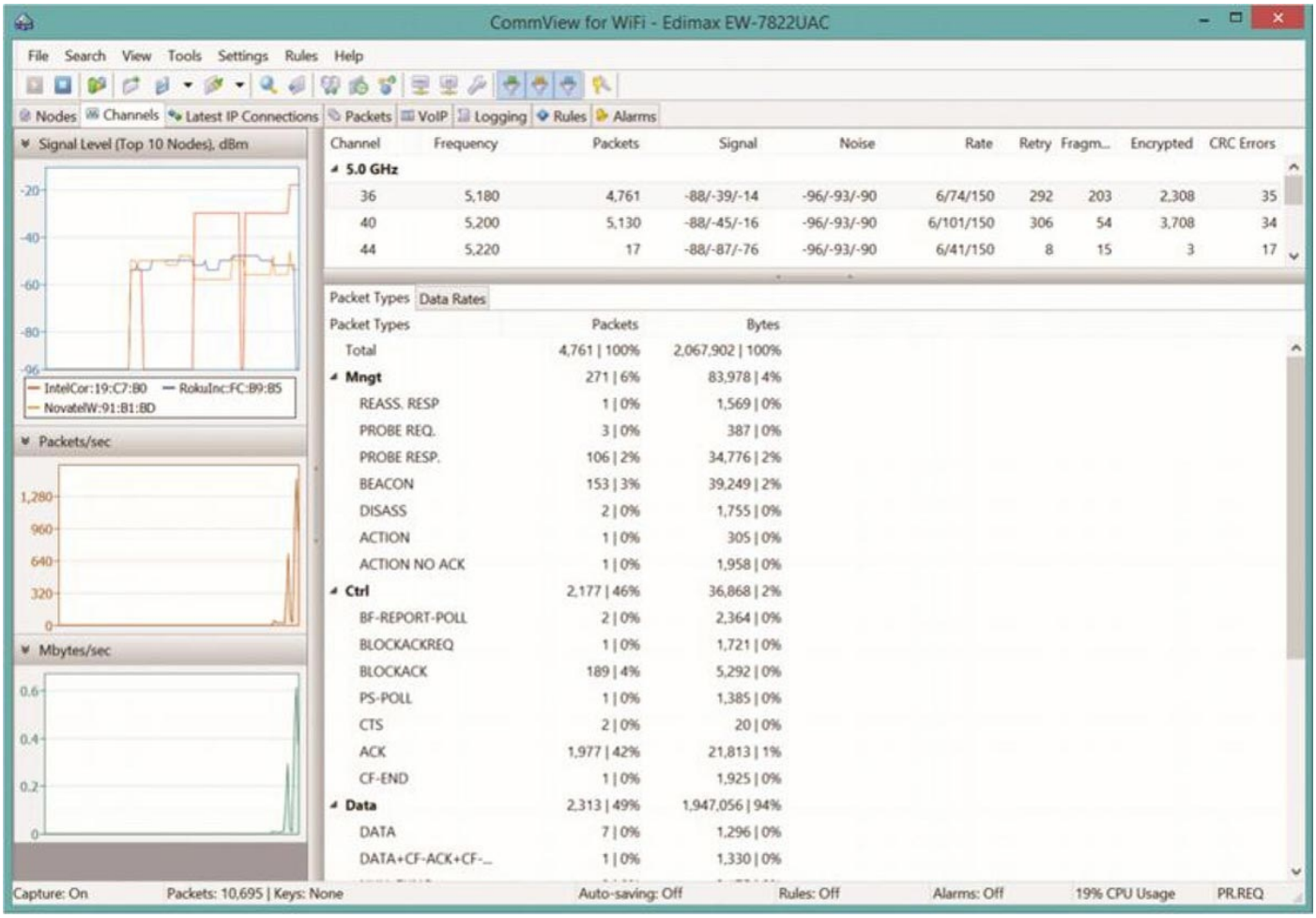


Figure 5.24: CommView for WiFi Channel Display

Wired Traffic

We cannot leave the topic of protocol analysis without speaking briefly of wired traffic analysis. Many problems that occur for WLAN clients are actually problems with the wired network, or services that are made available by the wired network. Therefore, capturing and analyzing wired traffic is also important.

Capturing Wired Traffic

Unlike enterprise WLANs, wired traffic is not typically encrypted on enterprise networks. It is a more trusted communication medium because the data is not sent over-the-air, but within wires. This fact is helpful when troubleshooting wired-side issues. You can see the actual details of DHCP requests, DNS communications, NTP packets, and more that are frequently obscured when capturing on secure WLANs.

Wireshark is also an excellent protocol analyzer for wired-side capture as it works with practically any Ethernet adapter. The key factor is determining where to capture the packets. This will be decided based on the problem scenario.

For example, if you are troubleshooting QoS issues, placing the Wireshark analyzer between the switch and the final destination device can reveal whether QoS tags made it through the network or not. If they did not, you can then backtrack through the network until you locate the device that is dropping the QoS tags. More information about QoS troubleshooting is found in Chapters 7 and 8.

Due to the fact that wired communications are mostly full-duplex with switches today, it is also important to consider how to capture the traffic. Two primary options are used today:

- **Port Mirroring (Port Spanning):** This option is configured in the switch and basically takes all the frames passing through a given interface and sends them through the mirrored interface as well. This works well in many environments. To use it effectively, the wired network should provide an open port for analysis in each switch.
- **Hubbing Out:** This option is implemented by plugging the Ethernet cable from the monitoring target into a hub as well as the analyzer. Then connect the hub to the switch. A hub sends out all data on all ports, so this method works even when no available ports exist in the switch for port mirroring or when port mirroring is not supported by the switch (such as an unmanaged switch).

Hubbing out is not very effective if your goal is performance monitoring. The hub will degrade the performance significantly, particularly since most available hubs only support 100 Mbps. An alternative would be switching out. In this case, you would use a small managed switch (portable in nature) that supports port spanning or port mirroring. It would work in the same way, but you could permanently configure it to span a given port so that it is ready to use. An example of such a device is the NETGEAR ProSAFE® GS108E 8-Port Gigabit Web Managed (Plus) Switch (GS108E-300NAS) shown in Figure 5.25.

Figure 5.25: Small NETGEAR Managed Switch for Capturing Ethernet Frames

Note: **Networking taps are also available. These are special devices designed for network monitoring. They look much like a switch or a hub, but are design for this purpose.**

Analyzing Wired Traffic

In relation to WLANs the primary wired traffic analysis tasks are related to the following topics which are covered in detail in Chapter 7:

- **DHCP traffic analysis:** It is common for a WLAN client to connect but be unable to use the network because of DHCP issues. Looking at DHCP requests can help resolve these issues.
- **DNS traffic analysis:** DNS is used for several operations in relation to WLANs, including captive portals, lightweight AP operations, and access to internal services.
- **QoS traffic analysis**: QoS must operate end-to-end to be effective. Verifying proper QoS tagging throughout the network is essential to effective Voice-over-WLAN operations.
- **Service traffic analysis:** Many other services may be used by WLAN clients including onboarding, authentication and internal service access.

To analyze these wired networking communications, you can use Wireshark or another wired analyzer to capture and view the frames, dashboards, and expert analysis tools. Figure 5.26 shows the capture of DNS traffic on a wired network in Wireshark. Figure 5.27 shows QoS tagging in OmniPeek. Figure 5.28 shows DHCP operations in Wireshark. Figure 5.29 shows an NTP capture in Wireshark.

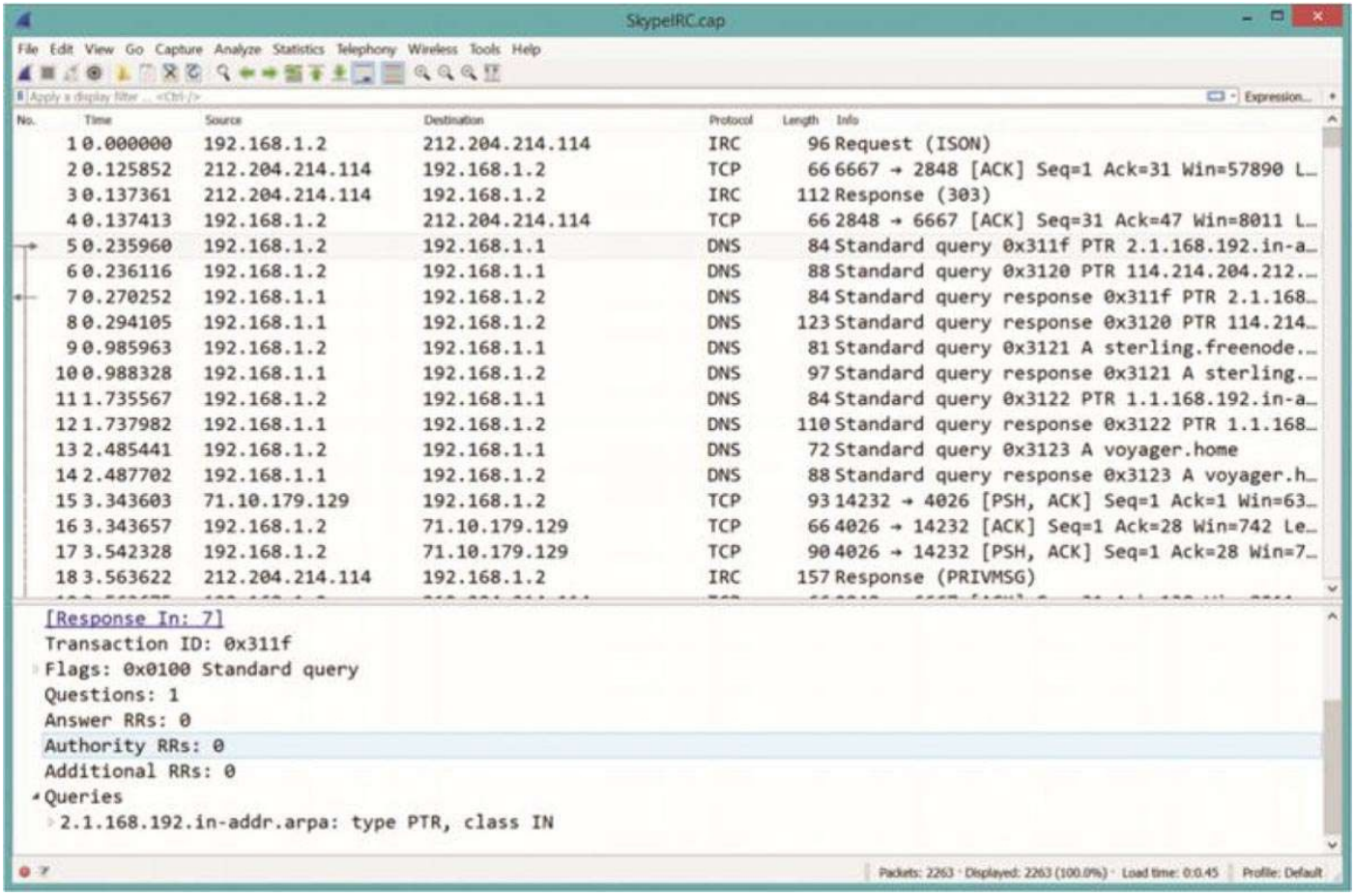


Figure 5.26: DNS Traffic in Wireshark

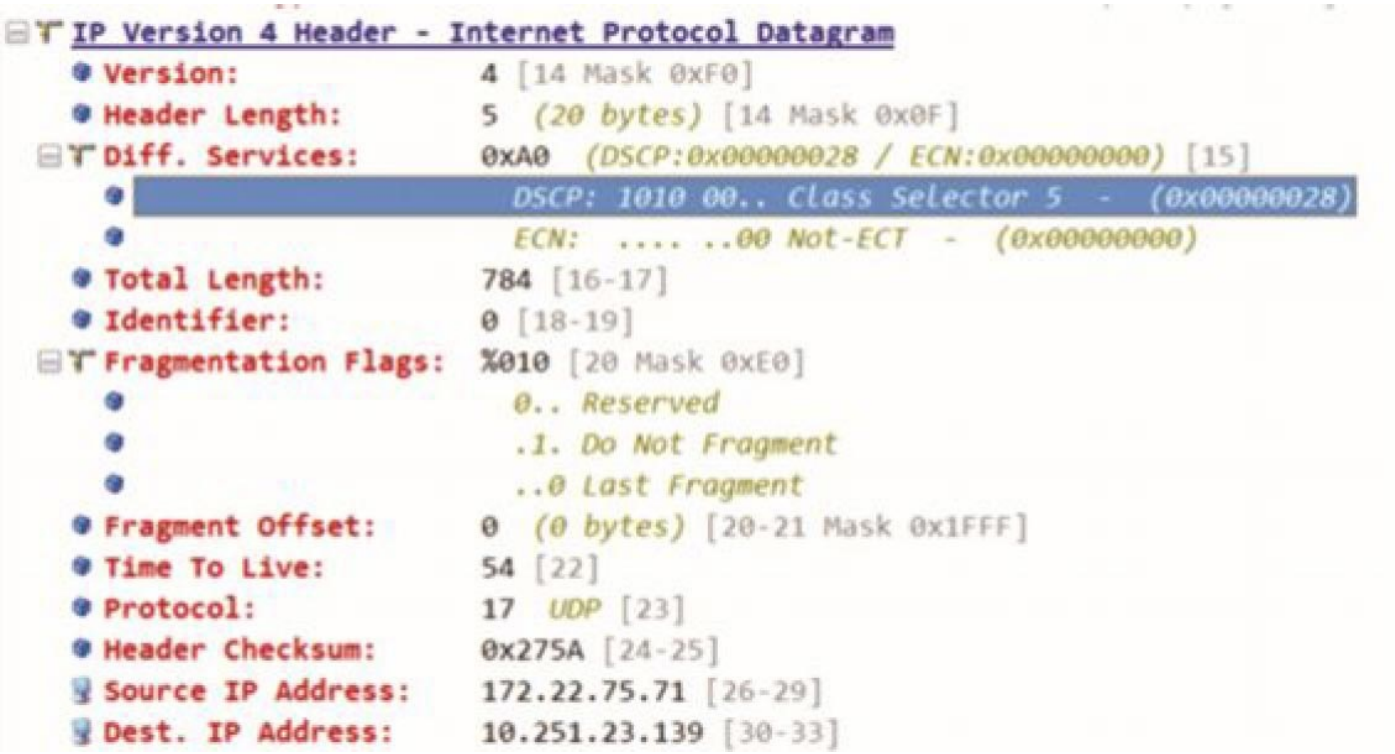


Figure 5.27: QoS Tags in OmniPeek

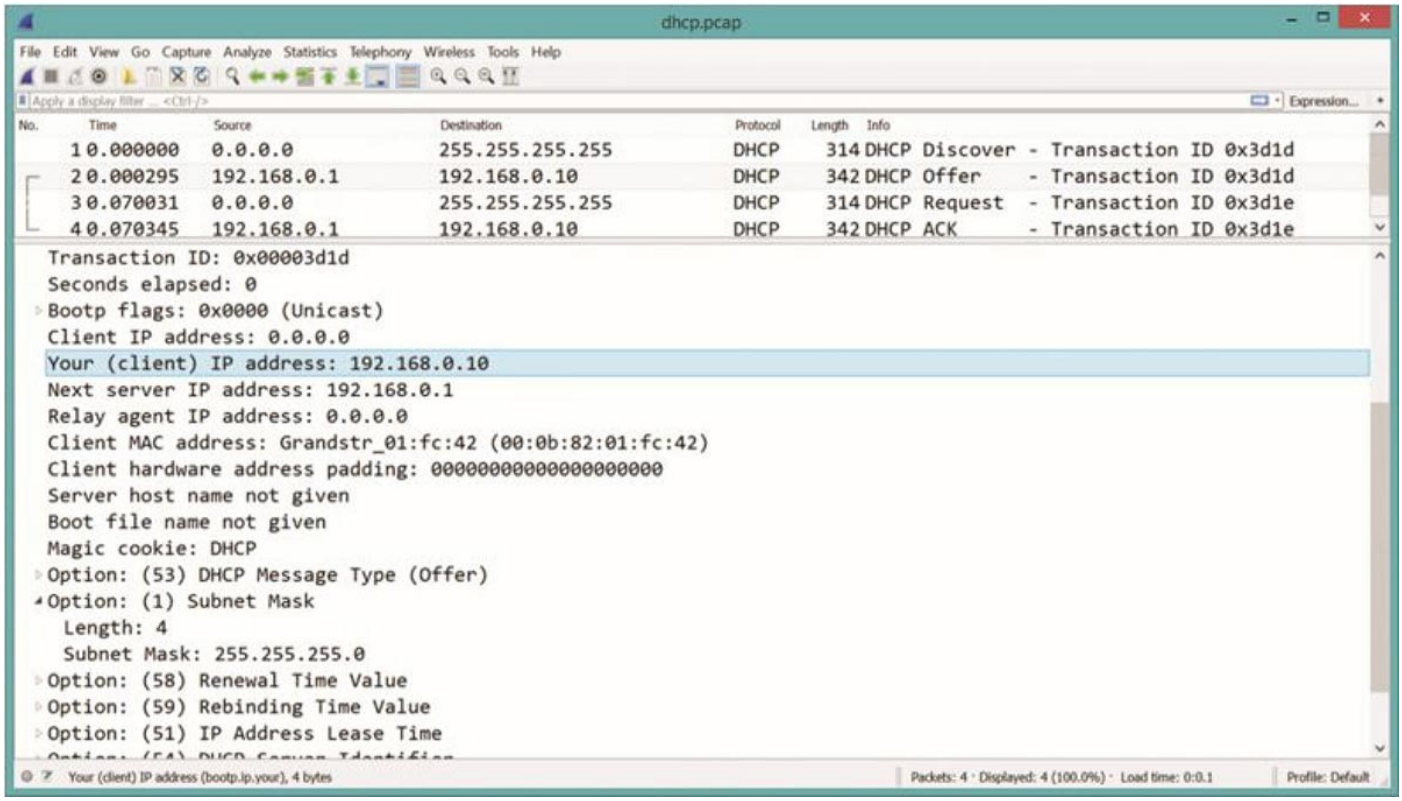


Figure 5.28: DHCP Operations in Wireshark

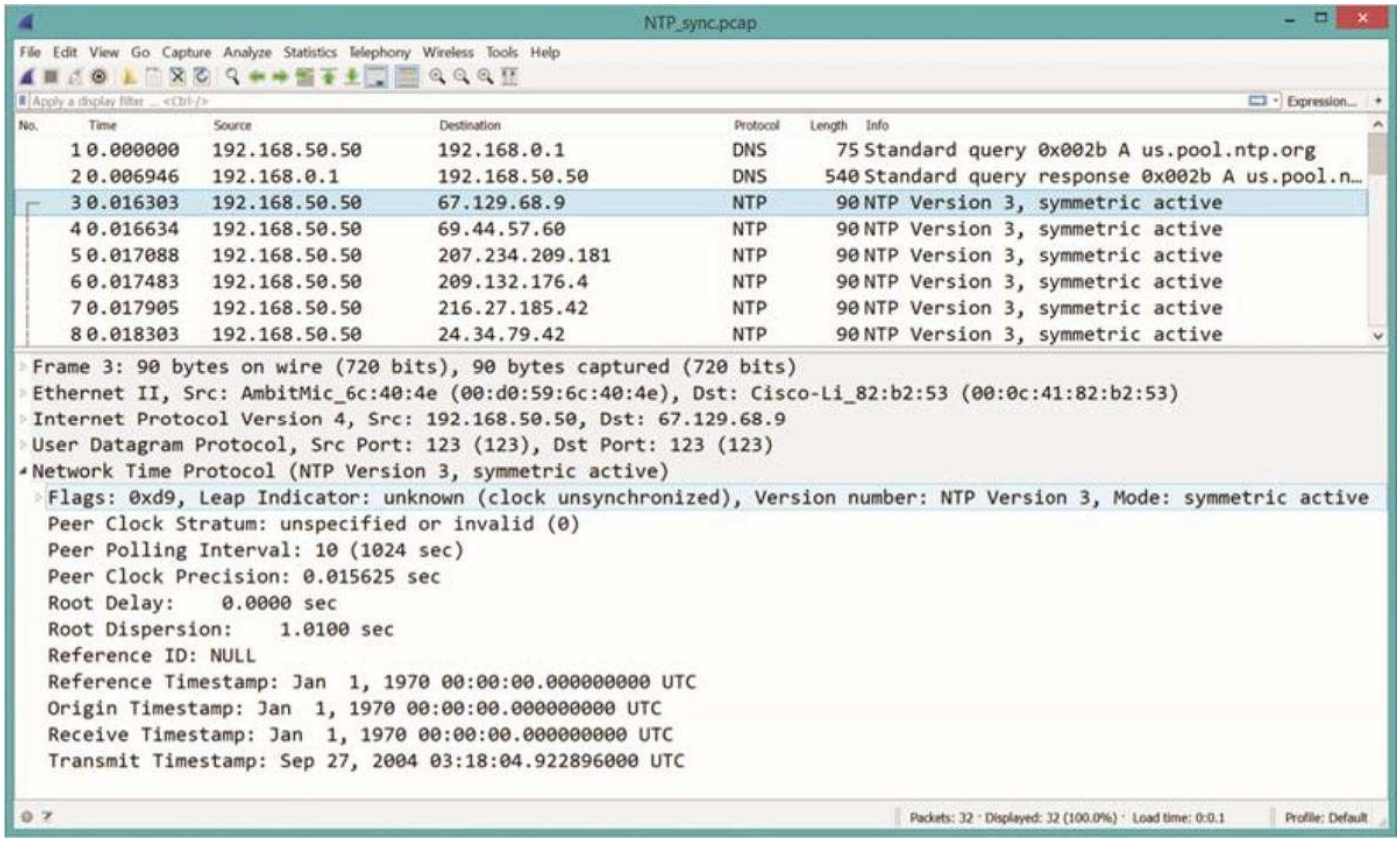


Figure 5.29: NTP Protocol Operations in Wireshark

Chapter Summary

In this chapter, you learned about protocol analyzers and how they are installed, configured and used to capture and analyze traffic. The lessons learned in this chapter will be applied to common troubleshooting scenarios in Chapters 7 and 8.

Review Questions

1. Which one of the following is not a key factor in selecting a protocol analysis solution for laptop-based or mobile analysis?
    a. Adapter hardware
    b. Operating system
    c. Drive spindle speed
    d. Analysis software
2. When using an infrastructure protocol analyzer, what device captures the 802.11 frames?
    a. Laptop
    b. AP
    c. Ethernet switch
    d. USB adapter
3. When a capture adapter uses an Express Card interface, what device will be used in combination with it to build a protocol analyzer solution?
    a. Laptop
    b. AP
    c. WLAN controller
    d. USB port
4. Which one of the following is not a solution for powering an AP used in a mobile capture solution?
    a. Wall outlet power
    b. PoE injector
    c. PoE switch
    d. Ethernet hub
5. Which one of the following is an open source protocol analysis solution?
    a. OmniPeek
    b. Wireshark
    c. CommView for WiFi
    d. Wi-Fi Analyzer Pro
6. In addition to the basic PHY/MAC support based on the standard, what else must be supported to capture all frames transmitted on the BSS?
    a. 802.1p

b. IPSec

c. 802.3 bridging

d. Spatial streams

7. In what mode must an adapter be able to run in order to capture all WLAN frames and not simply the frames in and out of the capture computer?

   a. Ad-hoc

   b. Enterprise

   c. Intelligent

   d. Promiscuous

8. What does it mean to say that an adapter is in monitor mode?

   a. It passes the frames up to the decoder for processing

   b. It shows information but doesn't retain it

   c. It is able to see WLANs, but cannot capture the frames

   d. It can capture frames, but cannot decode them

9. What is it called when a protocol analyzer captures a few frames from each channel as it moves from channel to channel dwelling for only a fraction of a second or a few seconds on each channel?

   a. Scanning

   b. Bandsteering

   c. Airtime fairness

   d. Overclocking

10. Why would you use packet truncating (also called packet slicing)?

    a. To retain the frame body but remove the header information

    b. To reduce the size of the capture file but retain the important header information

    c. To capture only every other frame

    d. To capture only frames matching the truncating filter

11. Which one of the following is not a common view provided by a decode engine for display in a protocol analyzer?

    a. ASCII

    b. Hexadecimal

    c. Rich text format

    d. Hierarchical decode

12. What is used as the criteria for colorization in Wireshark? (Choose the single best

answer.)

a. Filters

b. MAC addresses

c. IP addresses

d. ASCII codes

13. When using dashboards and other visual display tools in a protocol analyzer, what feature is being used?

    a. Expert analysis

    b. Packet decode

    c. Packet export formatting

    d. Filtering

14. When licensing protocol analysis software, what is a common requirement?

    a. Hardware key

    b. Serial number

    c. Telephone call to support

    d. Windows 8.1 or higher

15. What can be used with protocol analysis software to tag frames based on the location of the analyzer at the time of capture?

    a. Cellular triangulation

    b. Wi-Fi triangulation

    c. GPS

    d. Switchport MAC address

16. When a protocol analyzer captures to a buffer, where is the capture stored?

    a. Disk

    b. In the AP

    c. Memory (RAM)

    d. In the controller

17. When a protocol analyzer lists a vendor name without you entering it for captured devices, how is this determined?

    a. OUI MAC address

    b. Complex algorithms that do signature detection

    c. Vendor-specific elements in the frame

    d. Vendor-specific elements in the signal

18. What may cause a variation in signal strength report between an AP and an analyzer located very close to the AP?
    a. Quality of the components in the adapter
    b. Shannon-Hartley theorem
    c. Lack of PHY support
    d. Lack of MAC support
19. When you are experiencing problem reports from all users in a BSS, what is the best location to use for WLAN packet capture?
    a. Near the client farthest from the AP
    b. Near the AP
    c. On the wired LAN
    d. Near the user who complained the most
20. Why would you apply filtering in display instead of during frame capture?
    a. To ensure that frames are captured from all client STAs
    b. To ensure that the capture file complies with privacy policies
    c. To ensure that the capture file is as small as possible
    d. To ensure that all possible frames are available for analysis
21. To what does the delta time typically refer in a protocol analyzer?
    a. The time between consecutive packets
    b. The time the packet was transmitted on the WLAN
    c. The time the packet was bridged through the AP to the wired LAN
    d. The time the protocol analyzer first started capturing packets
22. What is the operator used in Wireshark to indicate “equals”?
    a. =
    b. ==
    c. !=
    d. <>
23. What Wireshark filter will show only 80 MHz frames?
    a. wlan_radio.11ac.bandwidth == 4
    b. radiotap.channel.flags.2ghz == 1
    c. wlan.analysis.retransmission
    d. wlan.fc.type_subtype == 0x1
24. What dialog in Wireshark is used as an expert analysis tool to show the percentage

of packets sent at varying size ranges?

a. I/O Graph

b. Packet Lengths

c. Frame Buffers

d. Top Talkers

25. You are troubleshooting performance problems in a WLAN. After adding several new client STAs that use 802.11g adapters, the network performance has degraded. What can be evaluated to measure protocol overhead in 802.11 BSSs?

a. Protection mechanisms

b. Use of MCS 9

c. CCI

d. ACI

Review Question Answers

1. **C** is correct. Very few laptops would have hard drives too slow to accommodate protocol capture today. The drive spindle speed would not be a likely factor.
2. **B** is correct. Of the listed items, the AP is the correct answer. The controller may actually capture the frames when using centralized forwarding models, but given that this was not an option, the only correct answer is that the AP captures the frames in an infrastructure protocol analyzer.
3. **A** is correct. Laptop computers are used with USB adapters, internal adapters, and Express Card adapters to capture 802.11 frames. APs that capture frames use the built-in radios. WLAN controllers that capture frames save the frames sent to them from the lightweight APs.
4. **D** is correct. You can power an AP used in a mobile capture solution with wall outlet power, PoE injectors and PoE switches. Hubs do not offer PoE.
5. **B** is correct. Of the listed protocol analyzers, only Wireshark is open source. The other protocol analyzers require software licenses to use them. In the past, some of these vendors offered free versions of their software, but they do not any longer.
6. **D** is correct. If the AP and some clients support three spatial streams, for example, and the capture adapter only supports two spatial streams, it will not be able to capture all frames transmitted on the BSS.
7. **D** is correct. An adapter running in promiscuous mode captures all frames and not only those destined for the analysis machine. To capture 802.11 frames, you must use an adapter that operates in promiscuous mode and is supported by the protocol analysis software.
8. **A** is correct. When an adapter is in monitor mode, it passes the 802.11 frames to the protocol analyzer decoder. Without monitor mode, only the upper layer information is sent to the analyzer.
9. **A** is correct. Protocol analyzers perform scanning by capturing frames on each channel for a small fragment of time. This mode provides an overview of the activity in the area, and if the dwell time is long enough it will show the active STAs in the BSSs.
10. **B** is correct. Packet truncating or slicing keeps the frame headers but removes all or much of the frame body. This is useful in reducing the size of capture files or limiting the consumption of buffer space.
11. **C** is correct. Protocol analyzers provide ASCI, hexadecimal, binary, and hierarchical decodes of the frames. If they use a Rich Text component to display the information, that is possible, but it is not considered a Rich Text view.
12. **A** is correct. Wireshark uses the filter engine for colorization. The process involved creating a color rule with a name and assigning a filter to it.
13. **A** is correct. Expert analysis includes the protocol analyzer options that go beyond

simple frame decodes. It may include dashboards, reports, and wizards.

14. **B** is correct. A serial number is required by all popular protocol analyzers. Some may also require a license file. Hardware keys have become less common today. Protocol analysis software may be associated with an adapter, an internal MAC address, or simply activated with the serial key.
15. **C** is correct. The Global Positioning System (GPS) can be used to tag frames with the location of the analyzer during frame capture. This can be useful as a reminder of the location where you captured the frames if viewing them at a much later time or sending them to another analyst for review.
16. **C** is correct. Protocol analyzers use RAM memory for buffers. Captures can be stored only in the buffer or also on disk.
17. **A** is correct. In most cases the Organizationally Unique Identifier (OUI) portion of the MAC address is used to define the vendor. Vendors, such as Apple, Cisco, Intel, etc. are assigned these OUIs by a central governing body.
18. **A** is correct. Enterprise APs typically use higher-quality components than clients or client adapters. This quality can impact the received signal and cause a disparity between the protocol analyzer and the AP.
19. **B** is correct. When all clients are reporting problems, capturing near the AP is the best first step. Then you can move to other areas to perform analysis if required.
20. **D** is correct. Applying filters during capture discards frames. Applying filters only in the display ensures that all frames are available for analysis.
21. **A** is correct. The delta time is the time between consecutive packets.
22. **B** is correct. The operator used for “equals” in Wireshark filters is ==. The = operator will not work and return an indicator that the filter contains an error. The != operator is used for “not equal.”
23. **A** is correct. The wlan_radio.11ac.bandwidth == 4 filter will show only 80 MHz frames. The radiotap.channel.flags.2ghz == 1 filter will show only 2.4 GHz frames. The `wlan.analysis.retransmission` filter will show only retransmissions. The `wlan.fc.type_subtype == 0x1` filter will show only Association Response frames.
24. **B** is correct. The Packet Length dialog shows packet counts based on size ranges. It is useful in determining the percentage of frames sent based on size.
25. **A** is correct. Evaluating protection mechanisms, such as RTS/CTS, can be useful in discovering protocol overhead.

Chapter 6:

Spectrum Analysis

Objectives

3.4 Describe and implement WLAN analysis hardware for protocol analysis and spectrum analysis.

4.4 Define terminology related to spectrum analysis including SNR, duty cycle, sweep cycles, signal strength, resolution bandwidth, and utilization.

4.5 Understand the common functions and features of a protocol analyzer as it relates to WLAN analysis.

4.6 Demonstrate the ability to install, configure, and use a PC-based spectrum analyzer to analyze RF activity in an area.

4.7 Recognize RF patterns of common devices including 802.11 devices, Bluetooth devices, microwave ovens, wireless video devices, and cordless phones.

Chapter 5 provided an overview and guidance for protocol analysis. However at times, seeing the 802.11 frames is not enough. You cannot use protocol analyzers to effectively detect non-Wi-Fi interference, for example. In such scenarios a spectrum analyzer must be used. In this chapter, you will learn about spectrum analysis hardware and software. You will also learn and review terminology important for spectrum analysis. Finally, you will explore spectrum analyzer features and see several device patterns commonly encountered when troubleshooting WLANs.

Spectrum Analysis Hardware

The first step in performing spectrum analysis, like protocol analysis, is getting the right hardware and software. This section provides an introduction to these components. Later sections describe the features, functionality, and use of a spectrum analyzer.

Hardware

Two primary types of spectrum analyzers are used by WLAN analysts are mobile and integrated. Mobile spectrum analyzers, like protocol analyzers, use adapters in laptops. Integrated spectrum analyzers use APs to monitor the RF. Figure 6.1 shows two of the more popular mobile analyzers, AirMagnet Spectrum XT and Metageek Wi-Spy DBx.

Figure 6.1: Spectrum XT and Wi-Spy DBx Adapters

Both adapters shown in Figure 6.1 are USB-based. Older Card Bus adapters may still be used by some analysts, but are difficult to acquire today. The best part about spectrum analyzers is that they do not require PHY/MAC upgrades as new 802.11 standards come out in 2.4 GHz and 5 GHz, as they look at the RF and only at the RF. If the software used with them shows 802.11 information, it is from the 802.11 radio in the laptop and not from the spectrum monitoring adapter.

While the image does not necessarily reveal it, both the Spectrum XT and Wi-Spy DBx adapter support external antennas. This allows you to use directional antennas for device

location. You will learn more about antennas and their impact on RF propagation and spectrum analysis in a later section of this chapter.

Integrated spectrum analysis uses the AP radios and chipsets to monitor the spectrum. In some cases, spectrum views are only available in the Web-based management interface of the infrastructure. In other cases, such as with Cisco CleanAir®, spectrum analysis software on the local computer can pull and display the spectrum data from the AP.

Integrated spectrum analysis has many advantages for network resiliency when interference is present on some portions of the radio band and if the automated channel selection algorithm uses non-Wi-Fi spectrum information to make channel decisions. It can also be valuable for remote troubleshooting in distributed enterprises. With an integrated spectrum analyzer, the AP may collect non-Wi-Fi data on the same channel where it is serving clients; alternately, integrated analyzers may be deployed in an overlay fashion to provide full-time spectrum scans to detect problematic interference sources and for remote troubleshooting without impacting client access. When used as a full-time spectrum analyzer, the AP cannot serve clients.

More details are provided on analyzer capabilities, including resolution bandwidth and narrowband versus wideband operations, later in this chapter.

Software

The second piece to the spectrum analysis equation is the software. Three popular software applications are available for mobile analysis. They are AirMagnet Spectrum XT, Metageek Chanalyzer, and Cisco® Spectrum Expert™. Today, Spectrum Expert is used mostly with Clean Air infrastructure solutions, but it may be used with a Card Bus adapter if one is available.

Both AirMagnet Spectrum XT and Metageek Chanalyzer can connect to Clean Air infrastructure solutions and use USB-based adapters. Figure 6.2 shows the Spectrum XT interface and Figure 6.3 shows the Chanalyzer interface. The features and views of spectrum analyzers are discussed in more detail later in this chapter.

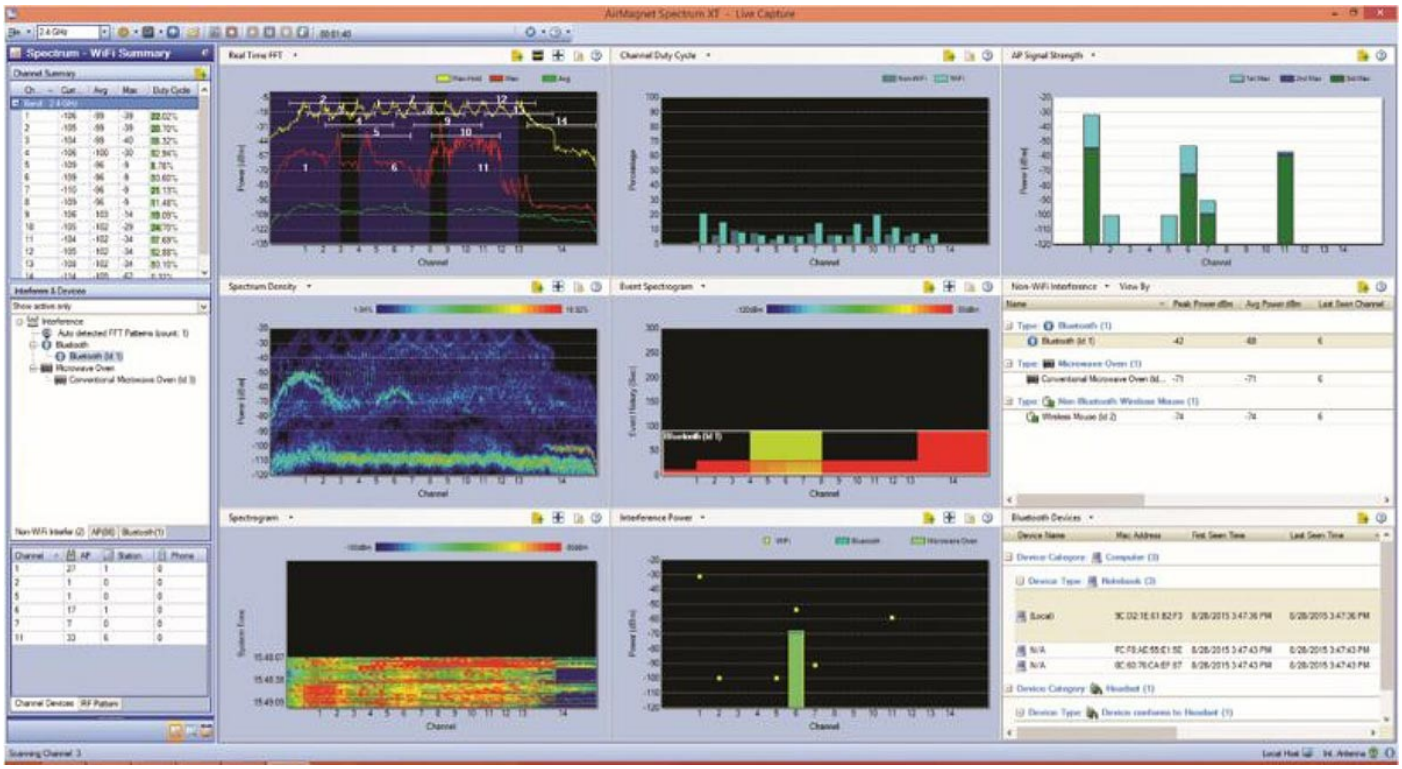


Figure 6.2: Spectrum XT

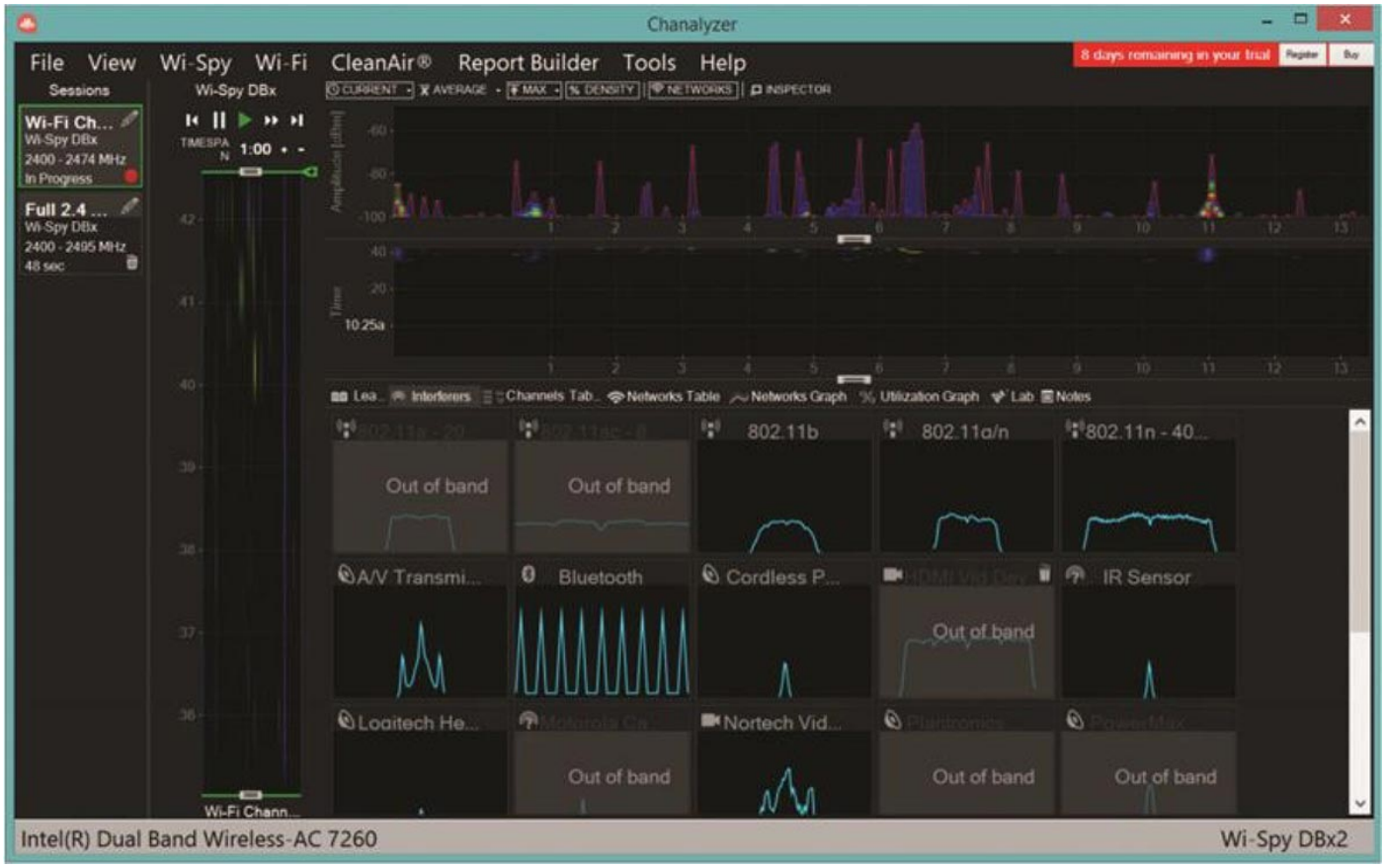


Figure 6.3: Chanalyzer

Terminology

To work with any system, you must understand the terminology. This section will review CWNA concepts needed for this discussion, and introduce new terminology unique to

spectrum analysis.

CWNA Terminology Review and RF Math

You might be wondering why you have go back to high school and study math to implement a network. After all, you have been able to implement wired networks for years with very little math other than counting the number of Ethernet ports needed for your users and making sure you buy 100 Mbps and 1 Gbps where needed. Wireless is different.

Because the wireless network uses an RF signal, you must understand the basics of RF math in order to determine if the output power of an RF transmitter is strong enough to get a detectable and usable signal to the RF receiver (or is so strong that you might be operating outside of regulations). You have to deal with similar issues with cabling in that you can only use a CAT 6 cable of a particular maximum length, but you did not really have to calculate anything most of the time. You simply know that you cannot span a greater distance than that which is supported by the cabling standards. The good news is that you do not have to really go back to high school. The bad news is that you might feel like it at times. I will make this coverage of RF math as easy to follow as possible, but it will become somewhat advanced out of necessity.

As you learned in your CWNA studies, you need to know a few basic things in order to fully understand RF math. First, you need to understand the units of power that are measured in RF systems. Second, you need to understand how to measure power gains and losses. Third, you need to understand how to determine the output power you will need at a transmitter in order to get an acceptable signal to a receiver. If you are creating a point-to-point connection using wireless bridges or if you are installing an AP in an access role, you will still need to understand these three basic concepts. In both wireless bridges and WLANs, a sufficient signal must reach the receiver listening on the other end of the connection.

Note: **For the real world, do not get too stressed over all this RF math. It is important, but you can plug the formulas into an Excel spreadsheet and let it do the work for you. For the CWAP exam, you will want to know the same rules of 10s and 3s from CWNA that are also discussed later in this chapter.**

<u>Watt</u>

The watt (W) is a basic unit of power equal to one joule per second. It is named after James Watt, an eighteenth-century Scottish inventor who also improved the steam engine among other endeavors. This single watt is equal to one ampere of current flowing at one volt. Think of a water hose with a spray nozzle attached. You can adjust the spray nozzle to allow for different rates of flow. The flow rate is comparable to amperes in an electrical system. Now, the water hose also has a certain level of water pressure–regardless of the amount that is actually flowing through the nozzle. The pressure is like the voltage in an electrical system. If you apply more pressure or you allow more flow with the same

pressure–either way, you will end up with more water flowing out of the nozzle. In the same way increased voltage or increased amperes will result in an increase of wattage since the watt is the combination of the amperes and volts.

Milliwatt

WLANs do not need a tremendous amount of power to transmit a signal over an acceptable distance. You can see a 7 watt light bulb from more than 50 miles (83 kilometers) away on a clear night with line of sight. Remember, visible light is another portion of the same electromagnetic spectrum and so this gives you an idea of just how far away an electromagnetic signal can be detected. For this reason many WLAN devices use a measurement of power that is 1/1000th of a watt. The unit of power is known as a milliwatt. 1 W, then, would be 1000 milliwatts (mW).

Enterprise class devices will often have output power levels of 1 mW to 100 mW while SOHO wireless devices may only offer up to 30 mW of output power. Some wireless devices may support up to 300 mW of output power, but these are the exception to the rule and tend to cause more problems than they are worth (as client STAs cannot match this or if it is in a client the AP does not match it). Ubiquiti Networks developed some such devices like their 300 mW CardBus wireless adapter and the 600 mW AP-ONE wireless hotspot solution, which was basically an AP with hotspot features and functionality.

For indoor use, it is generally recommended that you transmit at power levels of no more than 100 mW. In most cases, the minimum gain that will be provided by any connected antennas is2 dBi, which you will read about later. This means that the output power would actually be approximately 160 mW in the propagation direction of this antenna. This usually provides sufficient coverage for indoor WLANs (and actually in dense WLAN environments power is generally reduced to very low values). However, outdoor WLANs that are either providing coverage to a large outdoor area as either a public or private hotspot or are providing site-to-site links may use more power. The FCC limits the total output power from the antenna to 4 W for point-to-multipoint applications in the 2.4 GHz band, and this must be considered when implementing WLAN solutions.

> **EXAM MOMENT:** Know that the watt and the milliwatt are commonly used for RF measurements in WLANs. Remember that the milliwatt is 1/1000 of a watt and is represented as mW, while the watt is represented as simply W.

Decibel (dB)

The decibel is a comparative measurement value. It is a measurement of the difference between two power levels. For example, it is common to say that a certain power level is 6 dB stronger than another power level or that it is 3 dB weaker. These statements mean that a 6 dB gain and a 3 dB loss has occurred respectively.

Because a wireless receiver can detect and process very weak signals, it is easier to refer to the received signal strength in dBm rather than in mW. For example, a signal that is transmitted at 4 W of output power (4000 mW or 36 dBm) and experiences -63 dB of loss has a signal strength of .002 mW (-27 dBm). Rather than say that the signal strength is .002 mW, we say that the signal strength is -27 dBm. I will provide more details on the difference between dB (which is relative) and dBm (which is absolute) later in this section.

A decibel is 1/10th of a bel. You could equally say that a bel is 10 decibels. The point is that the decibel is based on the bel, which was developed by Bell Laboratories in order to calculate the power losses in telephone communications as ratios. The definition of a bel is simple: 1 bell is a ratio of 10:1 between two power levels. Therefore a power ratio of 200:20 is 1 bell (10:1) and 200:40 is .5 bels (5:1) and 200:10 is 2 bels (20:1). In the end, the decibel is a measurement of power that is used very frequently in RF mathematics.

You may have been asked the same question that I was asked as a child: Would you rather have $1,000,000 at the end of a month or one cent doubled in value every day for a month? Of course, the latter option is worth more than $5,000,000 by the end of the month. This is the power of exponential growth. RF signals experience exponential decay rather than growth as they travel through space. This is also called logarithmic decay. The result is a quickly weakening signal. This power loss is measured with decibels.

The decibel is relative where the milliwatt is absolute. The decibel is logarithmic where the milliwatt is linear. To understand this, you'll need to understand the basics of a logarithm, or you will at least need a good tool to calculate logarithms for you, such as a spreadsheet like Microsoft Excel.

> **EXAM MOMENT:** Remember that the decibel is used to measure differences in power levels and it is relative to an absolute value. Absolute values (watts and milliwatts) may be said to increase or decrease in decibels.

A logarithm is the exponent to which the based number must be raised to reach some given value. The most common base number evaluated is the number 10, and you will often see this referenced in formulas as log10. For example, the logarithm or log of 100 is 2 with a base of 10. This would be written:

```
log10(100) = 2
```

This is a fancy way of saying $10^2 = 100$, which is a shorthand way of saying 10 * 10 = 100. However, knowing the logarithm concept is very important in many RF-based math scenarios. You will need to be able to calculate power level problems for the CWAP exam. So how will you deal with these problems? Using the rules of 10s and 3s. This system will usually allow you to calculate RF signal power levels without ever having to resort to logarithmic math. Here are the basic rules:

1. A gain of 3 dB magnifies the output power by two.
2. A loss of 3 dB equals one half of the output power.
3. A gain of 10 dB magnifies the output power by ten.
4. A loss of 10 dB equals one tenth of the output power.
5. dB gains and losses are cumulative.

> **EXAM MOMENT:** Many who have passed the CWNA exam still struggle with this. On the professional level exams (CWAP, CWDP and CWSP), you will not be tested directly on the rules of 10s and 3s; however, you must still be able to do RF math problems. Be sure you have mastered this before exam day.

Now, let us evaluate what these five rules mean and the impact they have on your RF math

calculations. First, 3 dB of gain doubles the output power. This means that 100 mW plus 3 dB of gain equals 200 mW of power, or 30 mW plus 3 dB of gain equals 60 mW of power. The power level is always doubled for each 3 dB of gain that is added. Rule five stated that these gains and losses are cumulative. This means that 6 dB of gain is the same as 3 dB of gain applied twice. Therefore, 100 mW of power plus 6 dB of gain equals 400 mW of power. The following examples illustrate this:

```
40 mW + 3dB + 3dB + 3dB = 320 mW
40 mW * 2 * 2 * 2 = 320 mW
```

Both of these formulas are saying the same thing. Now consider the impact of 3 dB of loss. This scenario halves the output power. Look at the impact on the following formula:

```
40 mW + 3 dB + 3 dB - 3 dB = 80 mW
40 mW * 2 * 2 / 2 = 80 mW
```

Again, both of these formulas are saying the same thing. You can see, from this last example, how the accumulation of gains and losses are calculated. Now, rules three and four say that a gain or loss of 10 results in a gain of 10 times or a loss of 10 times. Consider the following example, which illustrates rules 3, 4, and 5:

```
40 mW + 10 dB + 10 dB = 4000 mW or 4 W
40 mW * 10 * 10 = 4000 mW or 4 W
```

As you can see, adding 10 dB of gain twice causes a 40 mW signal to become a 4000 mW signal, which could also be stated as a 4 W signal. Losses would be subtracted in the same way as the 3 dB losses were; however, instead of dividing by 2, we would now divide by 10 such as in the following example:

```
40 mW - 10 dB = 4 mW
40 mW / 10 = 4 mW
```

You should be beginning to understand the five rules of 10s and 3s. However, it is also important to know that the 10s and 3s can be used together to calculate the power levels after any integer gain or loss of dB. This is done with creative combinations of 10s and 3s. For example, imagine you want to know what the power level would be of a 12 mW signal with 16 dB of gain. Here is the math:

```
12 mW + 16 dB = 480 mW
```

But how did I calculate this? The answer is very simple: I added 10 dB and then I added 3 dB twice. Here it is in long hand:

```
12 mW + 10 dB + 3 dB + 3 dB = 480 mW
12 mW * 10 * 2 * 2 = 480 mW
```

Sometimes you are dealing with both gains and losses of unusual amounts. While the following numbers are completely fabricated, consider the assumed difficulty they present to calculating a final RF signal power level:

```
30 mW + 7 dB - 5 dB + 12 dB - 6 db = power level
```

At first glance, this sequence of numbers may seem impossible to calculate with the rules of 10s and 3s; however, remember that the dB gains and losses are cumulative, and that

this includes both the positive gains and the negative losses. Let us take the first two gains and losses: 7 db of gain and 5 db of loss. You could write the first part of the previous formula like this:

```
30 mW + 7 dB + (-5 dB) = 30 mW + 2 dB
```

Why is this? Because +7 plus -5 equals +2. Carrying this out for the rest of our formula, we could say the following:

```
30 mW + 7 dB + (-5 dB) + 12 dB + (-6 dB) = 30 mW + 2 dB +
6 dB
```

or

```
30 mW + 8 dB = power level
```

The only question that is left is this: How do we calculate a gain of 8 dB? Well, remember the rules of 10s and 3s. We have to find a combination of positive and negative 10s and 3s that add up to 8 dB. Here's a possibility:

```
+10 + 10 - 3 - 3 - 3 - 3 = 8
```

If we use these numbers to perform RF dB-based math, we come up with the following formula:

```
30 mW + 10 dB + 10 dB - 3 dB - 3 dB - 3 dB - 3 dB = 187.5
mW
30 mW * 10 * 10 / 2 / 2 / 2 / 2 = 187.5 mW
```

To help you visualize the math, consider the following step-by-step breakdown:

```
30 mW * 10 = 300 mW
300 mW * 10 = 3000 mW
3000 mW / 2 = 1500 mW
1500 mW / 2 = 750 mW
750 mW / 2 = 375 mW
375 mW / 2 = 187.5 mW
```

In the end, nearly any integer dB-based power gain or loss sequence can be estimated using the rule of 10s and 3s. Table 6.1 provides a breakdown of dB gains from 1 to 10 with the expressions as 10s and 3s for your reference. From this table, you should be able to determine the combinations of 10s and 3s you would be able to use to calculate the power gain or loss from any provided dB value. Always remember that, while plus 10 is actually times 10, plus 3 is only times 2. The same is true in reverse in that minus 10 is actually divided by 10 and minus 3 is divided by 2.

> **EXAM MOMENT:** When you add 3 dB, you double the absolute power. When you add -3 dB (or subtract 3 dB), you halve the absolute power. When you add 10 dB, you multiple the absolute power by 10. When you add -10 dB (or subtract 10 dB), you divide the absolute power by 10.

Gain in dB	Expression in 10s and 3s
1	+ 10 – 3 – 3 – 3
2	+ 3 + 3 + 3 + 3 – 10
3	+ 3
4	+ 10 – 3 – 3
5	+ 3 + 3 + 3 + 3 + 3 – 10
6	+ 3 + 3
7	+ 10 – 3
8	+ 10 + 10 – 3 – 3 – 3 – 3
9	+ 3 + 3 + 3
10	+ 10

Table 6.1: Expressions of 10s and 3s

dBm

dBm is an absolute measurement of power where the *m* stands for milliwatts. Effectively, dBm references decibels relative to 1 milliwatt or that 0 dBm equals 1 milliwatt. Once you establish that 0 dBm equals 1 milliwatt, you can reference any power strength in dBm. The formula to get dBm from milliwats is:

```
dBm = 10 * log10(Power-in-mW)
```

For example, if the known milliwatt power is 30 mW, the following formula would be accurate:

```
10 * log10(30) = 14.77 dBm
```

The result of this formula would often be rounded to 15 dBm for simplicity; however, you must be very cautious about rounding if you are calculating a link budget because your end numbers can be drastically incorrect if you have performed a lot of rounding along the way. Table 6.2 provides a list of common milliwatt power levels and their dBm values.

One of the benefits of working with dBm values instead of milliwatts is the ability to easily add and subtract simple decibels instead of multiplying and dividing often huge or tiny numbers. For example, consider that 14.77 dBm is 30 mW as you can see in Table 6.2. Now, assume that you have a transmitter that transmits at that 14.77 dBm and you are passing its signal through an amplifier that adds 6 dB of gain. You can quickly calculate that the 14.77 dBm of original output power becomes 20.77 dBm of power after passing through the amplifier. Now, remember that 14.77 dBm was 30 mW. With the 10s and 3s of RF math, which you learned about earlier, you can calculate that 30 mW plus 6 dB is equal to 120 mW. The interesting thing to note is that 20.77 dBm is equal to 119.4 mW. As you can see, the numbers are very close indeed. While I have been using a lot of more exact figures in this section, you will find that rounded values are often used in vendor literature and documentation. Figure 6.4 shows a set of power level charts that can be used for simple mW to dBm and dBm to mW conversion.

mW	dBm
1	0.00
10	10.00
20	13.01 (rounded to 13)
30	14.77 (rounded to 15)
40	16.02 (rounded to (16)
50	16.99 (rounded to 17)
100	20.00
1000	30.00
4000	36.02 (rounded to 36)

Table 6.2: mW to dBM Conversion Table (rounded to two precision levels)

dBm	Watts	dBm	Watts	dBm	Watts
0	1.0 mW	16	40 mW	32	1.6 W
1	1.3 mW	17	50 mW	33	2.0 W
2	1.6 mW	18	63 mW	34	2.5 W
3	2.0 mW	19	79 mW	35	3 W
4	2.5 mW	20	100 mW	36	4 W
5	3.2 mW	21	126 mW	37	5 W
6	4 mW	22	158 mW	38	6 W
7	5 mW	23	200 mW	39	8 W
8	6 mW	24	250 mW	40	10 W
9	8 mW	25	316 mW	41	13 W
10	10 mW	26	398 mW	42	16 W
11	13 mW	27	500 mW	43	20 W
12	16 mW	28	630 mW	44	25 W
13	20 mW	29	800 mW	45	32 W
14	25 mW	30	1.0 W	46	40 W
15	32 mW	31	1.3 W	47	50 W

Figure 6.4: mW to dBM and dBm to mW Conversion Table

EXAM MOMENT: Remember a few mW to dBm comparisons for the exam. Examples include 1 mW equals 0 dBm, 10 mW equals 10 dBM, 100 mW equals 20 dBm, and 1000 mW equals 30 dBm. Also remember that negative values are used to represent low milliwatt power levels. For example, -10 dBm is 0.1 mW and -20 dBm is 0.01 mW.

dBi

dBi (the i stands for isotropic) is a measurement of power gain used for RF antennas. It is a comparison of the gain of the antenna and the output of a theoretical isotropic radiator. An isotropic radiator is an ideal antenna that we cannot create with any known technology. This is an antenna that radiates power equally in all directions. In order to do this, the power source would have to be at the center of the radiating element and be infinitesimally small. Since this technology does not exist, we call the isotropic radiator the ideal against which other antennas are measured. I will provide more details about dBi in the later section titled Isotropic Radiator. For now, just remember that dBi is a measurement of

directional gain in power and is not a power reference to the power fed into the antenna. The dBi value must be calculated against the input power provided to the antenna to determine the actual output power in the direction in which the antenna propagates RF signals.

dBd

Antenna manufacturers use both dBi, mentioned previously, and dBd to calculate the directional gain of antennas. Where dBi is a calculation of directional gain compared to an isotropic radiator, dBd is a calculation of directional gain compared to a dipole antenna. Therefore, the last *d* in dBd stands for dipole. Like dBi, dBd is a value calculated against the input power to determine the directional output power of the antenna.

What is the difference between dBi and dBd then? The difference is that a dBd value is compared with a dipole antenna, which itself has a gain of 2.14 over an isotropic radiator. Therefore, an antenna with a gain of 7 dBd has a gain of 9.14 dBi. Remember, to convert from dBd to dBi, just add 2.14. To convert from dBi to dBd, just subtract 2.14. To remember this, just remember the formula 0 dBd = 2.14 dBi.

Note: **I like to keep a spreadsheet for all the WLAN adapters in my inventory. For each one, I track the dBd and the dBi value. If the vendor does not provide one of the values, my spreadsheet calculates it with a formula. It is a great way to compare apples to apples when pulling adapters from inventory.**

Additional RF Terms

Four additional terms should be brought back to memory. They are frequency, wavelength, amplitude, and phase.

- **Frequency:** How often an RF wave oscillates over a period of time, measured as cycles per second (Hertz). 802.11 frequencies use either MHz (millions of cycles per second) or GHz (billions of cycles per second), such as 2400 MHz or 2.4 GHz.
- **Wavelength:** The physical distance of an RF wave for one cycle. This is measured from the same point in a wave to the same point in the previous or following wave.
- **Amplitude:** The power or strength of an RF wave.
- **Phase:** The fraction of a wave cycle that has elapsed relative to some point (or relative to another wave), measured in degrees.

Advanced RF Math

Now that you have the basics of RF math down, it is time to consider some of the more advanced uses of RF math. This section will cover the following concepts:

- SNR
- RSSI

- Link Budgets
- System Operating Margins
- Fade Margins
- Intentional Radiators
- EIRP

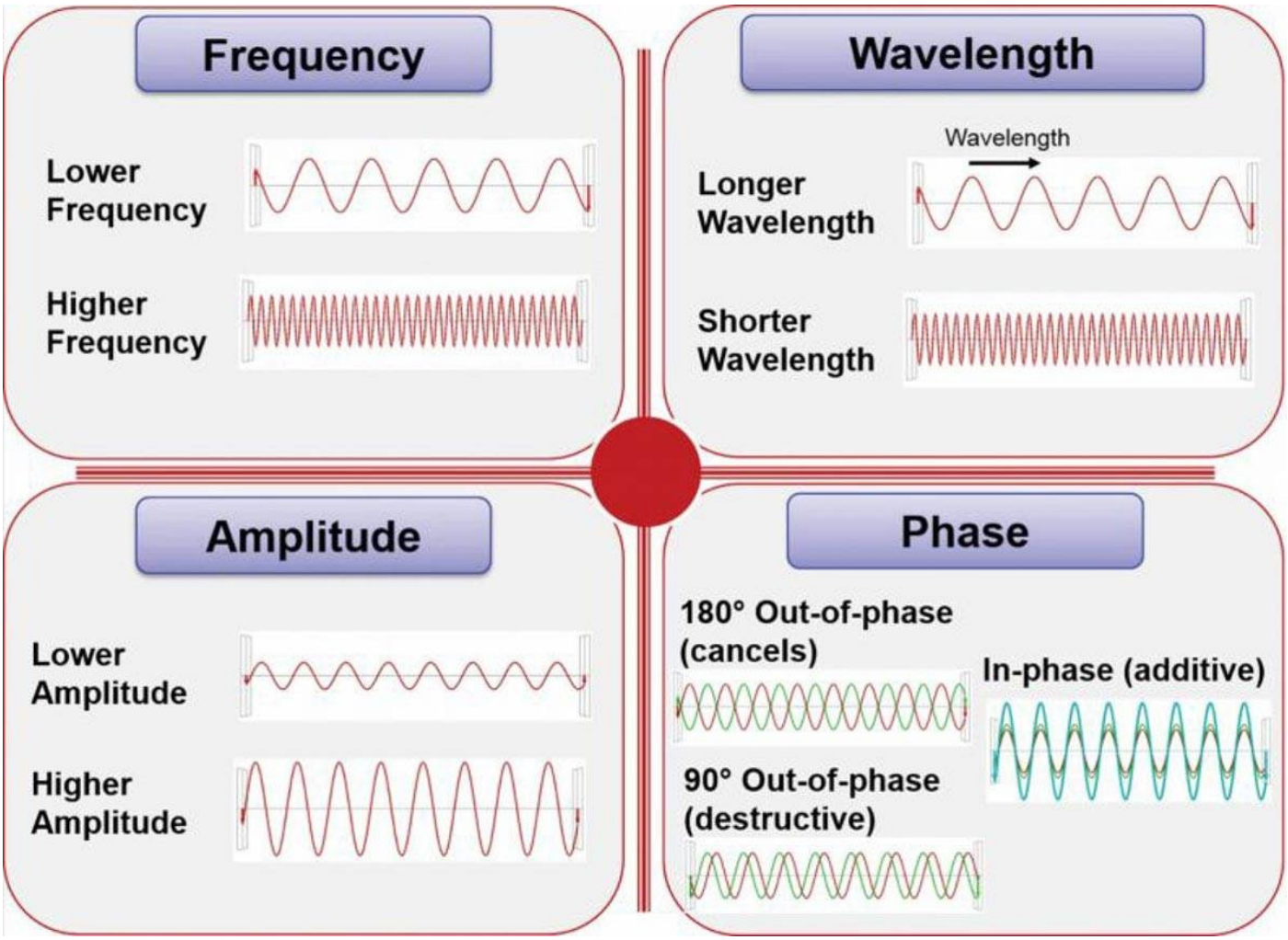


Figure 6.5: Illustrating RF Terms

<u>SNR</u>

Background RF noise, which can be caused by all the various systems and natural phenomenon that generate energy in the electromagnetic spectrum, is known as the noise floor. The power level of the RF signal relative to the power level of the noise floor is known as the signal-to-noise ratio (SNR). Hopefully this rings familiar from CWDP and CWNA.

Think of it like this. Imagine you are in a large conference room. Further, imagine that hundreds of people are having conversations at normal conversation sound levels. Now, imagine that you want to say something so that everyone will hear you; therefore, you cup your hands around your mouth and yell. You could say that the conversations of everyone else in the conference room is a noise floor and that your yelling is the important signal or information. Furthermore, you could say that the loudness of your yelling relative to the loudness of all other discussions is the SNR for your communication, but this SNR would

be measured at the ears of the hearers and not at your mouth. We measure SNR at the receiver because that is where it matters.

In WLAN networks, the SNR becomes a very important measurement. If the noise floor power levels are too close to the received signal strength, the signal may be corrupted, or it may not even be detected. It is almost as if the received signal strength is weaker than it actually is when there is more electromagnetic noise in the environment. You may have noticed that when you yell in a room full of people yelling, your volume does not seem so great; however, if you yell in a room full of people whispering, your volume seems to be magnified. In fact, your volume is not greater, but the noise floor is less. RF signals are impacted in a similar way.

Technically, SNR is defined as the difference between the noise floor and the signal of interest in dB. The formula for calculating SNR for RF networks is simple:

```
SNR = noise floor value in dBm - signal strength value in dBm
```

If the noise floor is rated at -95 dBm and the signal is detected at -70 dBm, the SNR is 25.

> **EXAM MOMENT:** Know how to calculate SNR. If given a noise floor rating value and a signal strength value, be prepared to calculate the SNR. Remember the simple formula of noise floor value - signal strength value = SNR. Know that the signal strength may be provided in mW and need conversion to dBM, but the mW value will usually be a basic value such as -0.1 or -0.01.

<u>RSSI</u>

The Received Signal Strength Indicator (RSSI) is an arbitrary measurement of received signal strength defined in the 802.11 standards. No absolute rule exists as to how this signal strength rating must be implemented in order to comply with the IEEE standard other than the fact that it is optional (though I have not encountered a vendor that has not implemented it in client devices in some way), it should report the rating to the device driver, and it should use 1 byte for the rating providing a potential range of 0 to 255.

In reality, no vendors that I have encountered have chosen to use the entire range. For example, Cisco uses a range of 0 to 100 (101 total values) in their devices and most Atheros-based chipsets use a range of 0–60 (61 total values). The IEEE does specify that a RSSI_MAX parameter should exist, which would be 100 for Cisco and 60 for Atheros and the maximum value is 255. The RSSI_MAX parameter allows software applications to determine the range implemented by the vendors and then convert the rating value into a percentage. It would not be very beneficial if the client software reported the actual rating to the user. Because of the different ranges used by the different vendors, using the actual rating would result in unusual matches. By this I mean that an RSSI rating of 75 in a Cisco client is the same relative rating as an RSSI rating of 45 in an Atheros chipset (assuming they are using similar linear stepping algorithms internally). Therefore, most applications use percentages.

If an Atheros-based client card reported a RSSI of 47, the software application could process the following formula to determine the signal strength in percentage:

```
47 / 60 * 100 = 78.3% signal strength
```

How does the software know to use the maximum value of 60? From the RSSI_MAX parameter that is required by the IEEE standard. Motorola/Symbol, for example, used an RSSI_MAX of 31. This means there is a total of 32 potential values with 31 of the values actually representing some level of usable signal strength. Most vendors have chosen to use an RSSI of 0 to represent a signal strength less than the receive sensitivity of the device and, therefore, a signal strength that is not usable. In the end, a RSSI of 16, with a Motorola/Symbol client would be 50% signal strength. A RSSI of 50 with a Cisco client would be 50% signal strength and a RSSI of 30 with an Atheros client would be 50% signal strength. This variance is why most client software packages report the signal strength in percentages instead of RSSI. The variability of RSSI calculations among vendors can be confusing, but is important to understand.

The formula to calculate percentages from RSSI values is:

```
Signal Strength Percentage = RSSI / RSSI_MAX
```

Where RSSI is the rating specified by the specific vendor chipset and RSSI_MAX is the highest RSSI rating possible. The result is the signal strength percentage value that you see in so many WLAN client software packages.

Now, let us make this even more complex—just for fun. Earlier I said that a Cisco rating of 75 is the same as an Atheros rating of 45, assuming the use the same linear stepping algorithm. By linear stepping algorithm, I am talking about the connection between dBm and RSSI rating. For example, one might assume that a dBm of -12 gets an RSSI rating of 100 for Cisco and that a dBm of -12 gets an RSSI rating of 60 for Atheros. It would make sense to assume that the RSSI_MAX parameter is equal to the same actual dBm signal strength with all vendors; however, since the IEEE leaves it up to the vendors to determine the details of RSSI implementation (mostly because it is an optional parameter anyway), the different vendors often use different dBm signal strengths for their RSSI_MAX parameter. What is the result of this complexity? You may show a 100% signal strength for one client device and show a lesser signal strength for another client device from the exact same location. Your assumption may be that the client device with the lesser signal strength is actually providing inferior performance when in fact they are identical or nearly so.

How can this be? Consider a situation where two vendors use a RSSI_MAX value of 100. However, one vendor (vendor A) equates the RSSI rating of 100 to -12 dBm and the other vendor (vendor B) equates the RSSI rating of 100 to -15 dBm. Now assume that both vendors use a linear stepping scale for their ratings, where a decrease in dBm of .7 causes the RSSI rating to drop by 1. This means that, at -15 dBm, vendor B will report 100% signal strength, but vendor A will have dropped the RSSI rating four times to a value of 96 and report a 96% signal strength. You can see how one might assume that vendor B’s client is performing better because it has a higher percentage signal strength when, in fact, the two clients simply use a different implementation of the RSSI feature.

Due to these incompatibility issues, RSSI values should only be compared with the values from other computers using the same vendor’s devices. RSSI values should never be conceptualized as universal or in any way determinant of the value of one vendor’s adapter over another vendor’s value. Apples must be compared with apples, or in other

words to avoid confusion, Ciscos with Ciscos and D-Links with D-Links.

The RSSI rating is also arbitrarily used to determine when to reassociate (roam) and when to transmit. Vendors will decide what the lowest RSSI rating should be before attempting to reassociate to a BSS with a stronger beacon signal. Additionally, vendors must determine when to transmit. To do this, they must determine a clear channel threshold. This is a RSSI value at which it can be assumed that there is no arriving signal and therefore the device may transmit.

> **EXAM MOMENT:** Remember that RSSI is the signal strength rating that is vendor-specific, even though it is based on limited IEEE standard specifications. Also, remember that the RSSI_MAX value determines the upper value of the RSSI rating.

Link Budget and System Operating Margin (SOM)

The term budget can be defined as a plan for controlling a resource. In a wireless network, the resource is RF energy and you must ensure that you have enough of it to meet your communication needs. This is done by calculating a link budget that results in a system operating margin (SOM). Link budget is an accounting of all components for power, gain, loss, receiver sensitivity, and fade margin. This includes the cables and connectors leading up to the antenna and the antennas themselves. It also includes the factor of free space path loss (FSPL or FPL). The many concepts we have been talking about so far in this chapter are about to come together in a way that will help you make effective decisions when building wireless links. You will take the knowledge you have gained of RF propagation and free space path loss from CWNA studies and the information related to RF math and use all of it to perform link budget calculations that result in a SOM.

When creating a financial budget, money management coaches often suggest to their clients that they should monitor how they are currently spending their money. Then they suggest that these individuals create a budget that documents this spending of money. The alternative would be to go ahead and create a financial budget without any consideration for what your expenses actually are. I am sure you can see that the latter simply will not work. First, you have to know how much money you need to live, and then you design your budget around that knowledge.

Note: **Link budgets in wireless connections are a lot like financial budgets. You have to meet your needs regardless of what you want. Make sure you have the signal strength needed for the data rate desired.**

Similarly, in WLAN links, you will need to first determine the signal strength that is required at the receiving device and then figure out how you will accomplish this with your link budget. The first calculation you should perform in your link budget is to determine the minimum signal strength needed at the receiver; this is called the receive sensitivity. Receive sensitivity is not a single dBm rating, but it is a series of dBm ratings required to communicate at varying data rates. For example, Table 6.3 shows the receive sensitivity scale for an older Cisco Aironet™ 802.11a/b/g CardBus adapter.

There are actually two ways to think of the receive sensitivity, the absolute weakest signal

the wireless radio can reliably receive and the weakest signal the wireless radio can reliably receive at a specific data rate. The lowest number in dBm, which is -94 dBm in Table 6.3, is the weakest signal the radio can tolerate. This number is sometimes referenced as the receive sensitivity or the absolute receive sensitivity. In more accurate terminology, the receive sensitivity of a card is the complete series or system of sensitivity levels supported by the card.

The receive sensitivity ratings are determined by the vendors. They will place the radio in a specially constructed, shielded room and transmit RF signals of decreasing strength. As the RF signal strength is decreasing, the bit-error rate in the receiving radio is increasing. Once this bit-error rate reaches a vendor-defined rate, the power level in dBm is noted and the radio is configured to switch down to the next standard data rate. This process continues until the lowest standard data rate for that 802.11-based device (1 or 6 Mbps) can no longer be achieved, and this dBm value becomes the lowest receive sensitivity rating. In the end, a lower receive sensitivity rating is better because it indicates that the client device can process a weaker signal.

dBm Power Level	Data Rate
-94 dBm	1 Mbps
-93 dBm	2 Mbps
-92 dBm	5.5 Mbps
-86 dBm	6 Mbps
-86 dBm	9 Mbps
-90 dBm	11 Mbps
-86 dBm	12 Mbps
-86 dBm	18 Mbps
-84 dBm	24 Mbps
-80 dBm	36 Mbps
-75 dBm	48 Mbps
-71 dBm	54 Mbps

Table 6.3: Cisco Aironet 802.11 a/b/g CardBus Adapter

The reason you need to know the receive sensitivity rating is that it is the first of your link budget calculations. The SOM is the amount of received signal strength relative to the client device's receive sensitivity. If you have a client device with a receive sensitivity of -94 dBm and the card is picking up the wireless signal at -65 dBm, the SOM is the difference between -94 dBm and -65 dBm. Therefore, you would use the following formula to calculate the link budget:

$$SOM = RS - S$$

Where S is the signal strength (the second link budget calculation used to determine the SOM) at the wireless client device and RS is the receive sensitivity of the client device. Plugging in our numbers looks like this:

```
SOM = (-94) - (-65)
```

The resulting SOM is 29 dBm. This means that the signal strength can weaken by 29 dBm, in theory, and the link can be maintained at some data rate. There are many factors at play when RF signals are being transmitted and this number, 29 dBm, will act as a good estimate. You may be able to maintain the link with a loss of 32 dBm and you may lose the link with a loss of 25 dBm. The link budget is a good estimate and should not be taken as a guarantee for connectivity. Additionally, you are often designing for higher data rates, so you will use the lowest data rate you are willing to accept to find the receive sensitivity and then to calculate the SOM.

Note: **Think of the receive sensitivity rating of a WLAN adapter as its "emotional intelligence." The receive sensitivity determines how sensitive it is to the signals passing by it much like a human's emotional intelligence level determines how sensitive he is of the signals put off by other humans (facial expressions, sighs, etc.).**

It is rare to calculate the link budget or SOM for indoor connections. This is because most indoor connections are not direct line-of-sight type connections, but instead they reflect and scatter all throughout the indoor environment. In fact, someone can move a filing cabinet and cause your signal strength to change. It can really be that fickle. However, understanding SOM and conceptualizing it extrapolated out to dozens of STAs connecting to the AP helps you think about the signals needed by each STA.

Outdoor links are the most common type of links where you will need to create a link budget and determine the SOM. A detailed link budget can be much more complex than that which has been discussed here. For example, it may include consideration for Earth Bulge, the type of terrain and the local weather patterns. For this reason, some vendors provide link budget calculation utilities.

Let us consider an actual example of a link budget calculation. Figure 6.6 shows a site-to-site link being created across a distance of 200 meters with 802.11 bridges. Based on the output power of the bridge, the attenuation of the cables, the gain of the antennas, and the free space path loss, we can calculate the link budget since the receive sensitivity of both bridges is -94 dBm. The calculations are as follows:

```
Link Budget calculation 1: 100 mW = 20 dBm

Link Budget calculation 2: 20 dBm - 3 dB + 7 dBi - 83 dB
= -59 dBm

Link Budget calculation 3: (-94 dBm) - (-59 dBm) = 35 dBm

SOM = 35 dBm
```

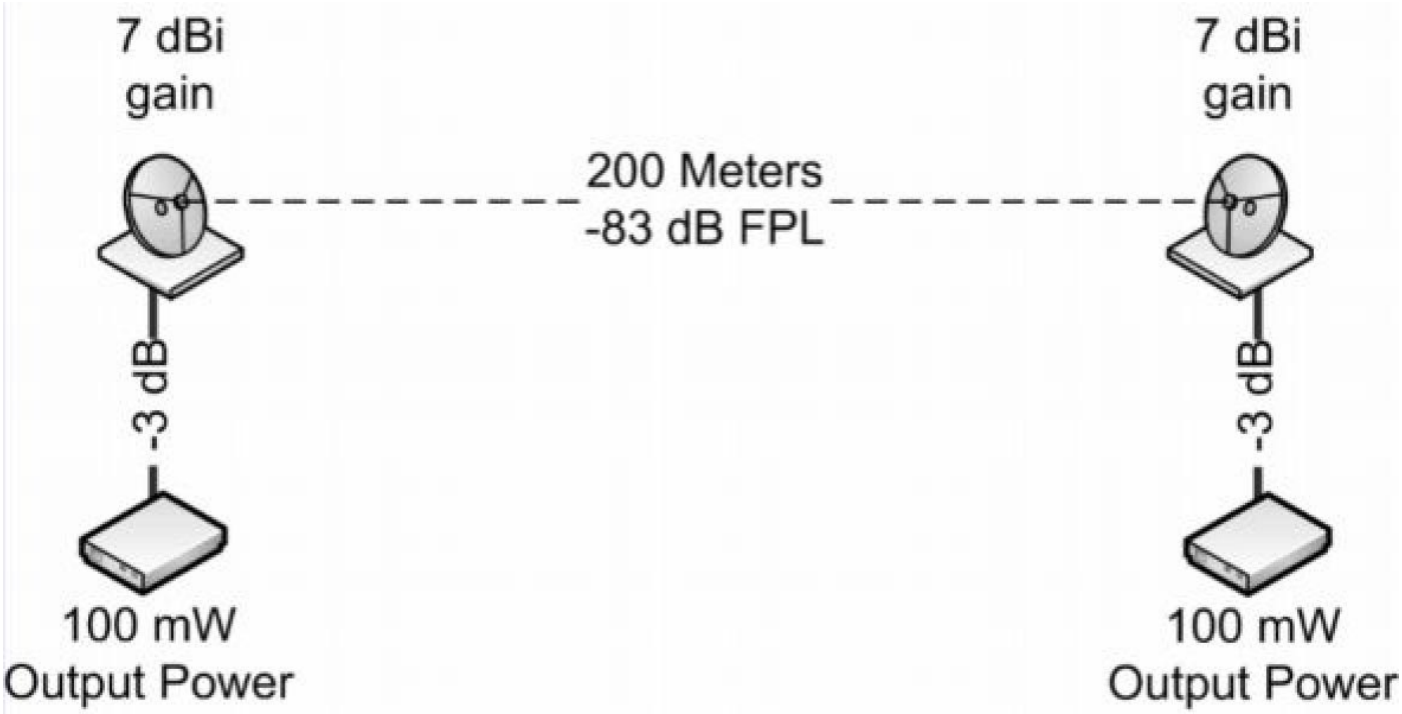


Figure 6.6: Link Budget Calculation

Fade Margin

Because of the variableness of wireless links, it is not uncommon to “pad the budget” much like a project manager may do for “risk factors” in a project. The padding of the budget is needed because, over time, the weather does change and trees grow and buildings are built. These factors, and others, can cause the signal to eventually. By including a few extra dB of strength in the required link budget, you can provide a link that will endure longer. The extra signal strength actually has a name, which is fade margin. You do not add to the link budget/SOM dBm value, but instead you take away from the receive sensitivity. For example, you may decide to work off of an absolute receive sensitivity of -80 dBm instead of the -94 dBm supported by the Cisco Aironet card mentioned early. This would provide a fade margin of 14 dBm.

When you create outdoor bridge links, a fade margin is a practical requirement. Careful link budget calculations should be made to determine the SOM and then you should pad that budget. Not drastically, but by all means pad the budget. The fade margin will give you two things: a more consistent link and a longer lasting link. Without the fade margin, you may notice that the link drops periodically in certain seasons of the year, or that the link simply fails to work after several months or years (due to changes in foliage or other environmental factors). Padding the budget with a fade margin helps in creating a more durable link.

For indoor communications, fade margins generally are not required. Why? Because we rarely perform full link budget calculations for standard indoor WLANs. We depend on reflections and diffractions to get the signal to the proper end location within the environment. For indoor bridge links (connections to remote location in large buildings), you may want to calculate the SOM. For all other indoor WLANs, you will likely just let the site survey do its job and ensure proper coverage in that way.

Intentional Radiator

The intentional radiator, as you learned in CWNA, is the point at which the antenna is connected. The signal originates at a transmitter and may pass through connectors, amplifies attenuators and cables before reaching the antenna. These components amplify or attenuate the signal resulting in the output power at the intentional radiator before entering the antenna. The FCC sets the rules in the United States regarding the power that can be delivered to and radiated by the antenna. Other regulatory agencies set similar regulations in other regions. These two points of power measurement have different allowances. The first is the intentional radiator and the second is the antenna element. For example, the FCC allows 1 watt of output power from the intentional radiator and 4 watts of antenna output power in a point-to-multi-point link in the 2.4 GHz band. To understand this, you will need to understand something called EIRP.

Equivalent Isotropically Radiated Power (EIRP)

The Equivalent Isotropically Radiated Power (EIRP) is the hypothetical power that is delivered by an intentional radiator to an imaginary isotropic antenna that would produce an even distribution of RF power with the same amplitude actually experienced in the preferred direction of the actual antenna. How is that for a technical definition? To make it simpler, it is the output power from the intentional radiator (output power from the transmitter plus any gains or losses leading up to the connection point of the antenna) plus the directional gain provided by the antenna. As an example, the FCC allows 1 watt of output power from the intentional radiator and then 6 dBi of gain at the antenna to equal 4 total watts of output power in a point-to-multi-point link in the 2.4 GHz ISM bands.

Antenna Factors

Different antennas have different beamwidths, which is the measurement of how broad or narrow the focus of the RF energy is as it propagates from the antenna along the main lobe. The main lobe is the primary RF energy coming from the antenna. Beamwidth is measured both vertically and horizontally, so do not let the term “width” confuse you into thinking it is a one dimensional measurement. Specifically, the beamwidth is a measurement taken from the center of the RF signal to the points on the vertical and horizontal axes where the signal decreases by 3 dB or half power. In the end, there is a vertical and horizontal beamwidth measurement that is stated in degrees. Figure 6.7 shows both the concept of the beamwidth and how it is measured, and Table 6.4 provides a table of common beamwidths for various antenna types (these antenna types are each covered in detail later in this chapter).

> **EXAM MOMENT:** Remember that the beamwidth is calculated where the signal reaches half power or -3 dB.

Antenna Type	Horizontal Beamwidth	Vertical Beamwidth
Omni-directional	360 degrees	7 to 80 degrees
Patch/panel	30 to 180 degrees	6 to 90 degrees
Yagi	30 to 78 degrees	14 to 64 degrees
Sector	60 to 180 degrees	7 to 17 degrees
Parabolic dish	4 to 25 degrees	4 to 21 degrees

Table 6.4: Various beamwidths for antenna types

Some example antennas are listed in Table 6.5 with their horizontal and vertical beamwidths.

Antenna Model	Horizontal Beamwidth	Vertical Beamwidth
Cisco 9.5 dBi sector antenna	60°	60°
Cisco 2.2 dBi dipole antenna	360°	55°
Cisco Multi-band wall-mount (patch/panel) antenna	68°	66°
Hyperlink Technologies 2.4 GHz die cast grid antenna	8°	8°

Table 6.5: Beamwidths for specific antennas

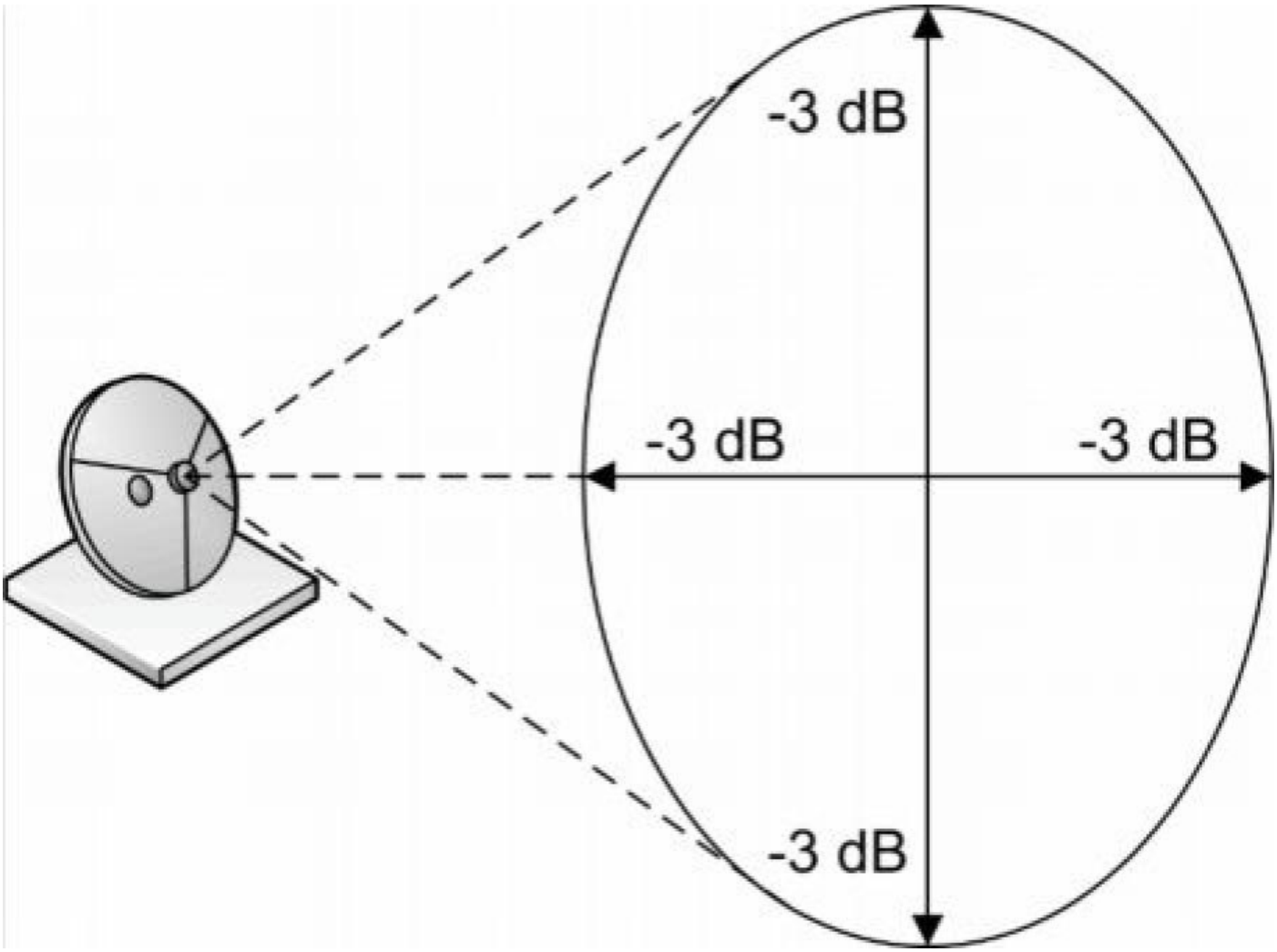


Figure 6.7: Beamwidth Concept and Measurement

While beamwidth measurements give us an idea of the propagation pattern of an antenna, they are less than perfect in illustrating the actual areas that are covered by the antenna. For more useful visual representations, you will want to reference Azimuth and Elevation charts.

Why are we discussing antennas in a chapter on spectrum analysis? Because the antenna you use with the analyzer will impact the view you have of the RF spectrum. A directional antenna will “see” more signal in the designed direction. An omni antenna will “see” signal or RF energy all around it equally.

Azimuth & Elevation

Where the beamwidth calculations provide a measurement of an antenna’s directional power, Azimuth and Elevation charts, which are typically presented together, provide a visualization of the antenna’s propagation patterns. Figure 6.8 shows an example of an Azimuth chart, and Figure 6.9 shows an example of an Elevation chart.

The difference between an Azimuth and an Elevation chart is simple: the Azimuth chart shows a top down view of the propagation path (to the left, in front, to the right and behind the antenna) and the Elevation chart shows a side view of the propagation path (above, in front, below, and behind the antenna). Think of these charts in terms of a dipole antenna that is positioned vertically upright. If you are standing directly above it and looking down on it, you are seeing the perspective of an Azimuth chart. If you are beside

it looking at it from a horizontally level position, you are seeing the perspective of an Elevation chart.

The Azimuth chart in Figure 6.8 is a chart of the Cisco 9.5 dBi sector antenna referenced in Table 6.5. As with most Azimuth charts, the direction of propagation is represented in the upward direction; however, the actual direction will depend on how you position the antenna—more on that in the later section titled Polarization. The chart is reporting the different signal strength you can expect at different degrees from the antenna. For example, at 90 and 270 degrees (to the immediate left and right of the antenna's intended propagation direction) you will see a loss of approximately 20 dB. Directly behind the antenna, at 180 degrees, you will see a loss of approximately 35 to 50 dB. This is a sector antenna and is intended to propagate its energy in one direction, but in a fairly wide path.

The Elevation chart in Figure 6.9 is for the same Cisco antenna. You will notice that the pattern of propagation is very similar to the Azimuth pattern. Like most Elevation charts, it is shown with the primary radiation direction to the right. Remember, this is intended to represent you looking at the antenna's propagation pattern from the side view. You can see that this antenna as very similar levels of loss along the same degree levels as the Azimuth chart.

> **EXAM MOMENT:** Azimuth charts show the propagation pattern from a top down perspective. Elevation charts show the propagation pattern from a side perspective.

Understanding antennas is key in spectrum analysis. Omni antennas are best used for a general picture of RF activity. Directional antennas are best used for device location.

Additional Spectrum Analysis Terminology

A few additional terms need to be defined specific to spectrum analyzers. They are:

- Duty Cycle
- Sweep Cycles
- Resolution Bandwidth
- Utilization
- RF Domains

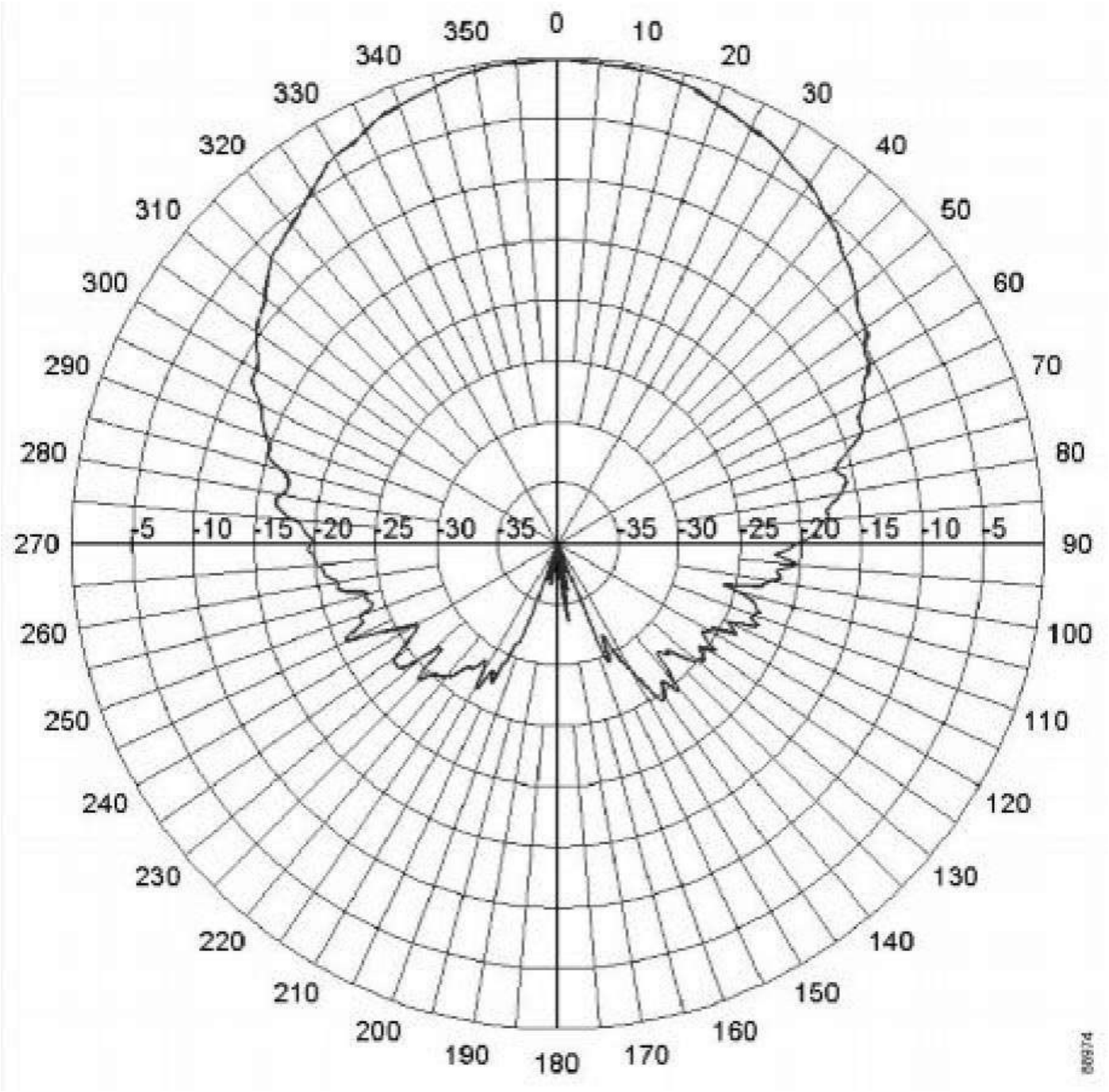


Figure 6.8: Azimuth Chart

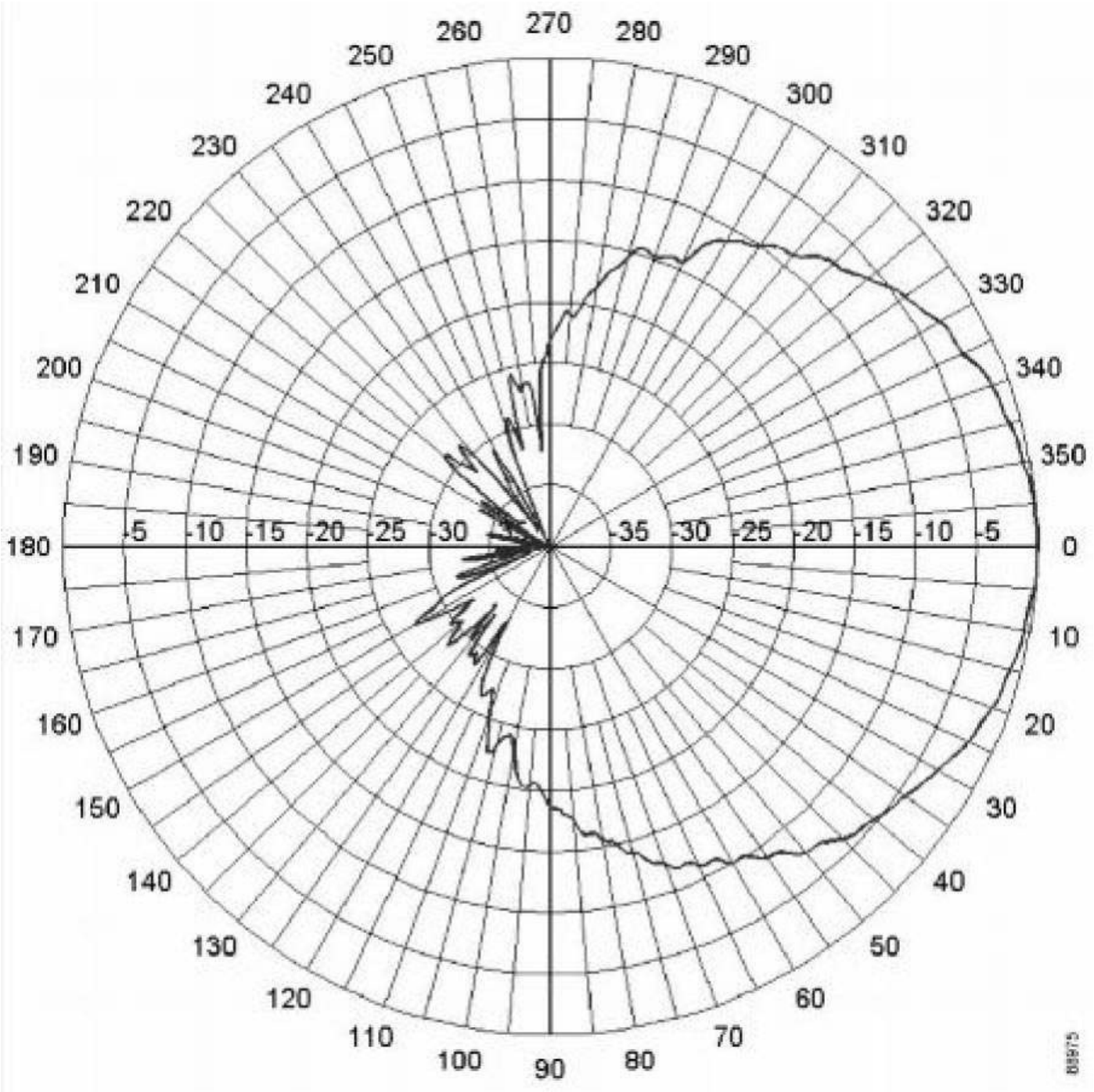


Figure 6.9: Elevation Chart

Duty Cycle

FFT Duty Cycle measurements are often an important way to determine the potential impact of an RF transmitter on WLAN operations. Duty cycle measures the amount of time in which the amplitude is above some arbitrary threshold (such as -95 dBm, or 15 dB above the noise floor, or -75 dBm). The threshold varies for each spectrum analyzer, so it is quite important to know the threshold for your specific software.

There are two common trains of thought in the duty cycle threshold settings, and both are valid. The key point is to evaluate your purpose in performing spectrum analysis.

The first thought is to keep the threshold somewhat low (say -90 dBm) so that the duty cycle of all transmitters are captured and not just those that are nearby at high power. On the other hand, a low threshold like -90 dBm does not necessarily indicate how the interferer will impact 802.11 devices, which use clear channel assessment thresholds to

determine whether the wireless medium is busy or idle. -90 dBm may not trigger the "busy" status, so it would raise the noise floor, but WLAN operations may continue normally, even with a device at 100% duty cycle.

Sweep Cycles

Understanding the advanced specifications of spectrum analyzers is not usually required for effective troubleshooting. However, understanding what a "sweep" is will be quite helpful because many of the most useful spectrum measurements are displayed relative to a sweep. In higher-end spectrum analysis tools, a sweep is measured as a single scan of the bandwidth span. So, if you're measuring 100 MHz of spectrum, a sweep is how long it takes to scan that 100 MHz band a single time.

In WLAN spectrum analysis tools, a sweep is more generic and is product-specific in behavior. The sweep is the period of time it takes to scan the band in view (2.4 GHz or 5 GHz for common Wi-Fi today). Many spectrum plots are updated with new data every sweep, which is often one second. In reality, WLAN analyzers are able to sample the bandwidth many times within that "sweep." It is important to understand that many data plots represent the measured data for the previous sweep.

For example, the real-time Fast Fourier Transform (FFT) plot shows amplitude (on the y axis) plotted over frequency (the x axis). Within the real-time FFT chart, there may be a trace for the maximum amplitude over the last sweep, the average amplitude over the last sweep, or possibly a "max hold" over all previous sweeps. When the plot updates after the next sweep, the data will be new, and will again be relative to the previous sweep.

Similarly, the duty cycle plot shows a percentage of time that transmitter amplitude is above a certain threshold over the course of a sweep. So, the charts represent data for a specific, limited time period. As an engineer, the conclusions that you draw are dependent upon understanding this time constraint.

Waterfall charts are also very common in spectrum analyzers. They may display FFT data or duty cycle data, but instead of showing data only for a single sweep, they update the waterfall with a single line for each sweep. The chart is designed to show historical data for some previous number of sweeps.

Resolution Bandwidth

Resolution bandwidth (RBW) is a reference to the smallest frequency that can be resolved by the receiver. RBW should be low enough to resolve spectral components of the transmissions being measured. Frequency hopping devices typically represent the smallest transmit shape that should be recognized by a spectrum analyzer in the Wi-Fi domain. If the resolution goes too low, sweep times decrease, that may impact sampling across the band.

You may never have to evaluate the RBW, and your product's RBW may be fixed. But as you use more advanced spectrum analyzers, the RBW may be variable. Figure 6.10 represents RBW graphically. The left image shows a RBW that is insufficient for detection of signals such as FHSS and narrowband signals effectively. The right image is a much better RBW. They are typically measured in kilohertz (kHz).

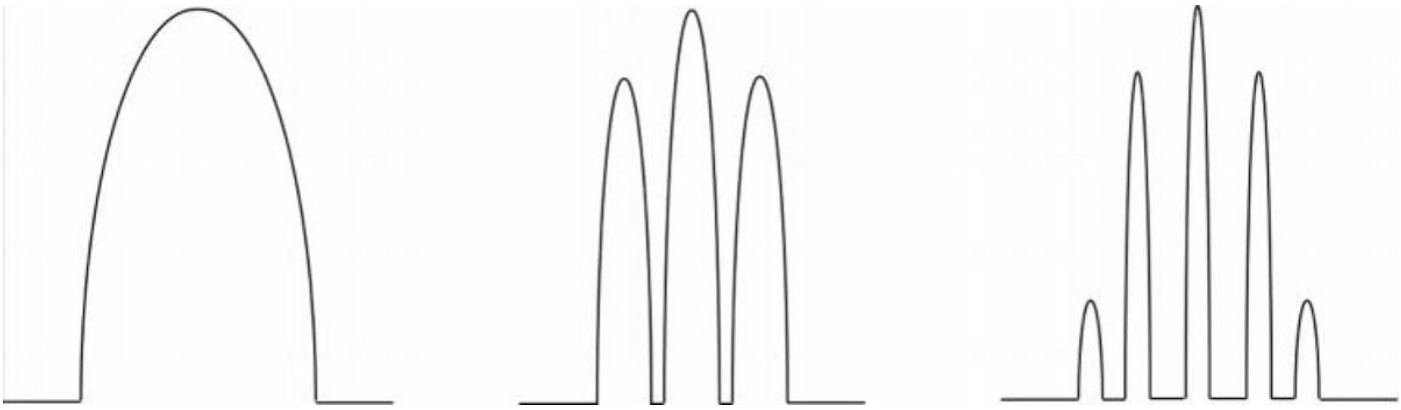


Figure 6.10: Resolution Bandwidth Visualized

Utilization

Utilization is a measurement of airtime consumed by the detected signal. It is often represented in color depth. For example, bright red would indicate a strong signal and seeing bright red continually on a waterfall or swept spectrogram view would indicate high utilization. Some spectrum analyzers may show the utilization as a percentage as well. High utilization indicates that the duty cycle is high continually. Low utilization indicates that it is low. This can help you determine if the detected signal will be a likely interferer on a continual basis in any channels in the same frequency space.

Spectrum Analyzer Features

Spectrum analyzers, like protocol analyzers, have a common set of features. These include views, reports, and Wi-Fi integration.

Views

Spectrum analyzer views show you various representations of the RF energy in the monitored spectrum. They may show RF activity over time, at the moment, or in the past when looking at saved captures. They will also show statistical information such as channel quality, maxim dBm, and utilization. (As you can imagine, spectrum analysis is used in support of many communications beyond Wi-Fi, as well.)

To understand the ways in which spectrum activity is displayed, it is important to grasp some basic concepts of RF representation. The first is the FFT. The FFT shows spectral activity in the frequency domain, while waterfall or swept spectrogram views attempt to represent RF activity over time. Figure 6.11 illustrates the frequency and time domains of spectrum analysis. You can think of the frequency domain as the way RF activity would appear if the waves were coming at you and the time domain as the way it would appear if the waves were going past you. While this is not a physically specific interpretation, it is helpful for understanding. The frequency domain shows each frequency with the amplitude of energy on that frequency at any given moment. The time domain shows each frequency as it existed over time while monitoring or sweeping the spectrum.

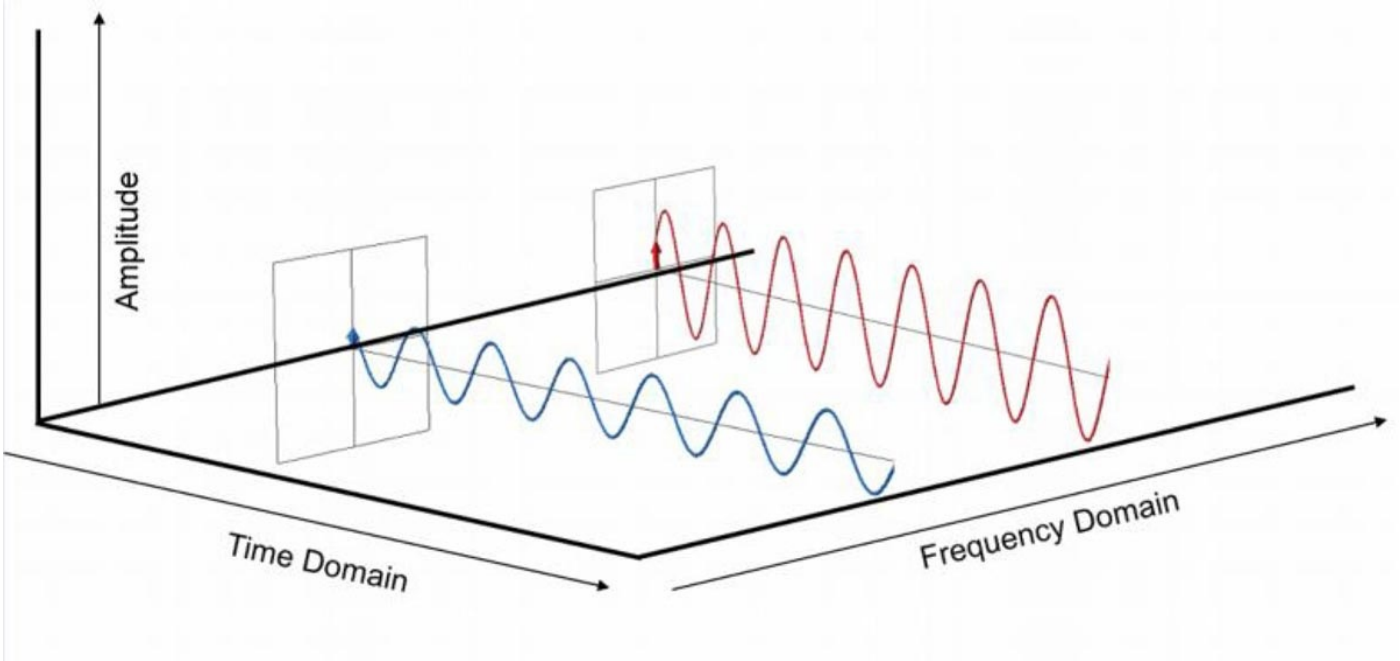


Figure 6.11: Frequency and Time Domains

Figure 6.12 shows the Spectrum XT view of the FFT information. This would be analogous to the frequency domain. In this case, it is also showing where the 2.4 GHz channels fit in this space. Along the left scale you can see the power level in dBm for the signal. Along the right scale you can see the 2.4 GHz channel numbers. From this, you can determine the channels that have the strongest active RF energy, and the weakest active RF energy. As Figure 6.12 shows, the energy in the 2.4 GHz spectrum at the location monitored included some very strong signals; however, this view does not reveal utilization, which is the key factor that will determine whether or not the signals will cause significant interference.

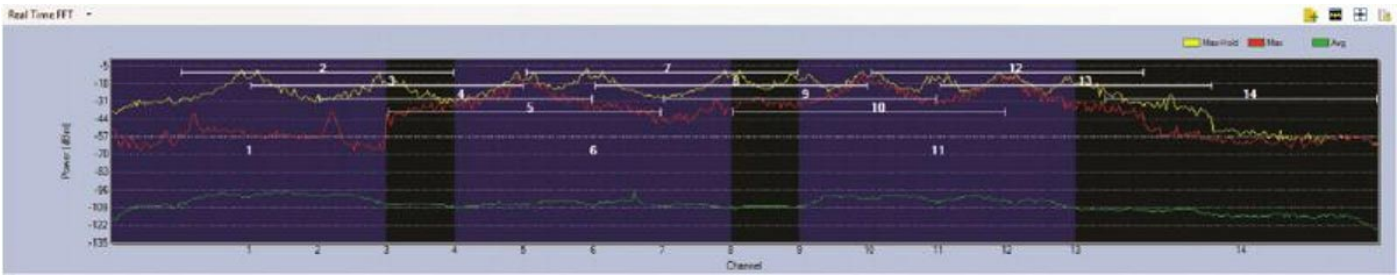


Figure 6.12: Spectrum XT FFT View

Additionally, the view represented does not reveal whether these signals include 802.11 signals, other wireless signals, incidental energy or anything else. That information will come from signature matching and Wi-Fi integration. Signature matching is used to detect (either automatically in software or manually by the viewing engineer) different signal types such as wireless phones, wireless cameras, Wi-Fi channels, and microwave ovens. In a later section, you will review signatures (or patterns) of common devices.

Figure 6.13 shows the FFT view in Chanalyzer (called the density graph) from Metageek. In this case, the bright red areas are revealing utilization. Deeper reds indicate higher levels of utilization. As with Spectrum XT, this view in Chanalyzer can reveal the max signal seen, average signal and current reading.

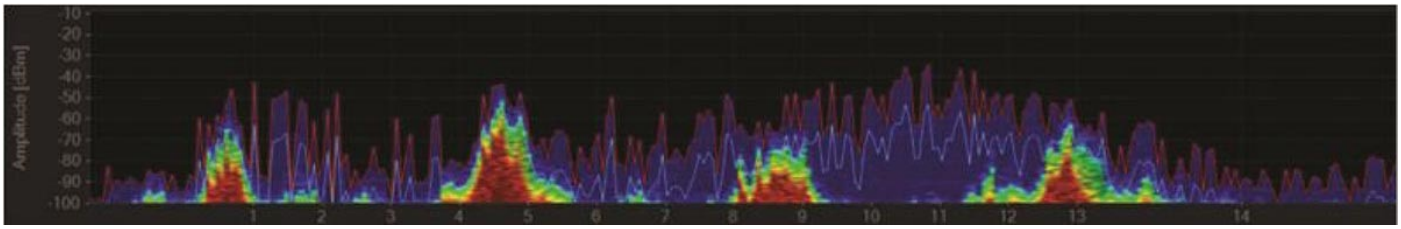


Figure 6.13: Chanalyzer FFT View

The waterfall view in Chanalyzer attempts to reveal the RF activity over time. Figure 6.14 shows Chanalyzer in the outdoor color scheme with the zoom on channel 11 and the waterfall view outlined in red.

Figure 6.14: Chanalyzer Waterfall View

Spectrum XT also supports such a view. Figure 6.15 shows the swept spectrogram view in Spectrum XT. Both of these views are useful to locate RF activity over time. Some interferers are sporadic in nature. They may appear only every few milliseconds, and the time views like the waterfall and spectrogram can help to detect such devices.

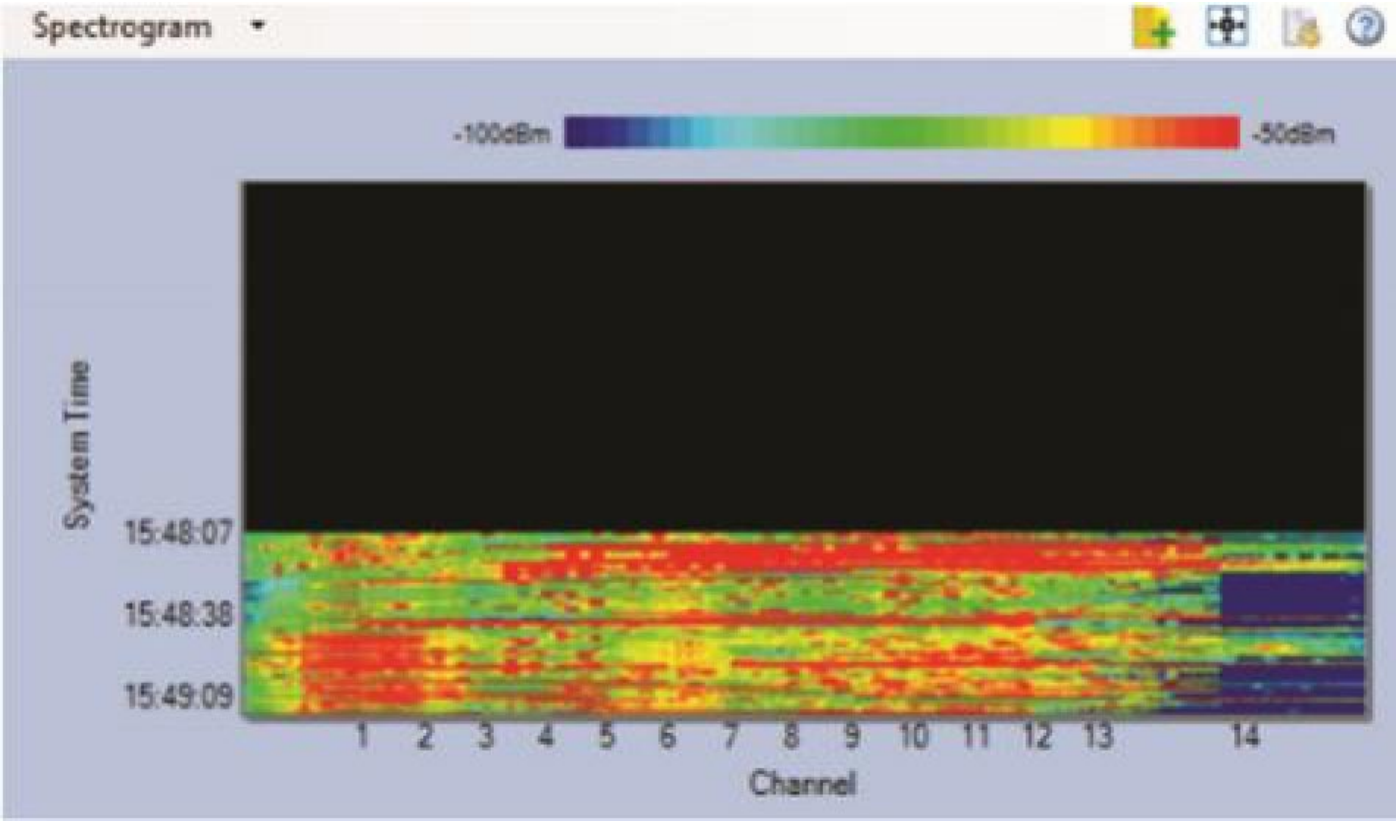
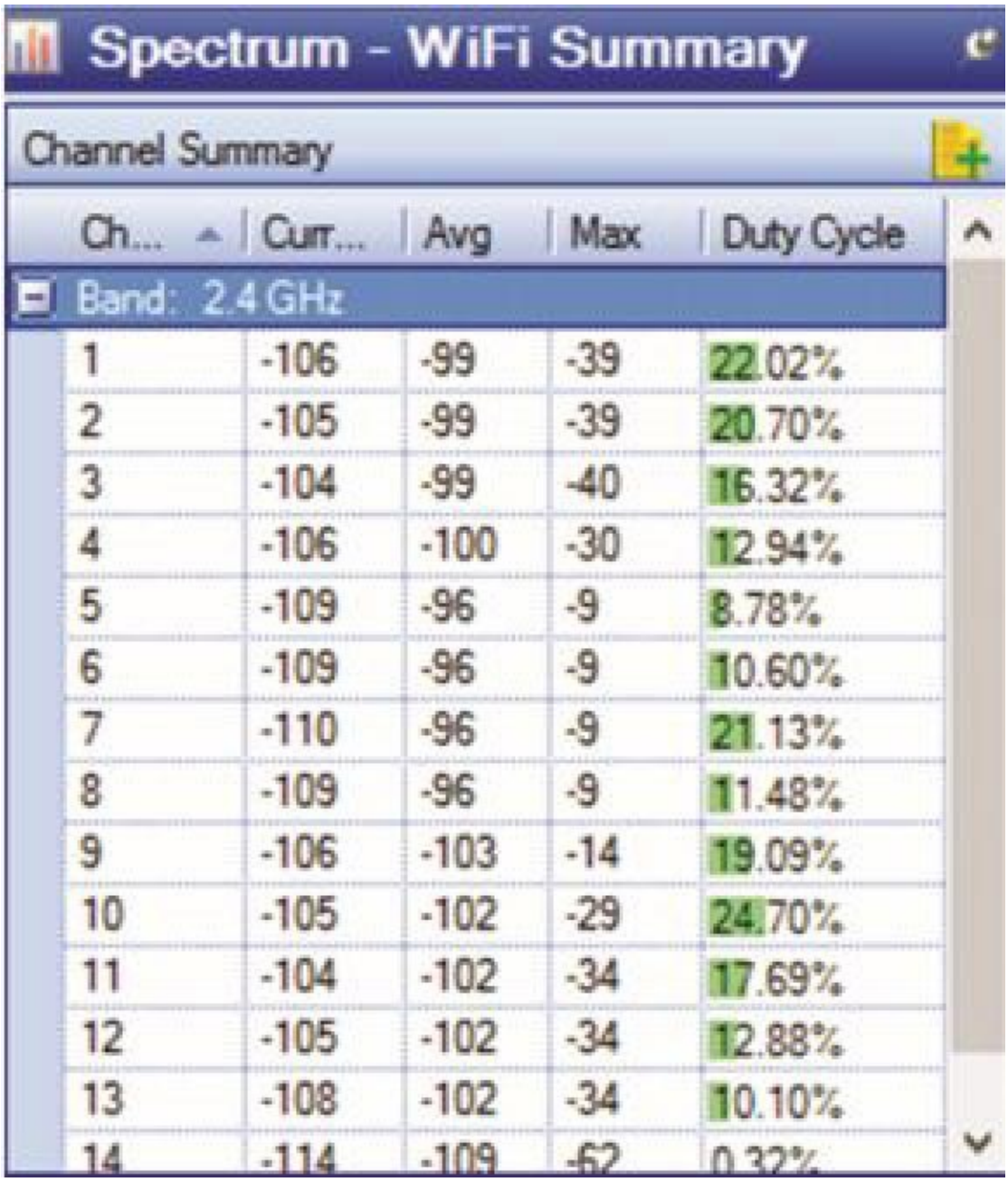


Figure 6.15: Spectrum XT

Finally, spectrum analyzers will present charts or tables with important statistical information. Figure 6.16 shows the Channel summary in Spectrum XT, and Figure 6.17 shows the Channels tab in Chanalyzer. Both reveal important information about the RF activity within 802.11 channel areas. Channel tables typically show the current RF amplitude, maximum, average and utilization or duty cycle. They may also list the number of APs on a channel when using Wi-Fi integration.



Spectrum - WiFi Summary

Channel Summary

Ch...	Curr...	Avg	Max	Duty Cycle
Band: 2.4 GHz				
1	-106	-99	-39	22.02%
2	-105	-99	-39	20.70%
3	-104	-99	-40	16.32%
4	-106	-100	-30	12.94%
5	-109	-96	-9	8.78%
6	-109	-96	-9	10.60%
7	-110	-96	-9	21.13%
8	-109	-96	-9	11.48%
9	-106	-103	-14	19.09%
10	-105	-102	-29	24.70%
11	-104	-102	-34	17.69%
12	-105	-102	-34	12.88%
13	-108	-102	-34	10.10%
14	-114	-109	-62	0.32%

Figure 6.16: Spectrum XT Channel Summary

Channel	Grade	Utilization	Average (dBm)	Current (dBm)	Max (dBm)	Noise Floor (dBm)	Access Points
1	98.0	1.1%	-82.5	-84.0	-70.0	-101.5	3
2	97.9	1.0%	-82.5	-101.0	-70.0	-102.0	0
3	97.8	1.1%	-82.5	-101.5	-70.0	-102.0	0
4	97.7	1.2%	-82.5	-98.0	-70.0	-101.5	0
5	97.5	0.7%	-76.5	-96.0	-63.0	-101.0	0
6	96.3	0.8%	-76.5	-96.0	-63.0	-100.5	7
7	94.7	1.5%	-76.5	-95.5	-63.0	-100.0	0
8	90.9	3.2%	-70.5	-92.5	-57.5	-99.5	0
9	86.7	4.8%	-70.0	-91.0	-57.0	-98.5	0
10	84.0	5.9%	-69.0	-91.0	-56.0	-98.0	0
11	82.6	7.2%	-68.5	-91.0	-55.5	-97.5	7

Figure 6.17: Chanalyzer Channels Tab

Reports

Report generation is a useful feature of spectrum analyzers. Figure 6.18 shows the report builder in Chanalyzer. This tool allows you to build reports from the different views in the

Chanalyzer software. You can also format the header, report title, author, location, and data. You can add custom blocks as well, where you might include photos or screenshots from other software.

Spectrum XT also includes report building features. According to Fluke Networks:

AirMagnet Spectrum XT's integrated report engine makes it easy to turn RF spectrum analysis sessions into professional reports. Customization features allow this Wi-Fi spectrum analyzer to generate reports on the RF spectrum graphs, Wi-Fi charts and the list of RF interference sources for the current environment. With the wireless spectrum analyzer, reports can be exported in the Word, RTF, PDF, HTML formats for handoff.

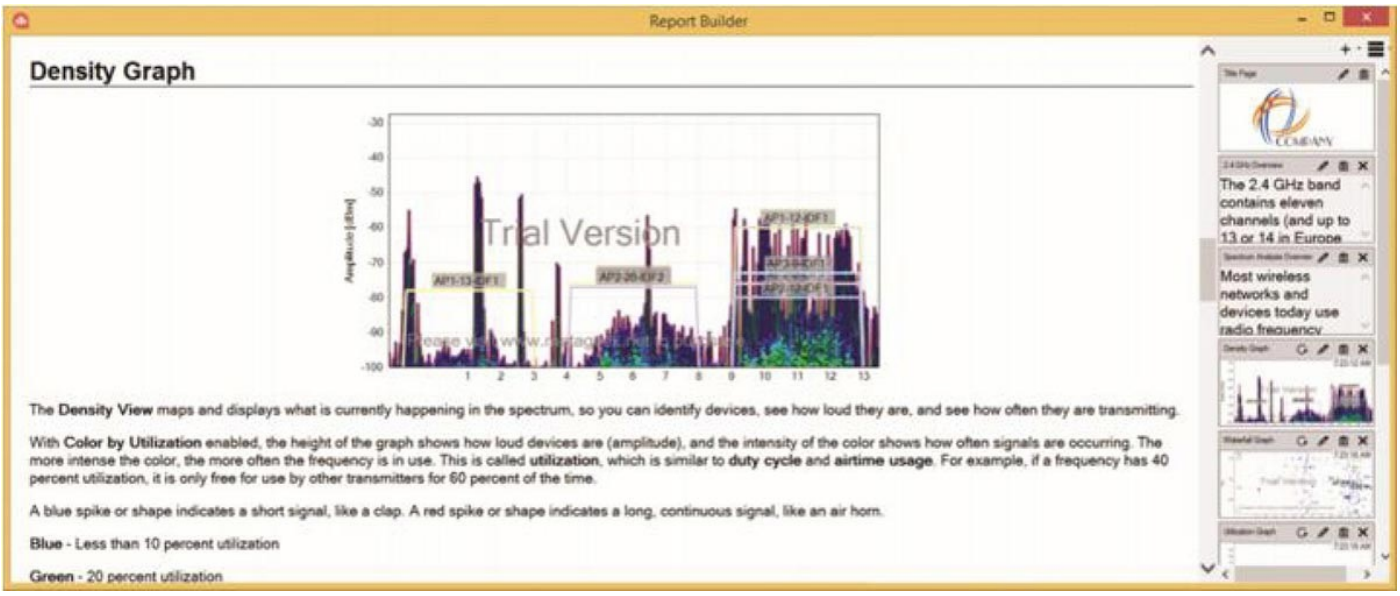


Figure 6.18: Chanalyzer Report Builder

The Chanalyzer report builder can save reports in the Wi-Spy Report Format only; however, you can export the report in PDF, Rich Text, or HTML formats as shown in Figure 6.19.

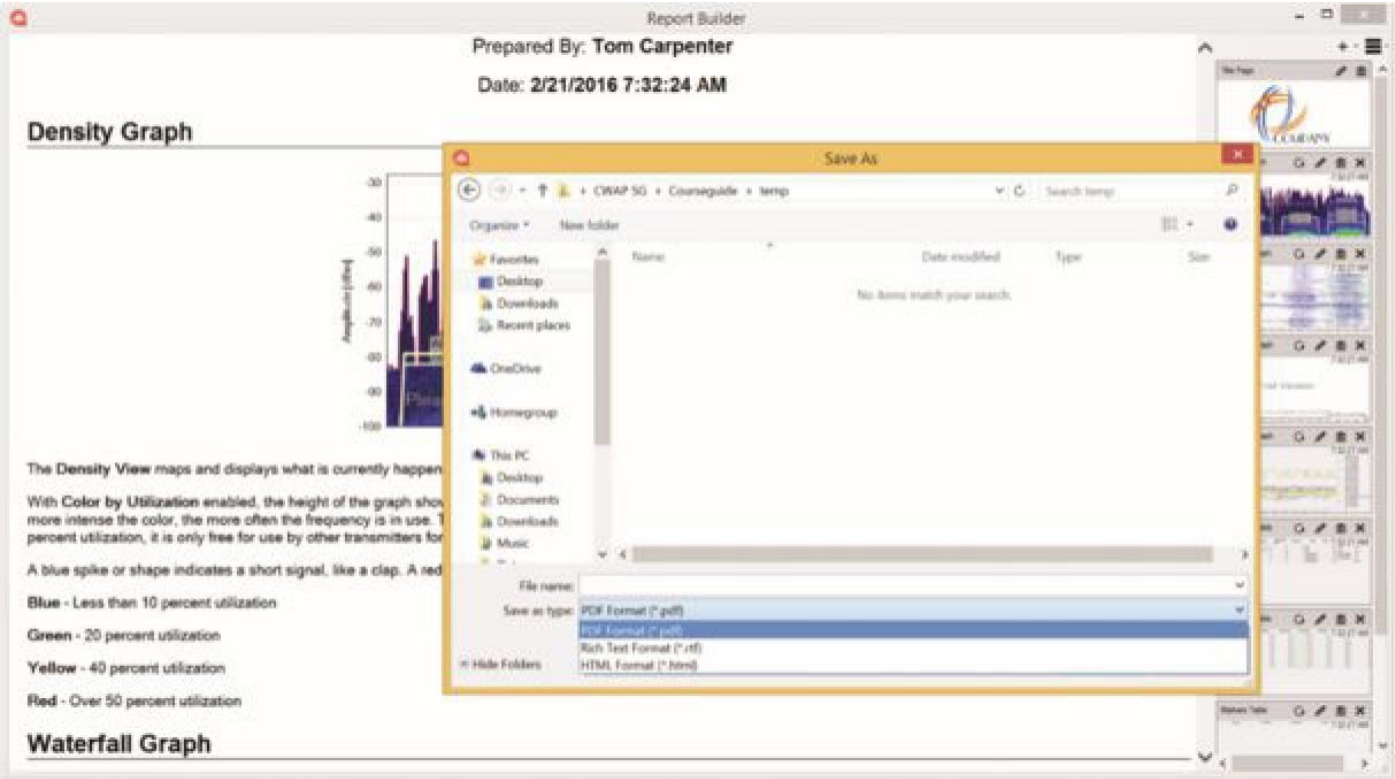


Figure 6.19: Chanalyzer Report Export Dialog

Wi-Fi Integration

Pure spectrum analysis is not specifically Wi-Fi aware with the exception of signal patterns. Many common transmitters use OFDM patterns such as HDMI wireless video devices, so relying on signal matching alone can be misleading. To properly detect 802.11, the spectrum analysis software needs to implement Wi-Fi integration. This simply means that the analyzer will use the laptop's 802.11 adapter to scan for and display wireless networks. The same basic information that is available in a Wi-Fi scanner like inSSIDer or Acrylic will be available in the spectrum analyzer software.

Figure 6.20 shows the information available in Chanalyzer with Wi-Fi integration. Notice the indicated networks in the density view (FFT) and the Networks Table tab shown below.

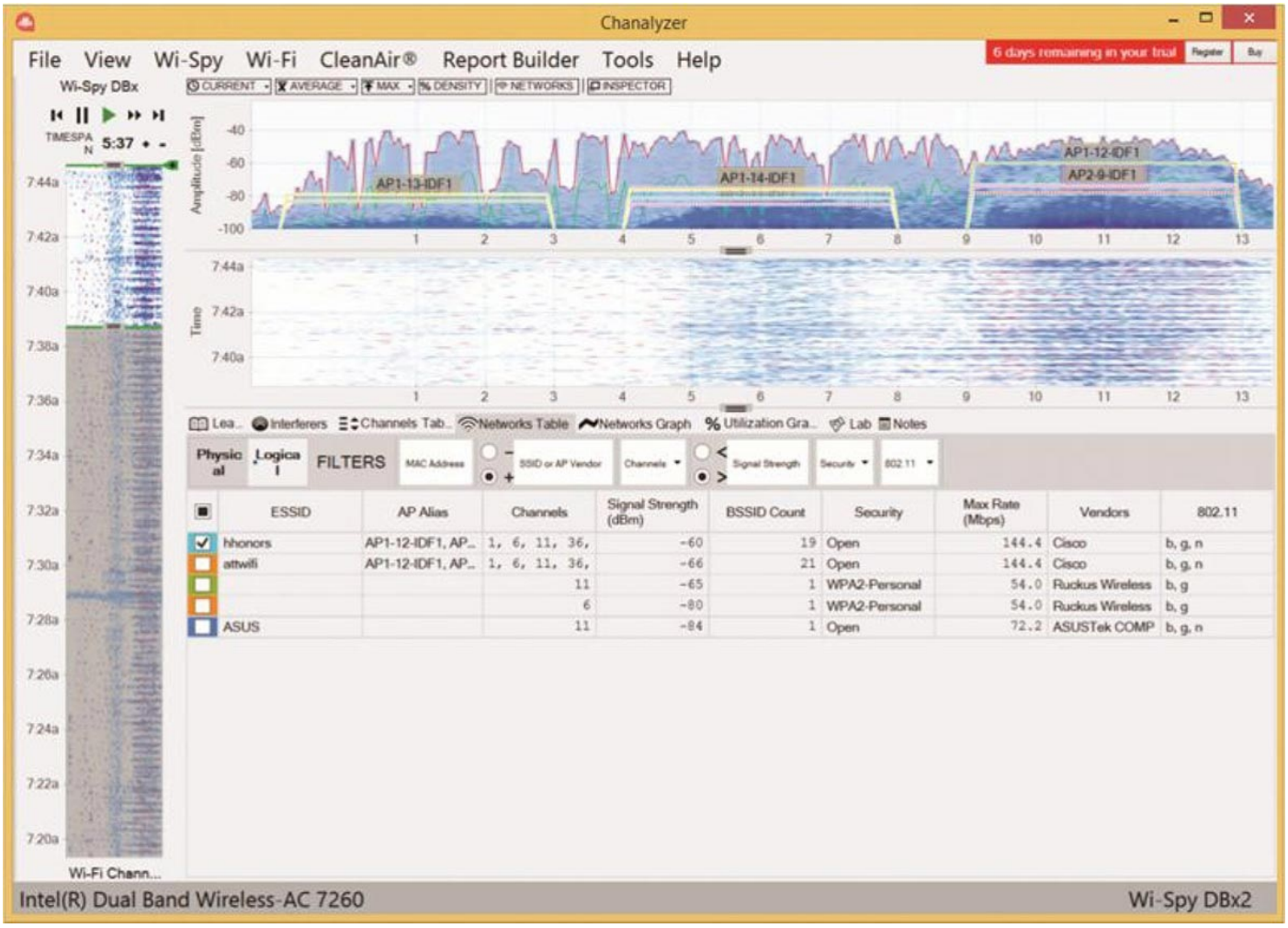


Figure 6.20: Chanalyzer with Wi-Fi integration

Figure 6.21 shows the Spectrum XT Wi-Fi integration from the perspective of detected Wi-Fi devices. This information is available due to actual frame captures instead of simple scanning. For this reason, both client devices and APs are shown with details on security features and frame times as well as APs to which client STAs are connected.

Additionally, on the left pane of Spectrum XT, you can see the channel summary and the channel devices with a count of APs, client STAs and phones per channel. Finally, based on signature matching, you can see possible interferers in the left pane, which in this case shows a wireless headset.

Note also, Figure 6.22 shows an example extract from the Spectrum XT report that has information available because of Wi-Fi integration. Particularly examine the AP and STA count columns.

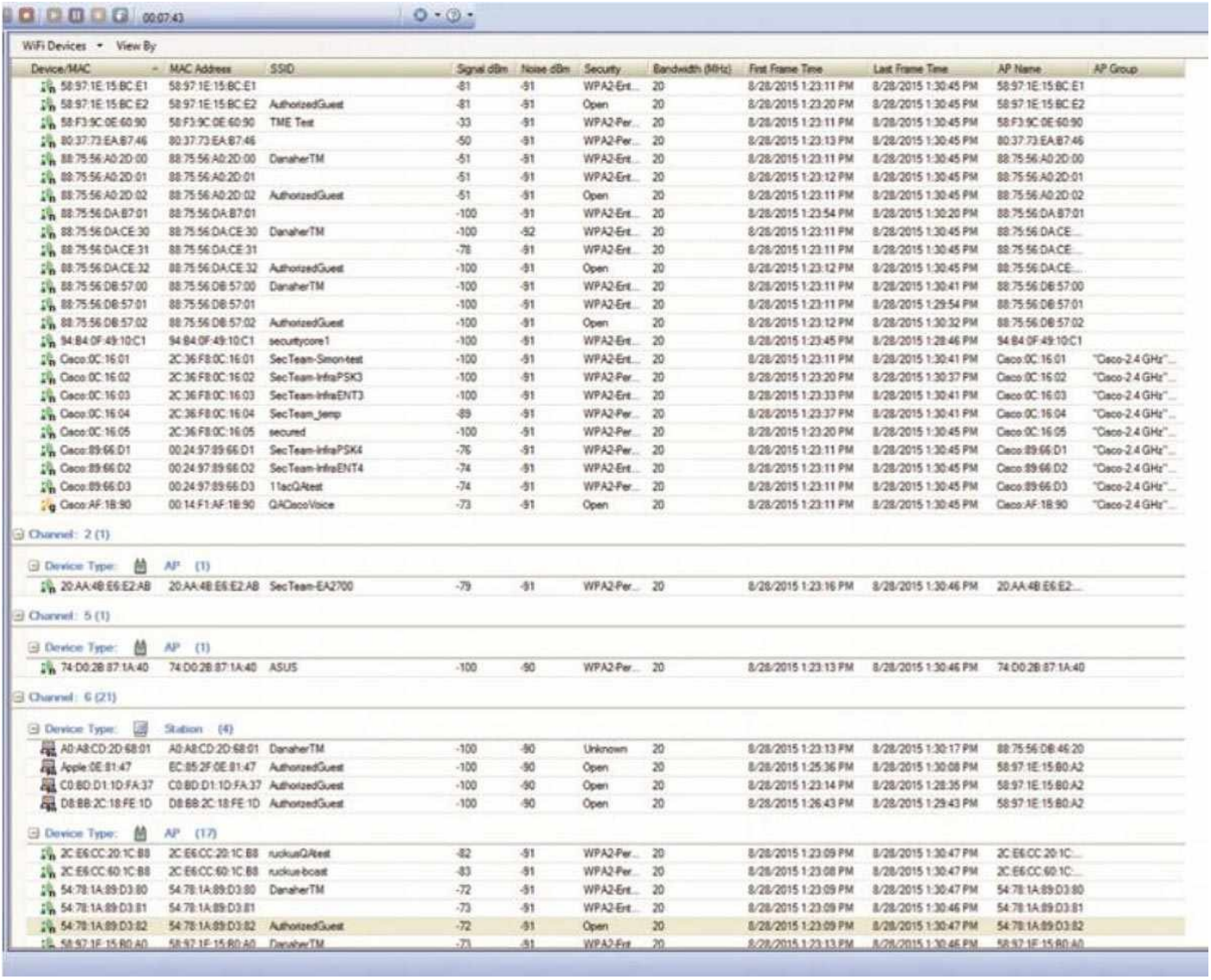


Figure 6.21: Spectrum XT Wi-Fi Devices View

Installing and Configuring

Installing and configuring a spectrum analyzer includes software and hardware installation, and the configuration of the software. Device drivers may be required for adapters used for Wi-Fi integration. This section provides a brief overview of the basic installation and configuration processes.

Install a Spectrum Analyzer

A USB-based spectrum analyzer should be inserted into an available USB port and the software installed. The software may require a license that is either tied to a simple serial number, or possibly linked to the hardware in the USB adapter (Spectrum XT links to the adapter and Chanalyzer requires only a serial number). The Spectrum XT license can be reattached to a new adapter by releasing it at the MyAirMagnet website.

When using an infrastructure analyzer, the software must be licensed and then connected to the infrastructure AP in spectrum mode. For example, in Chanalyzer, you will select the Clean Air option to connect to a Cisco AP in Clean Air mode.

Additionally, some vendors provide spectrum analysis in their management interfaces, including Meraki and Aerohive. With these solutions, you will connect to the web-based management interface and enable spectrum capture. It is important to know that, when using an AP in spectrum mode, the AP is usually taken out of standard AP mode so client access is interrupted on that AP.

WiFi Spectrum Environment Overview

2.4 GHz

This report provides information on channels 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14 operating in the frequency range 2.402 GHz to 2.842 GHz. The Maximum and the Average Power represents the maximum and average power levels across all channels in the 2.4GHz Band. This table also provides the number of APs, stations and phones found on the respective channels. Duty Cycle is defined as the percentage of time that a signal power above that of the noise floor is detected by the application

Channel	Average Power (dBm)	Maximum Power (dBm)	Average Duty Cycle (%)	Number Of APs	Number Of Stations	Number Of Phones
1	-100	-41	26.86	22	1	0
2	-100	-29	22.15	1	0	0
3	-100	-10	12.93	0	0	0
4	-100	-10	10.82	0	0	0
5	-97	-10	17.57	1	0	0
6	-97	-10	8.26	15	1	0
7	-97	-11	9.09	7	0	0
8	-97	-12	5.83	0	0	0
9	-103	-12	6.37	0	0	0
10	-103	-14	12.27	0	0	0
11	-103	-17	11.17	29	4	0
12	-103	-36	14.82	0	0	0
13	-103	-36	8.84	0	0	0
14	-108	-36	0	0	0	0

Spectrum Density Snapshot

The Spectrum Density graph shows the "popularity" of a particular frequency /power reading over time . The X-axis shows the frequency or channel for the 2.4GHz radio band; the Y-axis shows the minimum and maximum power readings in dBm .

Figure 6.22: Spectrum XT Report with Wi-Fi Integration Information

When you require a spectrum analyzer on a computer that does not natively run the software, you may be able to install the software in a virtual machine that runs the proper operating system. USB pass-through will usually work in such cases. This is true for spectrum adapters and protocol analysis adapters.

Configure a Spectrum Analyzer

Once installed, the spectrum analysis software will need to be configured. Several configuration options are common, including:

- Resolution bandwidth

- Scanning frequency
- Wi-Fi adapter

Resolution Bandwidth

If the spectrum analyzer supports adjusting the RBW, you may desire to do so. This is particularly true when scanning a smaller frequency range. However, understand that the sweep time is a factor of RBW, dwell time and frequency range. For example, if you increase the RBW (by selecting a lower kHz value), but do not scan a smaller frequency range or reduce the dwell time, it will take much longer to sweep the entire target frequency range. When it takes longer to sweep the target frequency range, it is possible that you might miss some intermittent signals or RF radiators. Carefully consider changes to RBW.

Scanning Frequency

The scanning frequency defines the band and range you will scan in the spectrum analyzer. Metageek Chanalyzer supports selecting the full 2.4 GHz band, the full 5 GHz band, and several other options. In addition, you can zoom into a specific frequency range to get a detailed view. Figure 6.23 shows the expanded menu for band/channel selection in Chanalyzer.

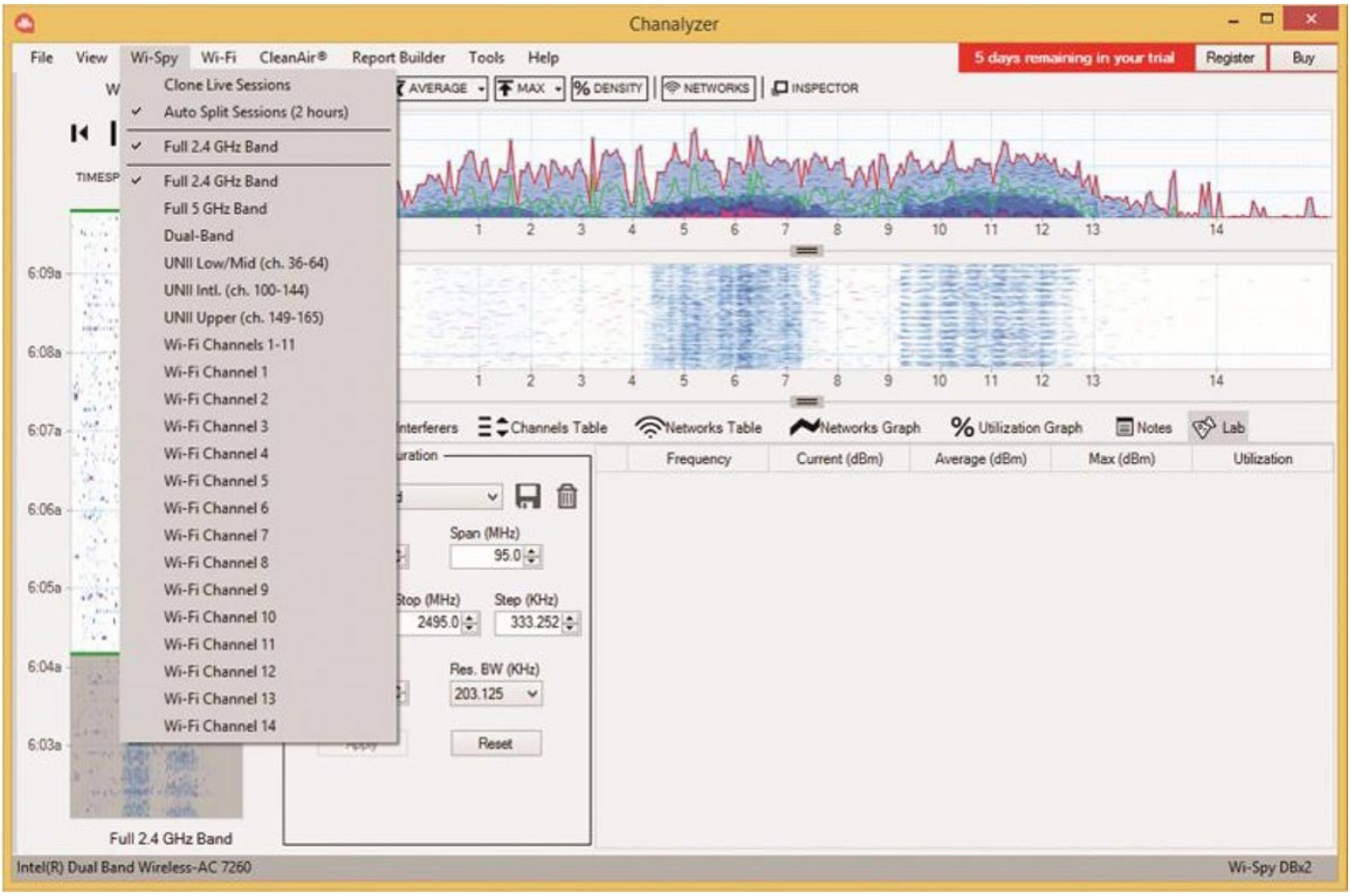


Figure 6.23: Selecting the Frequencies to Scan in Chanalyzer

Wi-Fi Adapter

Finally, for Wi-Fi integration, you can choose the wireless adapter you wish to use. For example, your laptop may have an integrated adapter that supports only 2.4 GHz bands. For this reason you may choose to use a USB adapter that supports 5 GHz as well. In

Metageek Chanalyzer, simply select Wi-Fi and then the adapter you desire as shown in Figure 6.24.

Performing Spectrum Analysis

Three spectrum analysis skills are essential for troubleshooting. First, recognizing patterns helps to identify devices. Locating devices helps to find interferers and remove or address them. Finally, discovering issues includes identification of high duty cycle devices in channels and other tasks as well. This final section provides an overview of these processes and identifies several common device patterns.

Recognizing Patterns

An important skill to develop in relation to spectrum analysis is pattern or signature recognition. You can often identify a signal by the RF signature it generates. For example, 802.11 signals are required to comply with specific spectral masks per the 802.11 standard. Figure 6.25 shows the standard OFDM 20 MHz channel spectral mask.

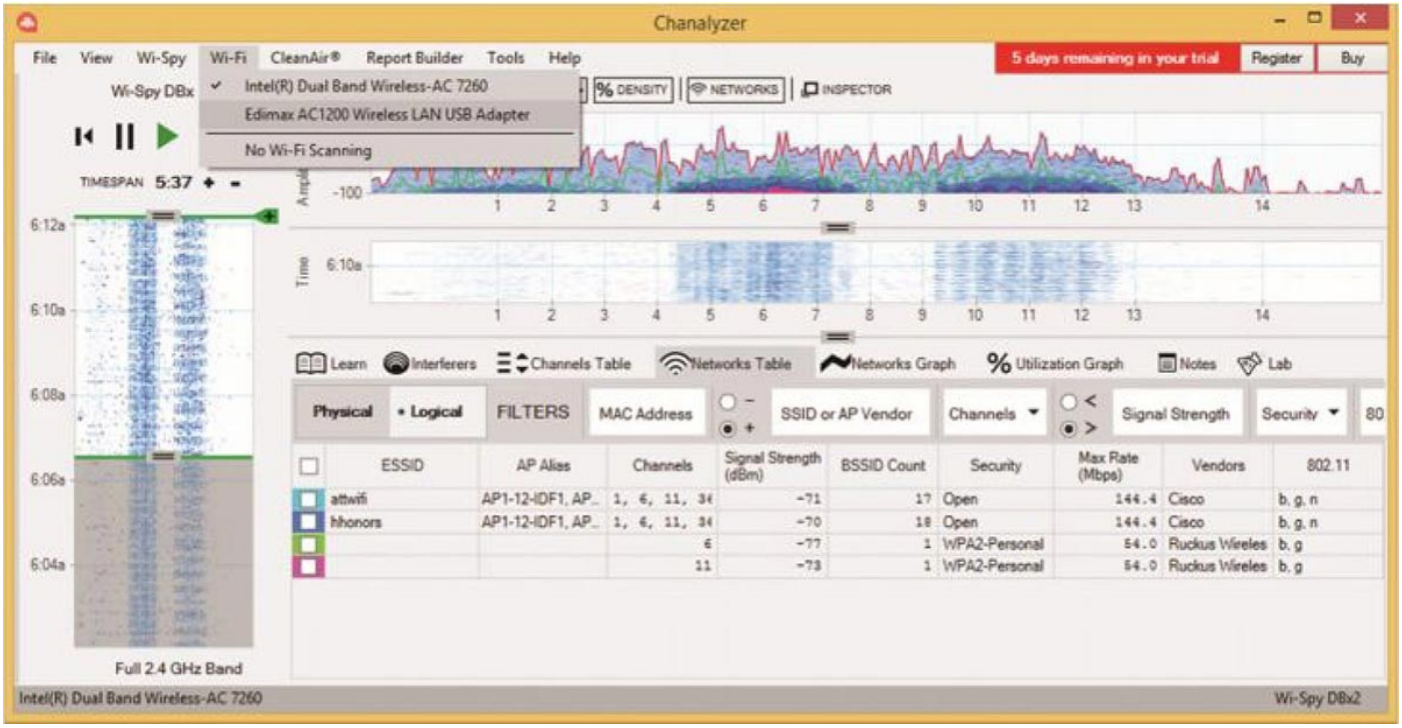


Figure 6.24: Selecting the Wi-Fi Adapter

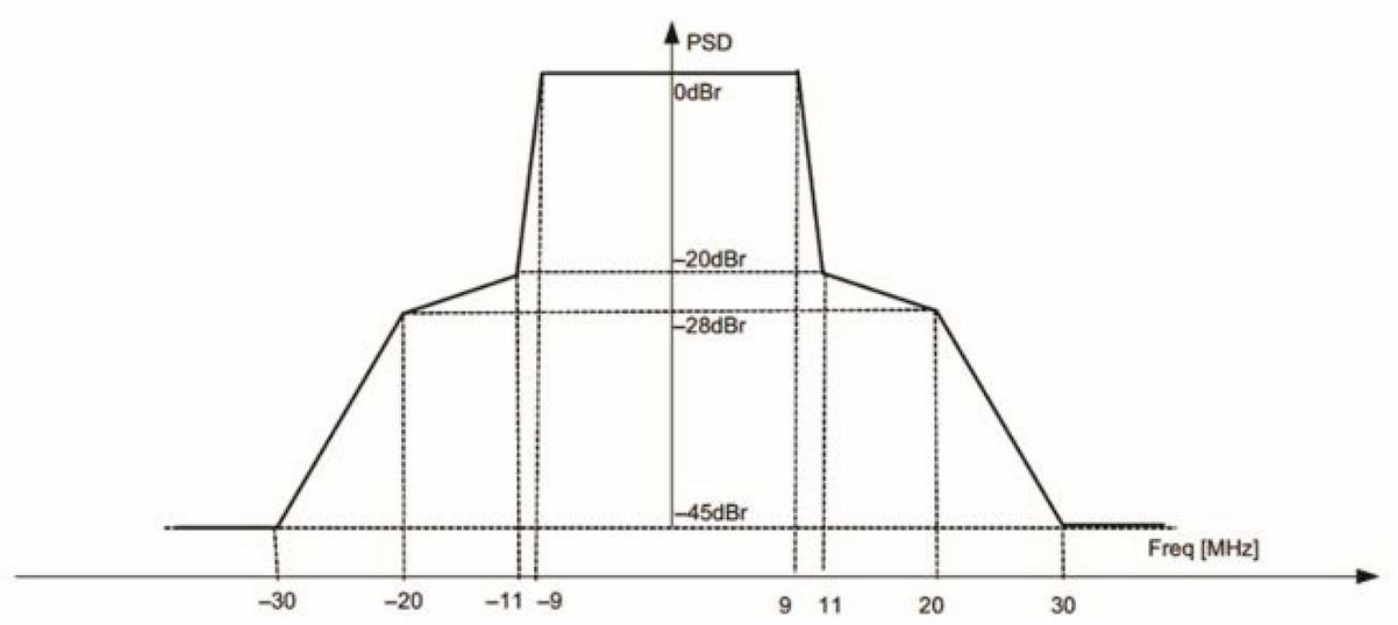


Figure 6.25: 20 MHz OFDM Spectral Mask from 802.11-2012

Note the characteristic flat top of the spectral mask. If you were to compare this to the older DSSS signal spectral mask, you would notice the DSSS mask has a rounded top as in Figure 6.26. The simple point is that these are signal signatures or patterns that can be recognized to help identify the type of wireless device detected in the spectrum analyzer. Figure 6.27 shows the pattern templates (interferer identifiers) available in Metageek Chanalyzer. Simply click on one of the templates to make it available for overlay in the density view as shown in Figure 6.27.

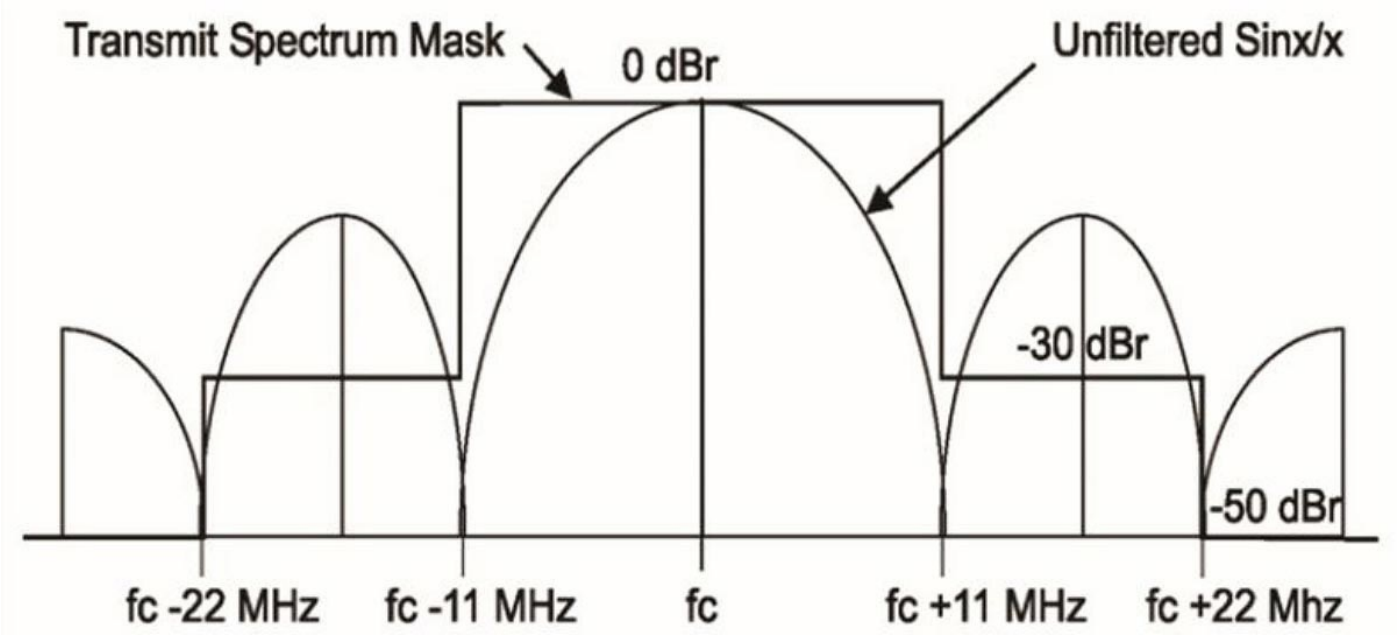


Figure 6.26: DSSS Spectral Mask

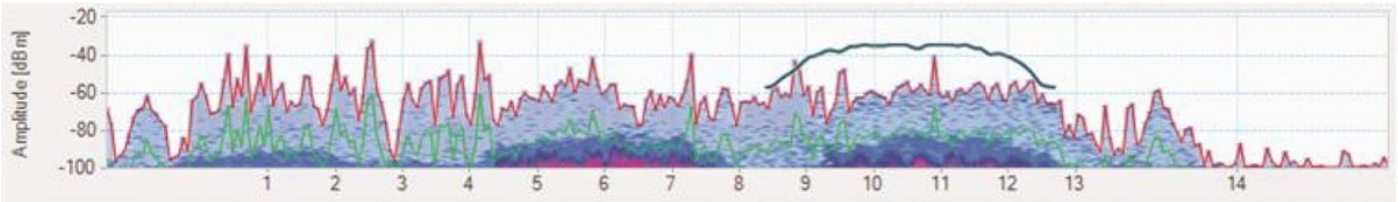


Figure 6.27: Interferer Identifier Overlay in Chanalyzer

The following pages will provide visualizations of common patterns exhibited by RF

signals and seen in spectrum analyzers. They should be useful in helping you to recognize common patterns in your tool of choice. It is important to know that some spectrum analyzers, such as Spectrum XT can perform automatic device identification based on the signal detected. For example, it can detect phones, microwave ovens, and headsets among other devices. Figure 6.28 shows this listing in Spectrum XT.

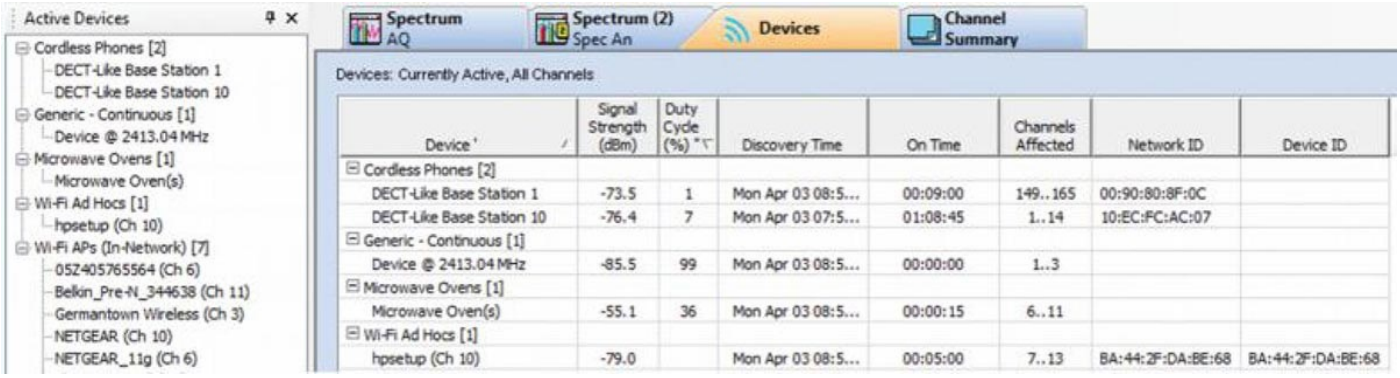


Figure 6.28: Identified Non-Wi-Fi Devices in Spectrum XT

20 MHz OFDM Signal Pattern

Figure 6.29 shows the 20 MHz OFDM signal represented in the spectral mask of Figure 6.25 captures in a protocol analyzer.

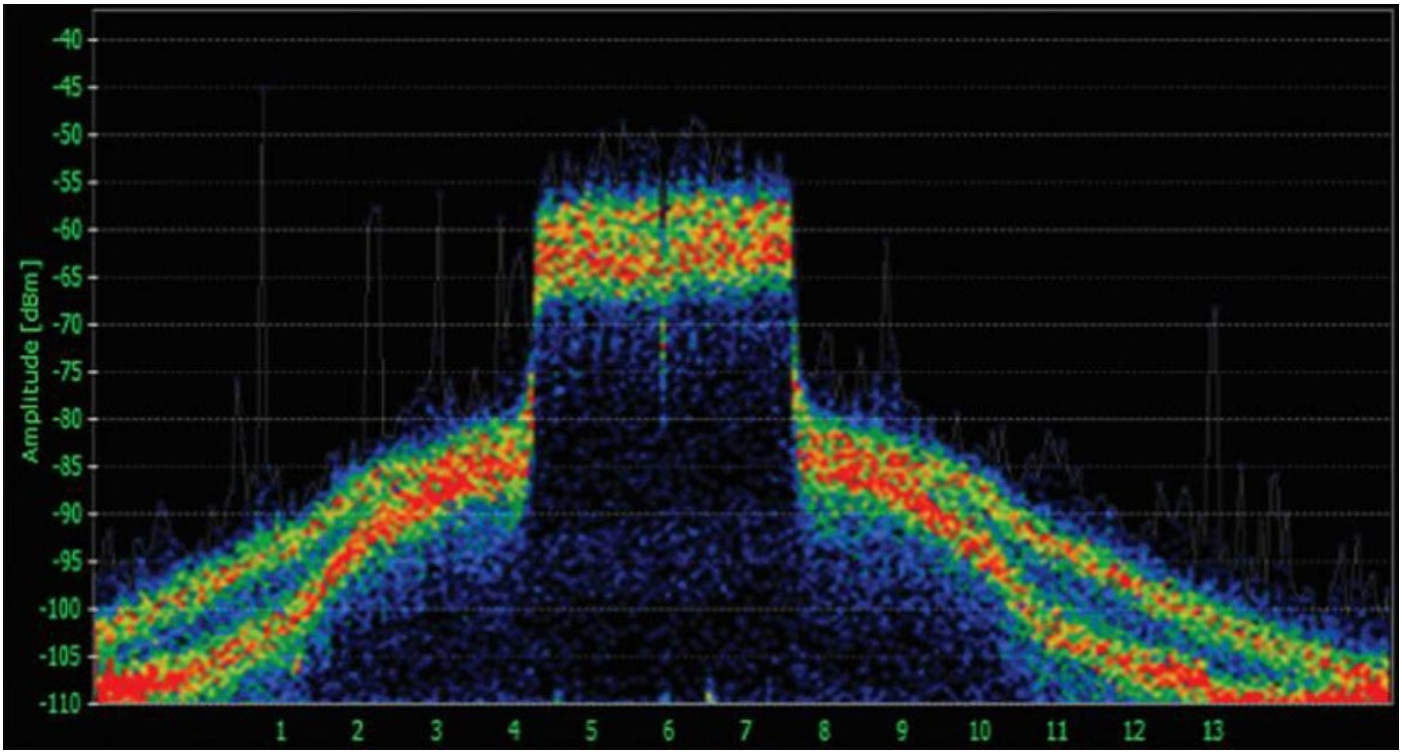


Figure 6.29: 20 MHz OFDM

40 MHz OFDM Signal Pattern

Figure 6.30 shows a 40 MHz OFDM spectral capture.

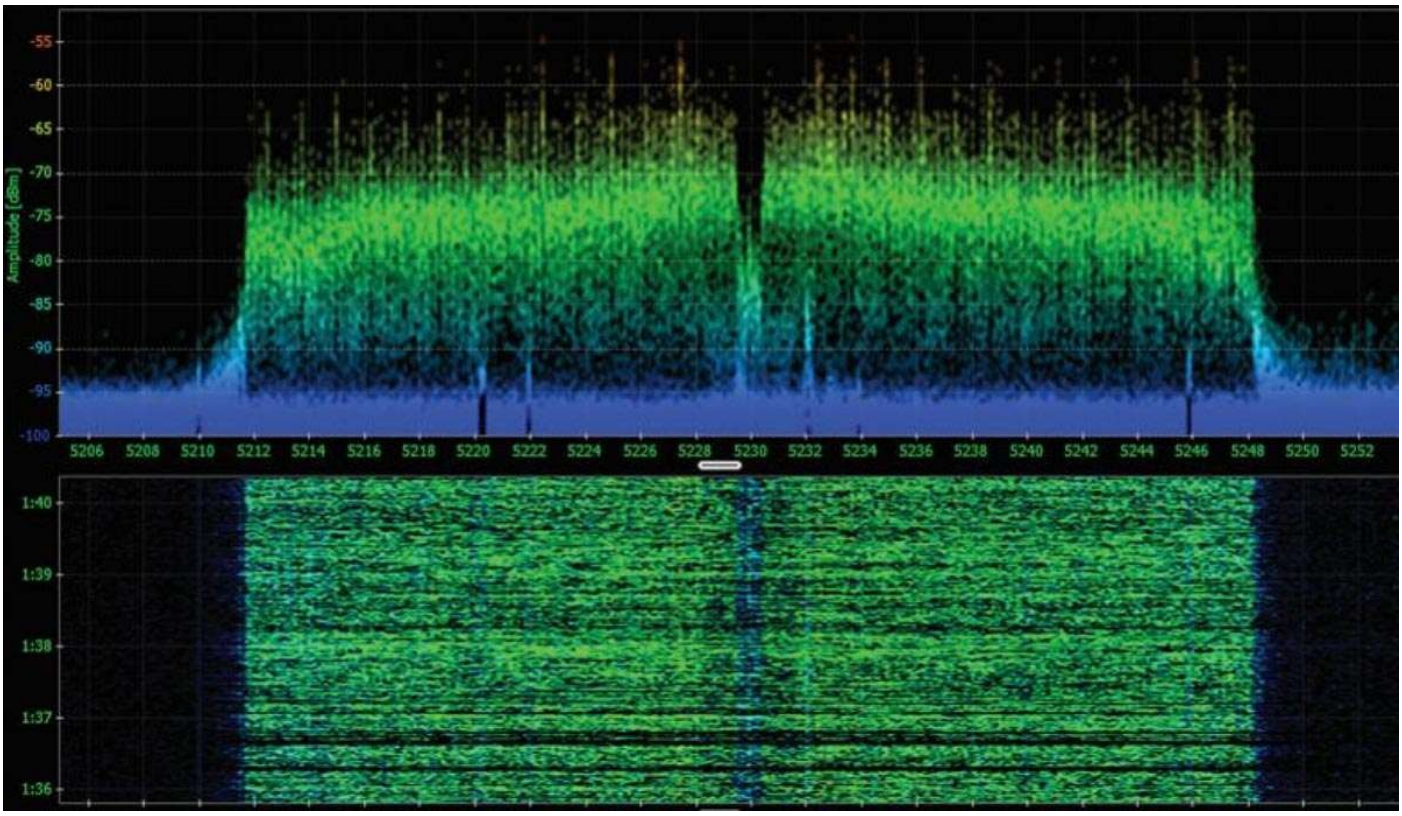


Figure 6.30: 40 MHz OFDM

Bluetooth Signal Pattern

Figure 6.31 shows Bluetooth discovery. Bluetooth devices have two distinct phases: Discovery and data transfer.

Bluetooth discovery uses a unique hop and dwell pattern that will create identifiable patterns over time. For example, in Figure 6.31, the swept spectrogram shows a Bluetooth discovery scan that includes some transmissions on the lower side of the band and some in the middle of the band. A small section of the band (perhaps 20 MHz wide, near Wi-Fi channel 3 or 4) is unused by this device in discovery. The real-time FFT pattern also has a distinct shape in Bluetooth discovery, whereas the “spikes” (for lack of a better word) appear more random in the data transfer stage.

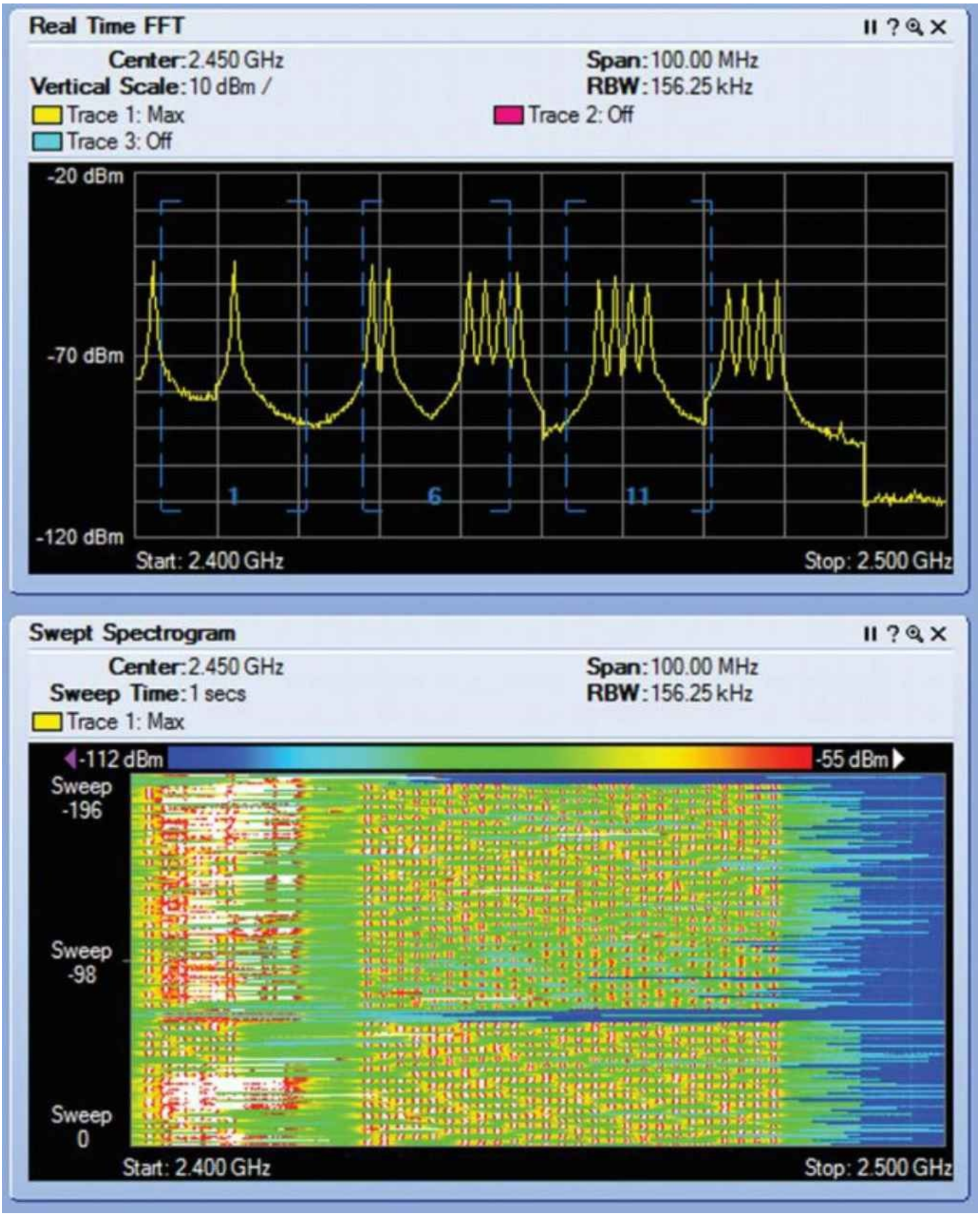


Figure 6.31: Bluetooth Discovery

Figure 6.32 shows Bluetooth in connected transfer mode. Compared with the discovery stage, you can see that the Bluetooth data transfer phase appears much more random (both in the real-time FFT and the swept spectrogram displays).

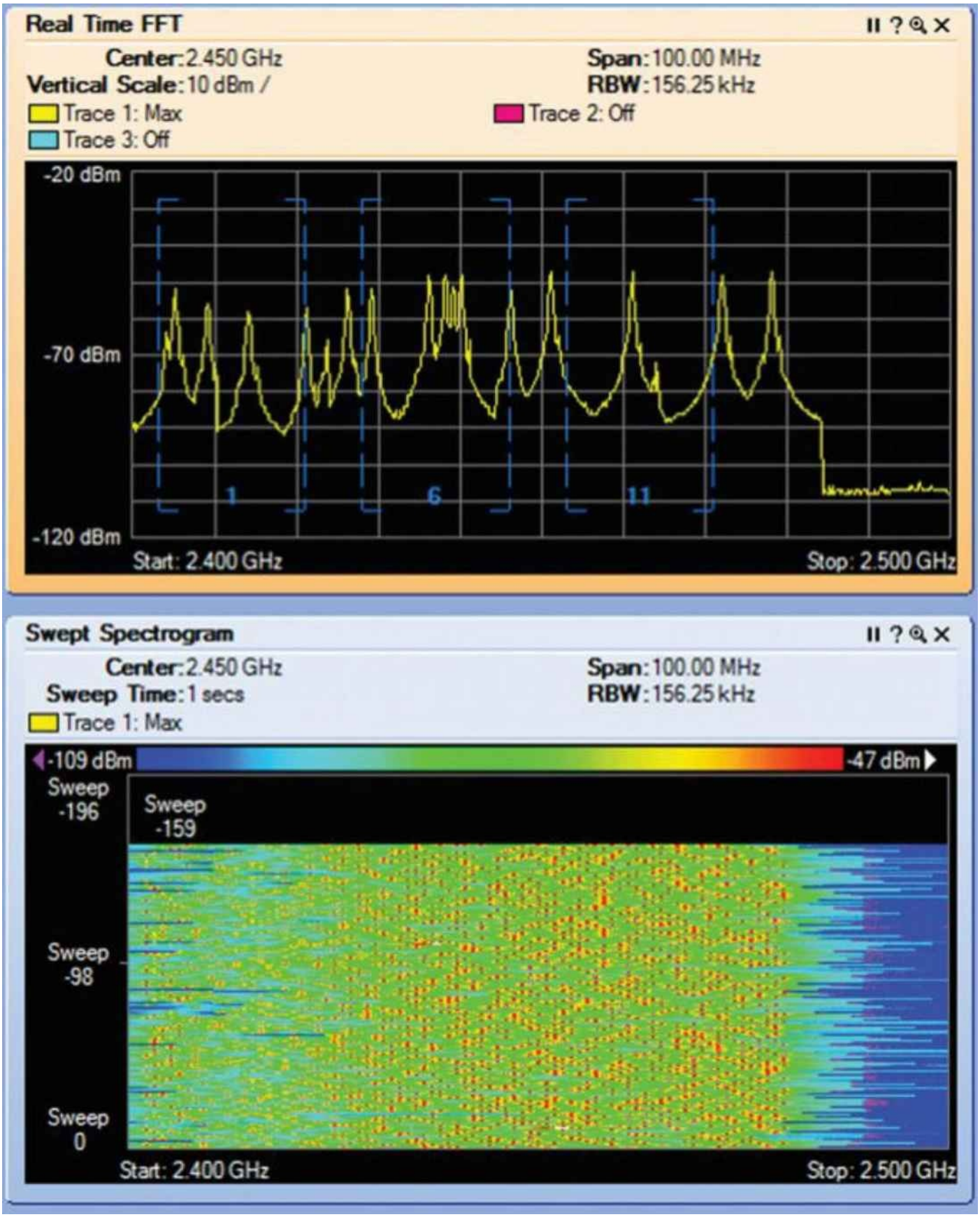


Figure 6.32: Bluetooth Transfer

Cordless Phone Signal Pattern

Cordless phones are narrowband transmitters, with a peak amplitude in the middle and a tapered edge. The image in Figure 6.33 shows a frequency hopping cordless phone that has transmitted in three places across this band. Other cordless phones may have narrower transmit signatures, but the consistent trait is the narrowband, high amplitude peak. Many

2.4 GHz and 5.8 GHz cordless phones are used today, so do not be surprised to see this interferer in 2.4 GHz or the higher end of 5 GHz bands. Figure 6.33 shows a spectrum capture of a cordless phone in 2.4 GHz.

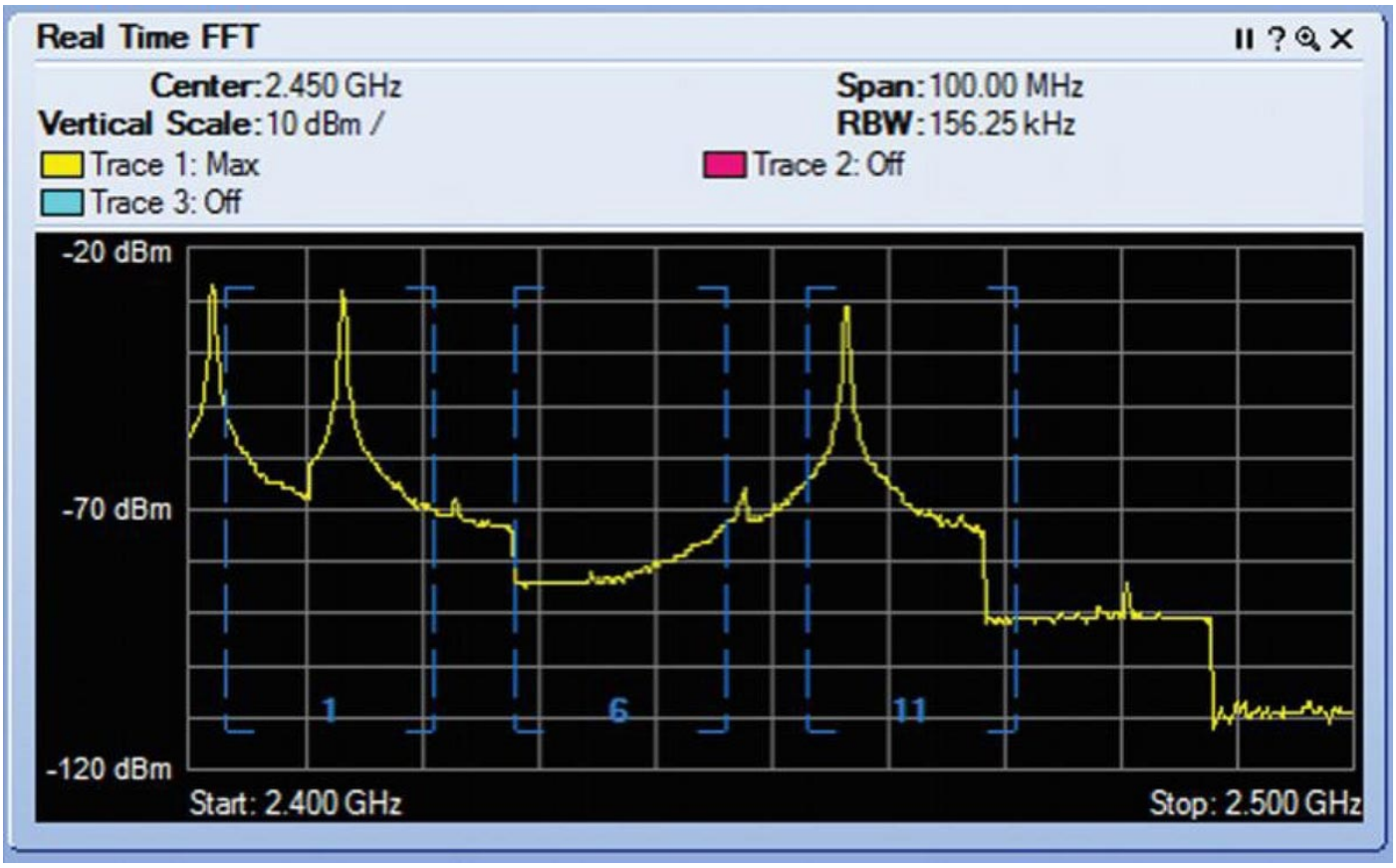


Figure 6.33: Cordless Phone

Video Transmitter Signal Pattern

Video transmitters have a similar transmit signature as audio transmitters with a narrow peak, high amplitude, and 100% duty cycle. Figure 6.34 shows a video transmitter. Some late-generation video transmitters operate in 5 GHz, and have a signal pattern that appears exactly like an OFDM signal, but with a very-high duty cycle.

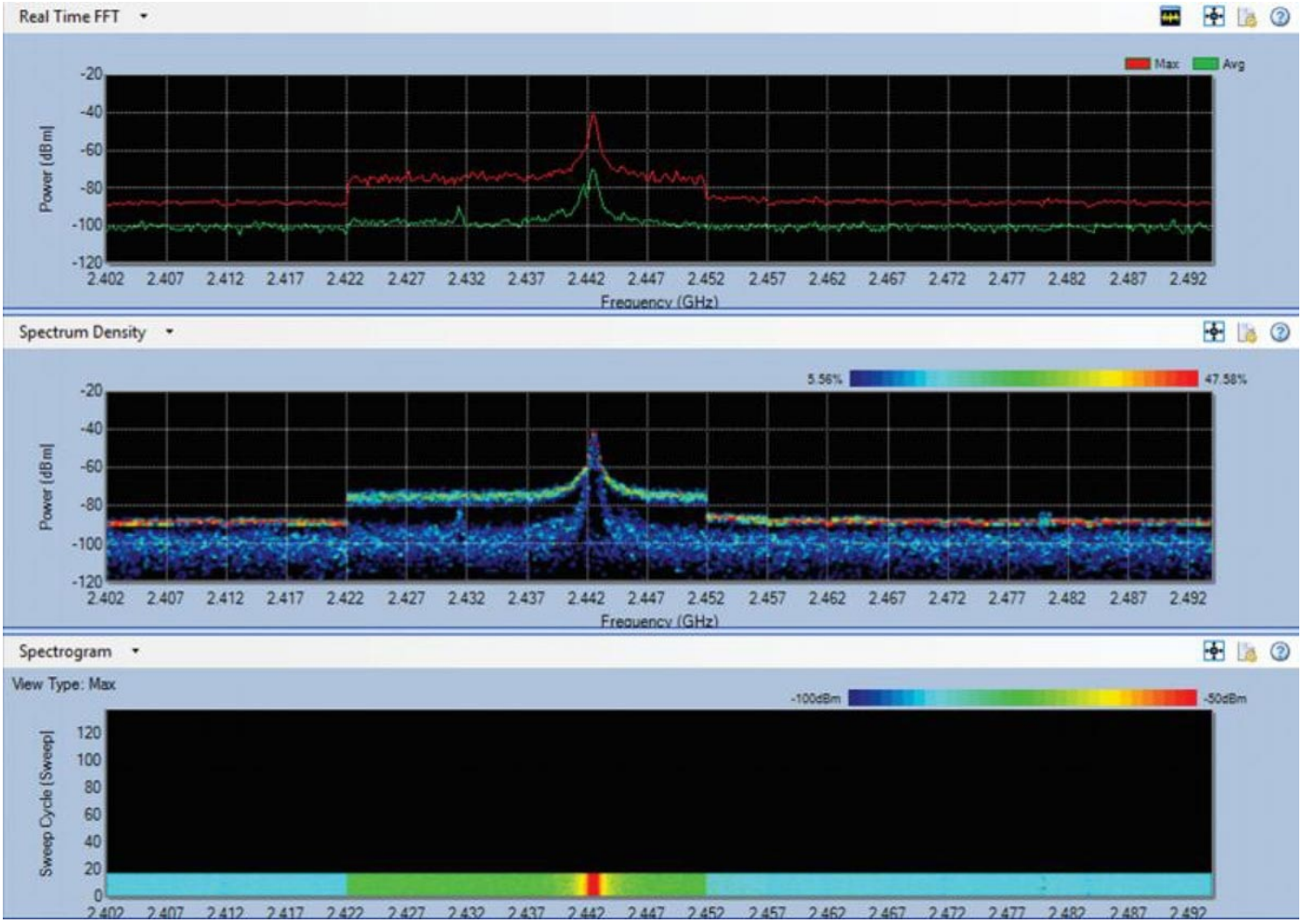


Figure 6.34: Video Transmitter

Wideband Jammer Signal Pattern

"Jammer" is a somewhat generic term for an RF signal generator. A signal generator is essentially a radio transmitter that can be designed for malicious purposes, or simply to test antennas or other RF components. In Figure 6.35, a wideband signal generator is emitting high-amplitude energy across the entire 2.4 GHz band. This would prevent any and all nearby 802.11 devices from communicating. Narrowband-signal generators are also common.

The word "jammer" typically alludes to malicious intent. Radio communications can be easily disrupted with a jammer.

Figure 6.35 shows a wideband jammer signal.

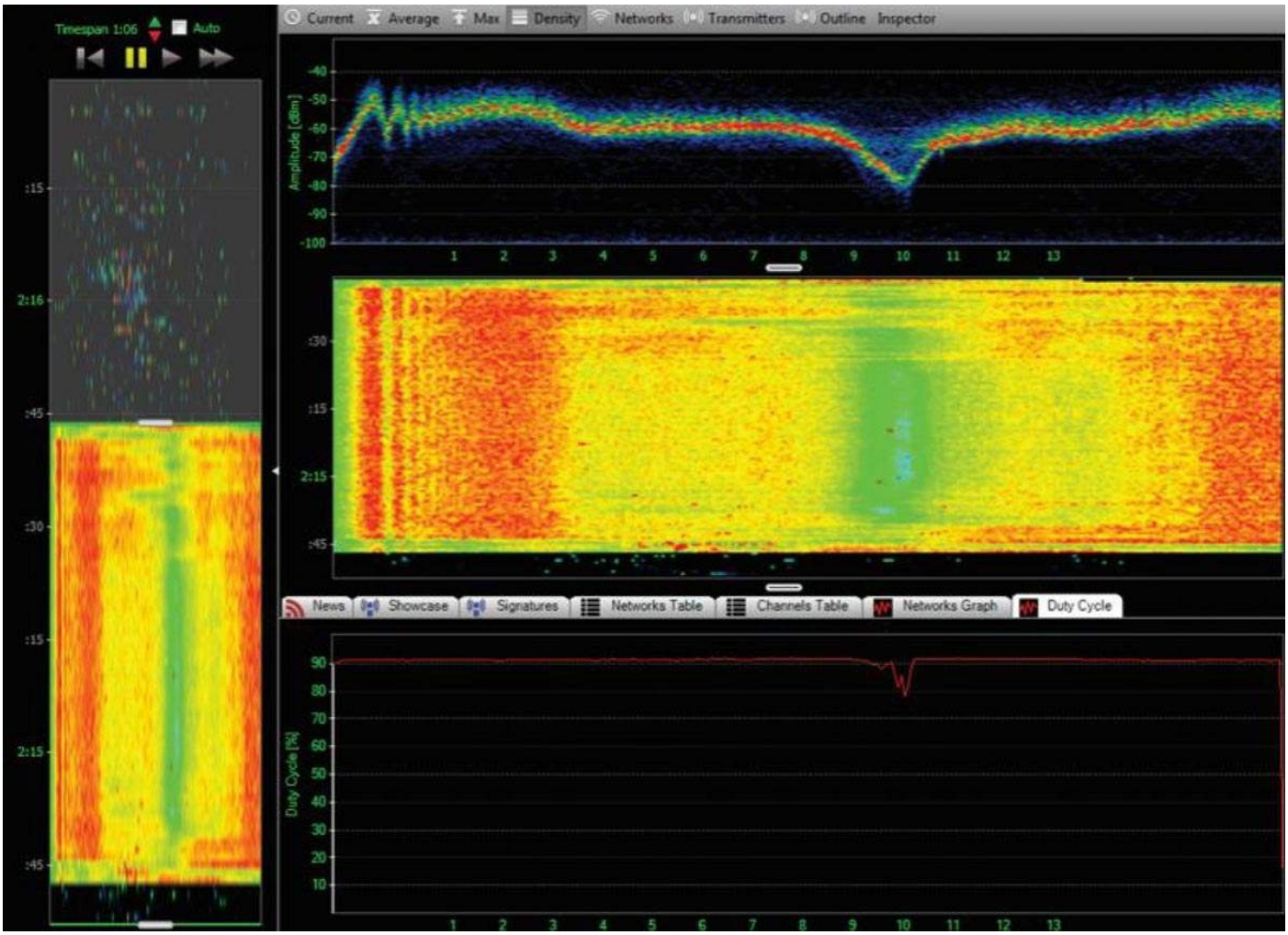


Figure 6.35: Wideband Jammer

Microwave Oven Signal Pattern

Microwave ovens come in all shapes and sizes, and their transmit masks vary right along with them. The consistent trend with microwave ovens is that they are high amplitude, and appear as fairly wide transmitters in a spectrum analysis. A microwave oven transmission typically centers between Wi-Fi channels 7–9. Cafeterias are well-known locations where microwave oven interference is likely.

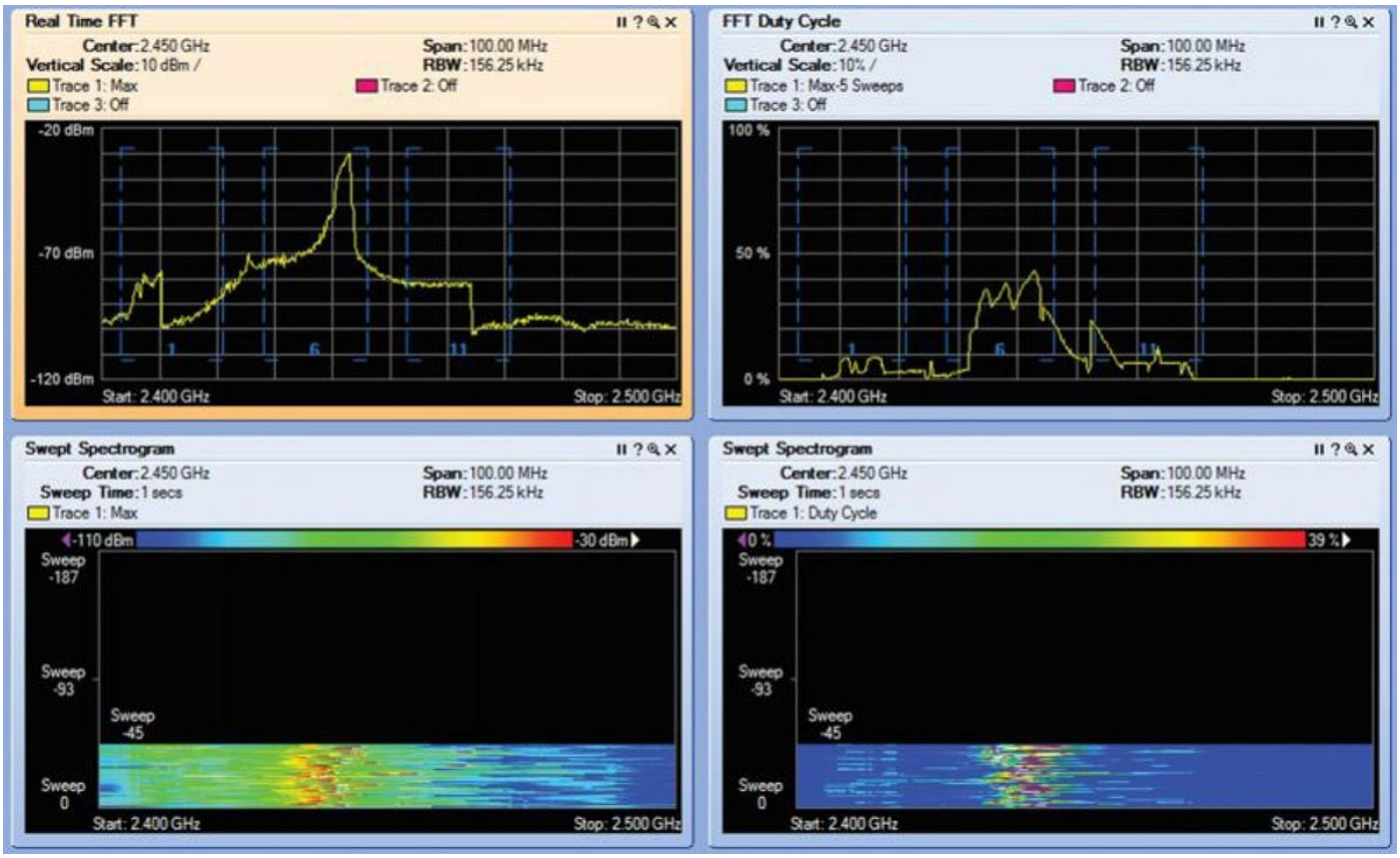


Figure 6.36: Microwave Oven

Locating Devices

The final component of performing spectrum analysis is device location. Locating devices is a process that involved:

1. Detecting a signal
2. Moving slowly to increase the received signal strength
3. Continuing to move in the direction of increased strength until the device is located

Directional antennas may be used to assist in device location. Metageek offers a directional antenna for the Wi-Spy DBx, and the Spectrum XT adapter supports external antennas as well. Using a directional antenna can make location procedures far more accurate.

> **EXAM MOMENT:** When locating devices, use a directional antenna to aid in the location of the signal source.

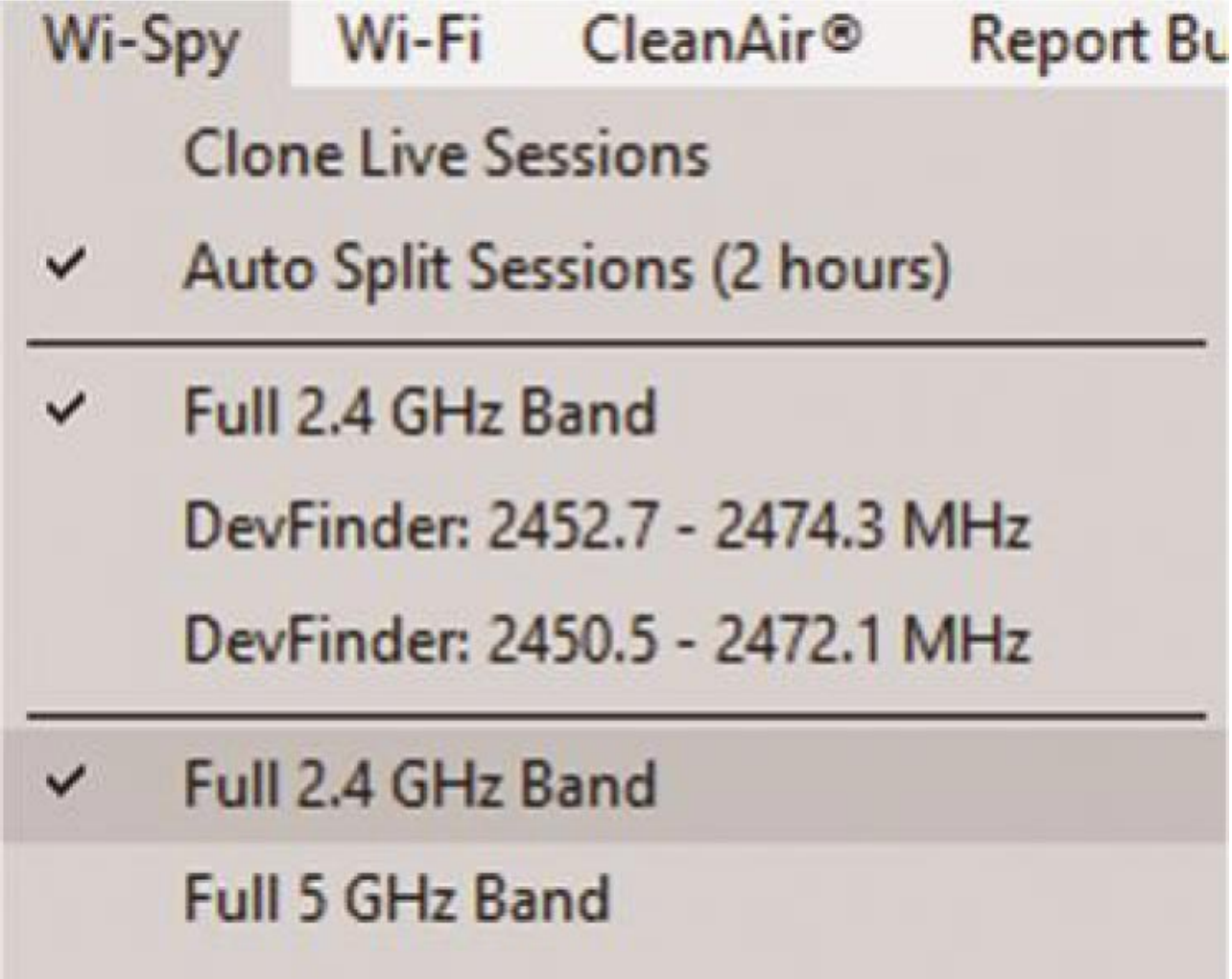
The software may also offer a device location feature. Figure 6.37 shows the device finder tool in Chanalyzer.

Figure 6.37: Chanalyzer Device Finder

Exercise 6

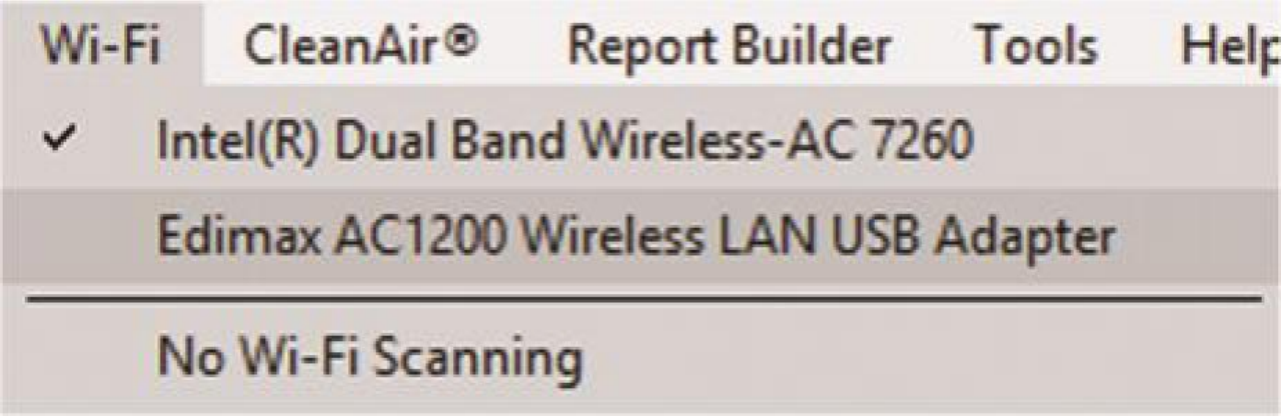
In this exercise, you will use a spectrum analyzer to first view the activity in the 2.4 GHz band and then the 5 GHz band. Additionally, you will use features of the analyzer to see the WLANs and their signals, as well as any other RF activity that may be outside the Wi-Fi signal space. If you do not have the Metageek Wi-Spy DBx adapter and Chanalyzer software to follow along with this exercise, you can view the video version of it at YouTube by searching for “CWNPTV Metageek spectrum analysis exercise.”

1. Insert the Wi-Spy DBz adapter into an available USB port.
2. Launch the Chanalyzer software.
3. Select Wi-Spy > Full 2.4 GHz Band from the menu.



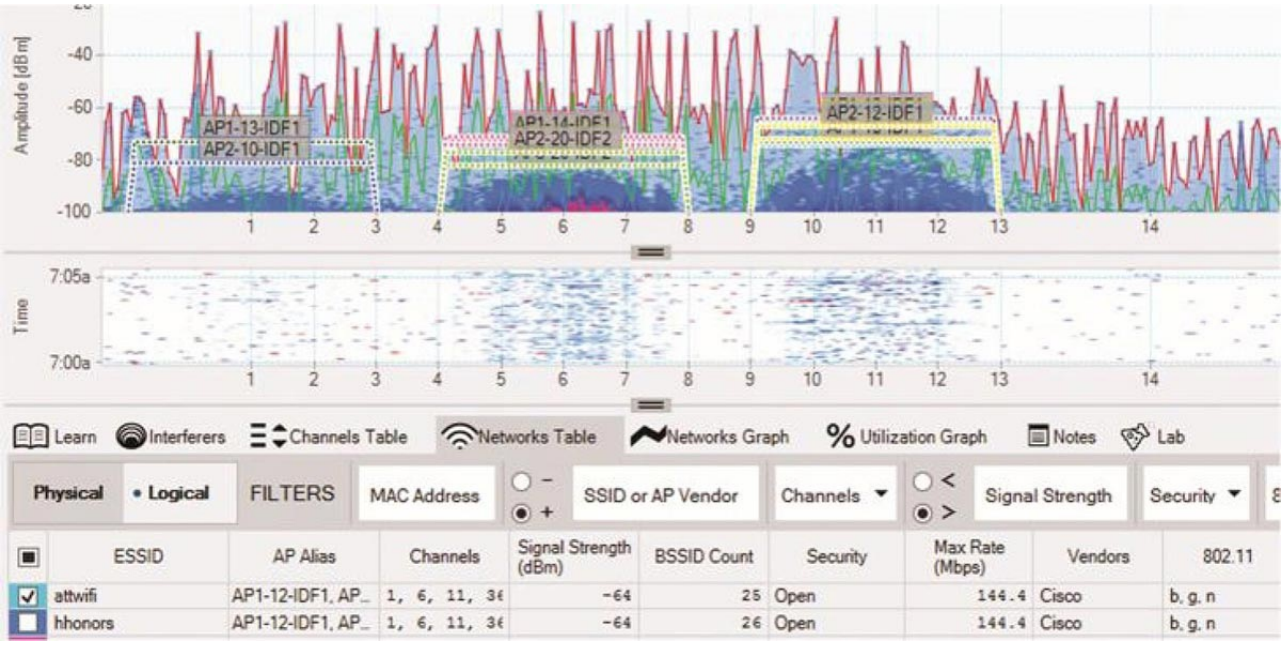
Graphic 6.1

4. Allow the spectrum analyzer to run for a minute or two to gather spectrum data.
5. Select Wi-Fi > *Your Adapter* to enable Wi-Fi integration.



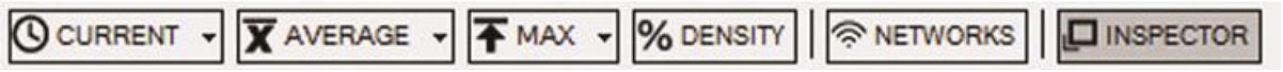
Graphic 6.2

6. Choose the Networks Table in the lower right pane of Chanalyzer.
7. Select (check) the networks you want to see in overlay in the density view.



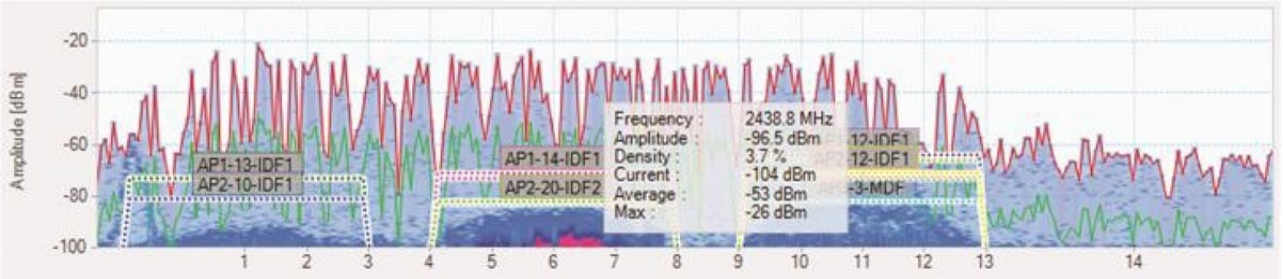
Graphic 6.3

8. Above the density graph, enable the INSPECTOR feature.



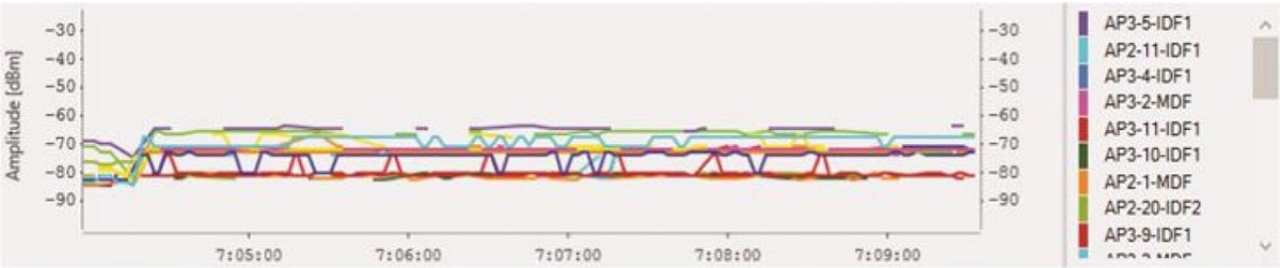
Graphic 6.4

9. Hover over an area of the density graph and notice the spectrum data it reveals with INSPECTOR enabled.



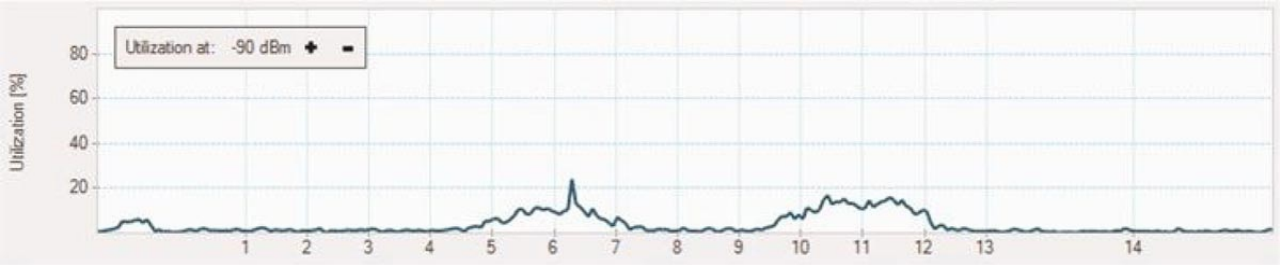
Graphic 6.5

10. Change to the Network Graph tab in the lower right pane. View the signal over time for the various networks.



Graphic 6.6

11. Change to the Utilization Graph and view the utilization. Notice you can change the signal strength at which to measure utilization (-90 dBm is shown).



Graphic 6.7

12. Select the Channels Table and note the information that can be gathered there. Grade is a measurement of interference impact versus a “perfect” channel. Higher grades are better.

Channel	Grade	Utilization	Average (dBm)	Current (dBm)	Max (dBm)	Noise Floor (dBm)	Access Points
11	90.4	8.8%	-58.0	-93.5	-31.5	-100.0	15
12	91.4	8.1%	-59.0	-84.0	-32.5	-100.5	0
10	91.4	8.3%	-57.5	-93.5	-31.0	-100.5	1
13	94.2	5.3%	-62.5	-84.0	-36.0	-101.0	0
9	94.2	5.9%	-57.0	-94.5	-30.5	-100.5	0
8	96.6	4.9%	-57.0	-92.5	-30.5	-100.5	0
6	97.1	4.7%	-55.5	-78.0	-29.5	-99.5	13
7	97.2	4.7%	-56.0	-78.0	-29.5	-100.0	0
5	97.3	4.7%	-56.0	-78.0	-29.5	-100.0	0
4	97.6	3.1%	-56.0	-78.0	-30.0	-101.0	0
1	97.7	1.5%	-60.0	-93.5	-33.5	-102.0	9
3	97.9	1.5%	-57.0	-95.5	-31.0	-101.5	0
2	98.1	1.1%	-58.5	-95.5	-32.0	-102.0	0
14	98.6	0.9%	-87.5	-84.0	-62.5	-102.5	0

Graphic 6.8

13. Select Wi-Spy > Full 5 GHz Band to switch to 5 GHz mode.

Graphic 6.9

14. Use the same features previously used in the 2.4 GHz band to gather information about the 5 GHz band.

Graphic 6.10

Chapter Summary

In this chapter, you studied spectrum analyzers. You learned about their features and capabilities, and gained insights into how to use them. You learned to select an antenna for spectrum analysis, and to use the typical configurations and features available. Finally, you learned to recognize common device patterns (signatures) and perform device location. In the final two chapters, you will learn to troubleshoot specific wired and wireless issues that impact your WLAN.

Review Questions

1. Which one of the following is not a spectrum analysis adapter or spectrum data source?
    a. Wi-Spy DBx
    b. Edimax
    c. Spectrum XT
    d. Clean Air
2. What kind of antenna is most useful when performing device location using a spectrum analyzer application like Spectrum XT or Chanalyzer?
    a. Omni
    b. Dipole
    c. Directional
    d. Rubber Ducky
3. A mW is what in relation to a Watt?
    a. 1/1000
    b. 1/100
    c. 1/10
    d. 1/100,000
4. To what is 0 dBm equal?
    a. 0 mW
    b. 1 mW
    c. 3 mW
    d. 10 mW
5. When a radio has an output power level of 100 mW and an antenna with 4 dB of gain is used, what is the output power at the antenna (EIRP)?
    a. 30 dBm
    b. 20 dBm
    c. 1000 mW
    d. 250 mW
6. When a radio has an output power level of 100 mW and an antenna with 7 dB gain is used, what is the output power at the antenna (EIRP)?
    a. 12 dBm
    b. 27 dBm

c. 150 mW

d. 600 mW

7. What measurement defines the amount of time in which the amplitude of RF energy in a frequency range is above an arbitrary threshold?

a. Sweep cycle

b. Duty cycle

c. Resolution bandwidth

d. Data rate

8. In what is RBW typically measured or assigned?

a. kHz

b. mHz

c. gHz

d. Hz

9. When using a higher RBW and longer dwell times, what is a potential problem?

a. Intermittent interferers may take much longer to detect

b. The ability to identify signal patterns will be lost

c. The spectrum analyzer may not be able to scan all of the selected range

d. 802.11 frames can no longer be captured by the spectrum adapter

10. Which of the following best defines a sweep cycle?

a. The length of time it takes to walk through a facility

b. The length of time between vacuuming the carpet

c. The length of time it takes to scan a band

d. The length of time it takes to gather all used data rates in a channel

11. In what domain does the real time FFT display the spectrum activity?

a. Frequency domain

b. Time domain

c. Windows domain

d. 2.4 GHz domain

12. Which of the following views would show RF activity over time?

a. Real time FFT

b. Swept spectrogram

c. Channel utilization

d. Channel client load

13. When a spectrum analyzer provides a grade or quality rating to a channel, what does this represent?
    a. The state of the channel compared with the previous channel in sequence
    b. The state of the channel compared with the next channel in sequence
    c. The state of the channel compared with some ideal perfect condition
    d. The state of the channel compared with the IEEE-specified proper channel condition
14. When a spectrum analyzers shows the actual SSIDs of WLAN channels in overlay mode on the spectrum views, what feature is being used?
    a. Wi-Fi integration
    b. Pattern matching
    c. Signature detection
    d. 802.11e
15. Which one of the following is likely to be used with an integrated spectrum analyzer?
    a. USB adapter
    b. Web-based interface
    c. Express Card adapter
    d. PCI adapter
16. When configuring a spectrum analyzer with a higher RBW, what additional setting or action would help reduce the amount of time required in each sweep cycle?
    a. Screen resolution
    b. Dwell time
    c. Disable Wi-Fi integration
    d. Connect the adapter to USB 3.0
17. What item in the IEEE 802.11 standard can reveal the expected pattern a WLAN channel should generate in a spectrum analyzer?
    a. Management frame format
    b. General frame format
    c. Spectral mask
    d. CCMP/AES encoding algorithm
18. What feature, if provided in a spectrum analyzer, would allow the automatic creation of a table of devices detected including non-Wi-Fi devices?
    a. Device identification

b. RBW adjustment

c. Dwell time adjustment

d. Reporting

19. What is a primary difference between Bluetooth in discovery versus Bluetooth in data transfer mode when seen in a Real-Time FFT view?

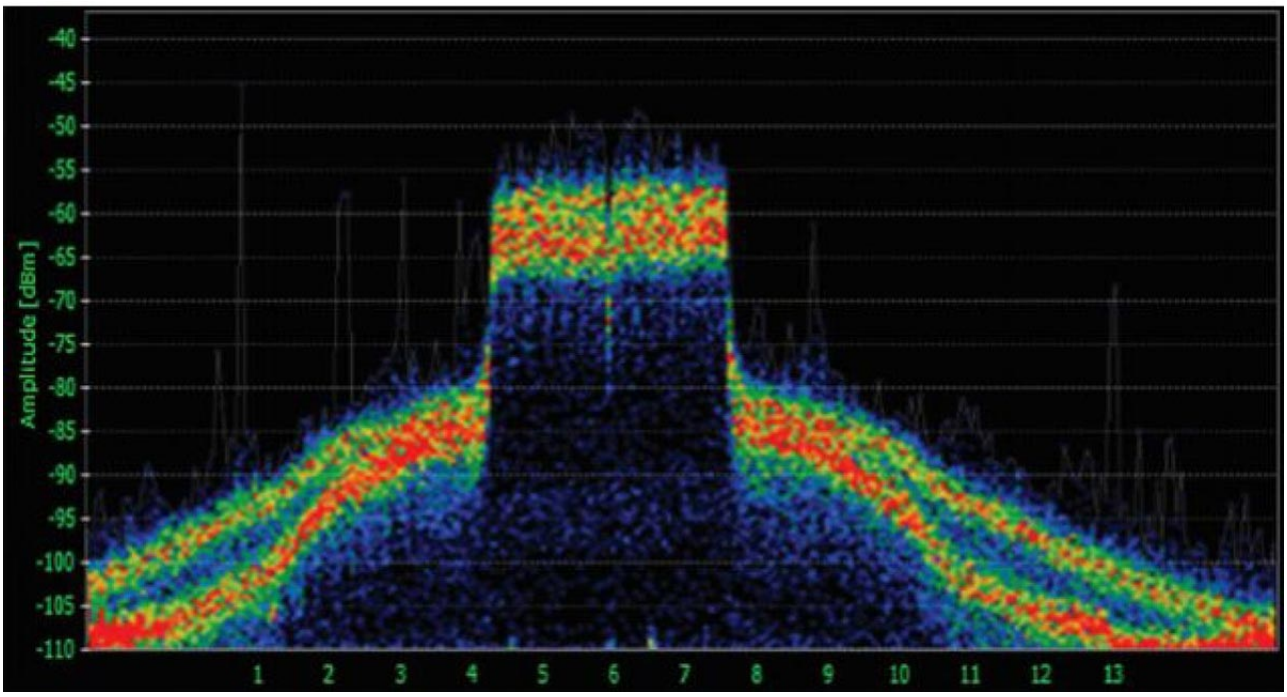
a. Discovery appears more structured than data transfer

b. Data transfer appears more structured than discovery

c. Discovery uses standard OFDM spectral masks

d. Data transfer uses standard DSSS spectral masks

20. What signal is represented in the following image?



a. Cordless phone

b. Bluetooth

c. 22 MHz DSSS

d. 20 MHz OFDM

21. What kind of device is represented in the following image?

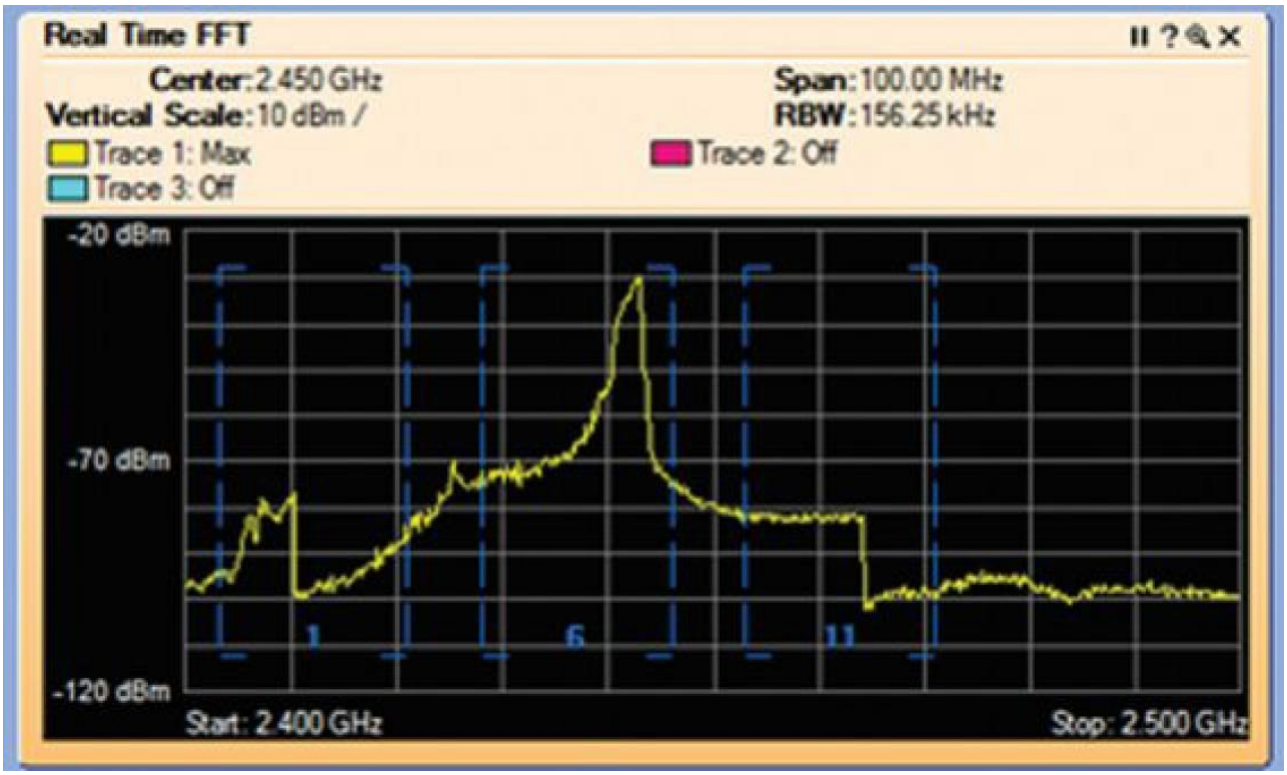
a. Bluetooth

b. 40 MHz OFDM

c. Cordless phone

d. Microwave oven

22. What kind of device is represented in the following image?



a. Bluetooth

b. Microwave oven

c. 802.11n

d. 802.11ac

23. When locating a device with a spectrum analyzer, what process should be used?

    a. Move quickly throughout the facility with a high RBW

    b. Move slowly throughout the facility while monitoring signal strength

    c. Use a protocol analyzer instead as the signal will be stronger

    d. Move in the direction of the weakened signal

24. To display AP information for BSSs in the 5 GHz band within a spectrum analyzer, what is required?

    a. A spectrum adapter supporting the 5 GHz band

    b. A wireless adapter supporting the 5 GHz band

    c. A dual-band wireless adapter

    d. An AP supporting spectrum monitoring

25. What can be used to run spectrum analysis software that required a different operating system than the one installed on a computer?

    a. An AP with spectrum monitoring support

    b. A serial link to another computer

    c. A virtualization solution

    d. A Metageek spectrum analysis PHY layer

Review Question Answers

1. **B** is correct. Edimax makes 802.11 adapters, but not spectrum analysis adapters. Wi-Spy DBx is a spectrum adapter and so it Spectrum XT. Clean Air is the spectrum monitoring feature of Cisco infrastructure solutions.
2. **C** is correct. A directional antenna will present a stronger signal when aimed toward the source of the signal. This would include reflected signals, so the path may change as you follow the signal.
3. **A** is correct. A mW is 1/1000 of a W. A microwatt (µW) is 1/1,000,000 of a W, therefore a µW is 1/1000 of a mW. Because received RF signals are so miniscule in power, they are represented in dBm instead of some fraction of a W.
4. **B** is correct. The fundamental formula of conversion between mW and dBm is the fact that 0 dBm is equal to 1 mW.
5. **D** is correct. 100 mW plus 10 dB is 1000 mW. 1000 mW minus 6 dB is 250 mW. Therefore, 100 mW with 4 dB of gain is 250 mW.
6. **B** is correct. Remember that 0 dBm is equal to 1 mW. Therefore, 10 dBm is 10 mW and 20 dBm is 100 mW. Given that 100 mW is 20 dBm, 100 mW with 7 dB of gain is 27 dBm or 500 mW (100 mW plus 10 dB minus 3 dB).
7. **B** is correct. Duty cycle is a reference to the RF energy measured above a given threshold. The default threshold can usually be changed in the spectrum analysis software. It is a time domain measurement.
8. **A** is correct. Resolution bandwidth (RBW) is measured or assigned based on frequency width and it is typically in kHz (kilohertz).
9. **A** is correct. With a higher RBW, scan times (sweep cycles) take longer. Longer dwell times also increase the time of the sweep cycle. The result of higher RBW and longer dell times is that intermittent interferers may take longer to detect because they may transmit at times when the analyzer is not reading the frequencies used.
10. **C** is correct. The sweep cycle is the length of time it takes to scan the band or frequency range configured for scanning in the spectrum analyzer.
11. **A** is correct. The real-time Fast Fourier Transform (FFT) view is in the frequency domain rather than the time domain.
12. **B** is correct. The swept spectrogram or waterfall views of spectrum analyzers would show RF activity over time.
13. **C** is correct. Spectrum analyzer channel grades are based on an ideal channel condition. A higher grade indicates a better channel condition.
14. **A** is correct. Wi-Fi integration, the use of an 802.11 adapter in addition to the spectrum adapter, is required to show information that would be revealed from beacon frames or other 802.11 communications.

15. **B** is correct. Integrated spectrum analysis is based on AP radios and does not use laptop adapters. Therefore, the Web-based interface is the likely listed item to be used.
16. **B** is correct. By reducing the dwell time, you can reduce the time required for a sweep when a higher RBW is used.
17. **C** is correct. The spectral mask is defined in the standard and provides a visualization of what, or relatively what, should be seen in a spectrum analyzer density or FFT view.
18. **A** is correct. Device identification is different from device detection. Device detection simply indicates that something is there. Device identification uses signal, signature or pattern matching to identify the actual device.
19. **A** is correct. Bluetooth discovery has a more organized appearance and Bluetooth in connected transmission mode has an appearance of randomness.
20. **D** is correct. The image shown is that of a 20 MHz OFDM signal, which appears the same in both 2.4 GHz and 5 GHz bands.
21. **A** is correct. The capture shown is of a Bluetooth device.
22. **B** is correct. The capture shown is of a microwave oven.
23. **B** is correct. Moving slowly in the continual direction of increased signal strength is key. It is important to remember that, due to reflections, it is possible that the direction of increased signal strength may vary as you move.
24. **B** is correct. A dual-band adapter is not required, but it usually selected. A 5 GHz adapter is required for the scenario.
25. **C** is correct. Many analysts use Mac OS X operating systems, which do not natively run most commercial WLAN protocol or spectrum analysis software applications. To remedy this, many analysts will run the software in a virtual machine with Windows installed as the guest operating system.

Chapter 7:

Wired Issues

Objectives

7.1 Understand and explain common wired problems that impact the WLAN including DNS, DHCP, switch configuration, WLAN controller access, and PoE.

7.2 Demonstrate the ability to troubleshoot wired issues using protocol analyzers, operating system commands, and hardware troubleshooting.

7.3 Select the appropriate location for placement of a protocol analyzer on the wired network and use it to troubleshoot common issues including DHCP, DNS, and data communications issues.

7.3 Analyze and repair Quality of Service issues on the wired side of the network.

Many “wireless” problems simply are not wireless problems. Stated clearly, they are not or 802.11 issues, but rather issues with supporting services. If the proper services for WLAN operations are not in place, the WLAN will either not function or not perform as intended. This chapter provides information on these supporting services in relation to WLANs and the techniques used to troubleshoot and repair them when those critical services experience problems.

First, you will explore a common set of problems that may occur. Then, you will explore the troubleshooting tools available, including protocol analyzers, operating system commands, and hardware troubleshooting. Finally, you will explore the issues related to Quality of Service (QoS) on the wired side that will determine whether the 802.11 QoS configuration (addressed more in Chapter 8) for a given WLAN achieves its ultimate goal.

Common Problems

Common problem areas in central network services include DNS, DHCP, switch configuration, WLAN controller access by APs, and PoE. This section will introduce the common problem areas, and the next section will provide actions steps for troubleshooting.

DNS

The Domain Name System (DNS) is used for host name to IP address resolution on networks of all types. On the Internet, it is used to resolve www.CWNP.com to the actual Web server IP address, for example. On internal networks it is certainly used for typical host name resolution, such as server1.company.local or client3.company.local. However, it is also used to resolve service locations. That is, a device may be used for more than one thing, and instead of resolving a single host name, multiple host names may point to a device.

In WLANs, at least three DNS host names are very important:

- WLAN controller host name
- RADIUS server host name
- LDAP or identity server host name

While this list is not exhaustive, it is enough to reveal the importance of DNS to WLAN operations. Without DNS, direct IP addresses would have to be used instead of host names. This would be quite challenging, particularly for the WLAN controllers, as a default DNS host name is typically preconfigured in the APs.

Two common problems occur with DNS when trouble hits: inability to reach the DNS server and inability to resolve a host name. Either issue results in a broken service in many instances. Some services have backup methods for determining the location of a device or service at the IP layer while others do not. If your service is entirely dependent on DNS, the service is broken when DNS is broken. Figure 7.1 shows the basic DNS name

resolution process. You will learn to troubleshoot DNS issues in the next major section titled Troubleshooting Issues.

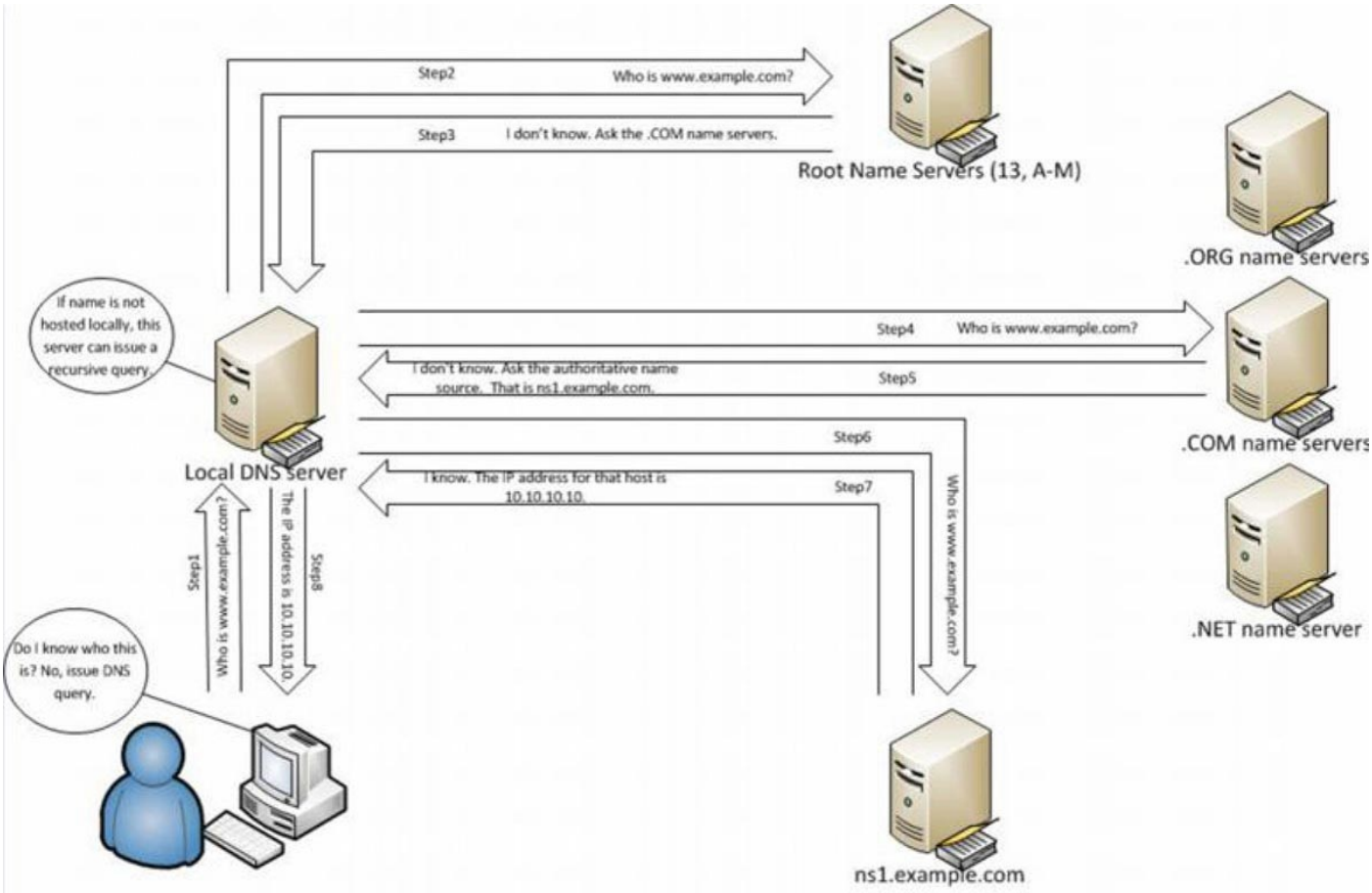


Figure 7.1: DNS Name Resolution Process

Figure 7.1 shows the typical DNS process; however, it is important to remember that for internal services, top level domain servers should not be required. When using a cloud-based WLAN vendor, Internet DNS servers are likely to get involved in the process. In order for internal DNS to work properly, the client (which can be a client STA, the AP, or the WLAN controller in a WLAN) must be able to reach the DNS server and the DNS server must contain the appropriate records (or be able to reach one that does) to service the client requests.

Troubleshooting DNS will be illustrated in a later section titled Troubleshooting Issues.

DHCP

The Dynamic Host Configuration Protocol (DHCP) is used to dynamically configure the host's IP protocol. These settings include the basic parameters such as IP addresses, subnet mask, default gateway, and DNS server. However, DHCP can provide more configuration details as well. Specifically, it supports vendor options. The vendor option is code 43, or DHCP option 43. It can contain data for different configuration parameters, but it is used in WLANs by many vendors to provide the IP address of the WLAN controller to lightweight APs.

Successful DHCP works using a four step process. This process is represented in Figure 7.2. It begins with a DHCP Discover message used to locate a DHCP server. The DHCP

server or servers will respond with a DHCP Offer message containing the IP configuration information and any options configured for the DHCP scope. The client responds with a DHCP Request (which is an acceptance communication) message followed by a DHCP Acknowledge message from the server. If everything works as expected, and the DHCP server is configured correctly and available, the result should be a device configured for proper operations on the local network at Layer 3 (Network Layer).

Note: **If you are newer to TCP/IP communications and administration, you may not be aware of the bootstrap protocol (BOOTP). BOOTP was created in 1985 and used for many years, but it lacked the ability to dynamically assign IP addresses. Instead it mapped MAC addresses to predefined addresses. In some systems DHCP may be referenced as BOOTP, but this is most often an inaccurate reference as the underlying protocol is actually DHCP. However, DHCP was based on BOOTP and was ratified as a standard via RFC in 1993, which was superseded ultimately by RFC 2131 in 1997.**

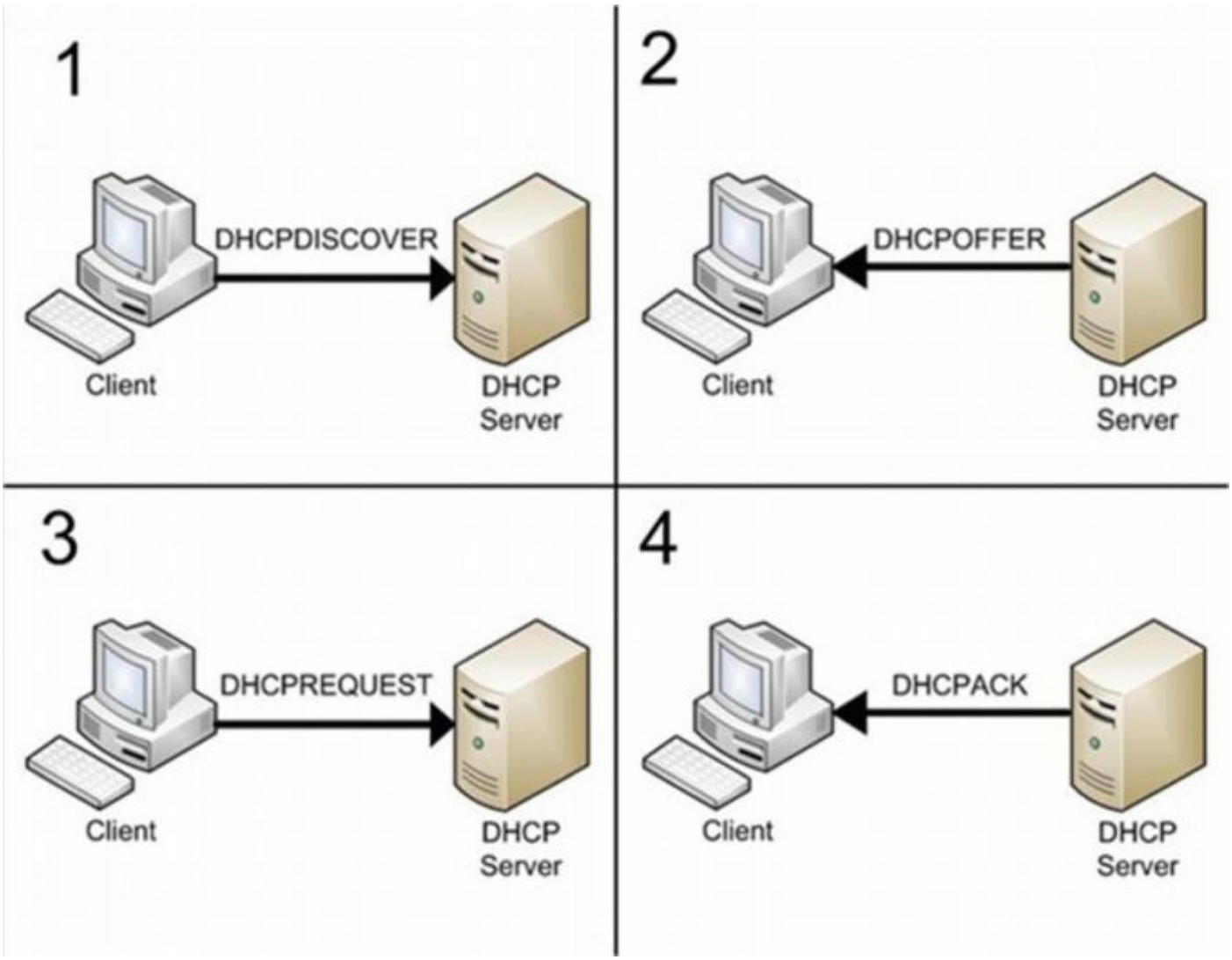


Figure 7.2: DHCP Process

When the DHCP server is not available, not operating properly, not configured properly,

or unable to handle more DHCP leases (the term used for a unique IP configuration for a specific client), the WLAN analyst must be able to identify resolve the issue. Troubleshooting DHCP will be illustrated in the later section titled Troubleshooting Issues.

Switch Configuration

Switch ports to which APs connect must be configured appropriately for the APs' requirements. With many lightweight APs, the switch port must be configured as an access port (though some lightweight APs do not require this). With many autonomous APs, the switch port must be configured as a trunk port for expected behavior and full VLAN support.

Troubleshooting switch configuration issues will be illustrated in the later section titled Troubleshooting Issues.

WLAN Controller Access

In a centralized WLAN model, the WLAN controller must be available for both APs to be configured and for many network operations to function. It is important that the APs be able to locate and access the controller. Four primary methods are used for this, and many vendors support all four methods. The methods are:

- Broadcast
- DHCP option
- DNS record
- Cached information

When using a broadcast message to locate the WLAN controller, the AP sends out a message to all devices on the same subnet in search of the controller. If a controller is available on the LAN (or through a VLAN that spans segments), it will respond to the AP. Using DHCP options (typically option 43), the AP received the controller IP address during DHCP configuration. In some instances a particular DNS record (for example Cisco-capwap-controller.mydomain.local) is created that points to the controller (or one specific controller if the organization has more than one). The APs know this DNS host name and perform a DNS query to resolve it to the controller's IP address. Finally, the AP may contain cached information indicating the IP address of the controller, and in such cases, it can use this to reach the controller.

Note: **Some vendors also support over-the-air-provisioning (OTAP). When supported, neighbor messages containing the controller IP address are sent from surrounding APs to the new AP. This feature is often disabled for security reasons.**

Troubleshooting WLAN controller access issues will be illustrated in a later section titled Troubleshooting Issues.

PoE

Power over Ethernet (PoE) is covered in detail in CWNA studies; however, troubleshooting PoE issues is an important skillset. The most common problem is simply insufficient or no power provided to the powered device (PD) from the power sourcing equipment (PSE). Troubleshooting PoE issues in a WLAN will be illustrated in the next section titled Troubleshooting Issues.

Troubleshooting Issues

This section introduces common wired problems that impact the WLAN and methods used to troubleshoot them. First, troubleshooting tools will be explored and then issues of importance.

Troubleshooting Tools

In earlier chapters you were introduced to basic troubleshooting tools and advanced tools like protocol analyzers. The range of tools include operating system commands, hardware troubleshooting components, and of course protocol analyzers.

Protocol Analyzers

On the wired network protocol analyzers are less difficult to implement and use than on the wireless network. This reality is because wired protocol capture can be performed with practically any Ethernet adapter. On the wireless side, a compatible adapter must be used that has matching protocol capture solutions (either built-into the protocol analyzer or as an external capture solution).

Wired protocol analysis is useful in determining problem locations in the network for QoS, DNS, DHCP, and other protocols that are used by wireless clients and APs. It will be used later in this chapter to explore troubleshooting procedures for various problems.

Operating System Commands

Operating system commands are simply computer programs or built-in commands provided with the operating system in use. Windows, Linux, and Mac OS X all support a basic set of commands used for troubleshooting and configuration with the TCP/IP protocol suite. These include:

- **IPCONFIG:** IPCONFIG is used to view the IP configuration, and when DHCP is used, request a new lease including whatever IP configuration settings and options are available from the DHCP server. On non-Windows operating systems, the IFCONFIG command can be used instead.
- **PING:** PING is useful when you need to quickly determine if an end system is

available on the network. As discussed in previous chapters, it uses the ICMP protocol to send and receive messages of specified length and provides insights into availability and loss of data. Its big brother, PATHPING, provides even more information with TRACEROUTE-type capabilities combined with statistical analysis.

- **TRACEROUTE:** If PING is unable to reach a destination end system, TRACEROUTE can be used to determine the route packets are typically traveling and the point at which they cannot continue their path to the end system. In Windows operating systems, it is the TRACERT command instead of TRACEROUTE.
- **NSLOOKUP:** NSLOOKUP is used to communicate with DNS servers. It is a useful tool to validate the existence of host records in the DNS zones managed by your servers and can play a key role in troubleshooting AP-to-controller access processes. On Linux systems the DIG command is often preferred, though NSLOOKUP is available.
- **NETSH:** NETSH can be used to view and configure many statistics and settings related to the wired and wireless network links in a Windows system. It is a large-scale system within itself and could be covered in a book-length treatment. It will be used later in this chapter to view some important configuration information. The ETHTOOL and IWCONFIG commands can perform some of the NETSH functions on Linux.

Hardware Troubleshooting

Hardware troubleshooting may include cable testing and physical evaluation of hardware indicators. For example, routers and switches use LEDs to provide status information on ports and overall device operational status. Because each vendor is different, the specific meaning of an LED will not be addressed here; however, it is important to know that you can evaluate LEDs to determine the state of the hardware.

In addition, you can use cable or line tester tools to determine the status of a cable or the links in the network. An example of such a device is the LinkSprinter 300 from Fluke Networks (the makers of AirMagnet Wi-Fi Analyzer Pro and Spectrum XT). Figure 7.3 shows this device. It can be used to quickly evaluate a wired link and verify DHCP, DNS, and Internet connectivity, as well as PoE. The LinkSprinter 300 can be connected to an Ethernet cable and, with Wi-Fi enabled on the LinkSprinter, be connected with any Wi-Fi browser-capable device. Detailed reports on PoE, the line speed, and more are made available. Such a device is useful for testing cables and connections before connecting an AP, and is also useful for troubleshooting line problems for installed APs.

Figure 7.3: LinkSprinter 300

```
C:\Windows\System32\cmd.exe

C:\Windows\System32>ping -a 192.168.10.1

Pinging VerizonBRV [192.168.10.1] with 32 bytes of data:
Reply from 192.168.10.1: bytes=32 time<1ms TTL=64
Reply from 192.168.10.1: bytes=32 time<1ms TTL=64
Reply from 192.168.10.1: bytes=32 time<1ms TTL=64
Reply from 192.168.10.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Windows\System32>
```

Figure 7.4: PING-based Name Resolution Testing Reverse Lookup

DNS Issues

Because APs use DNS to locate controllers, and all other IP devices use it for name resolution, it is a central part of your network. Most DNS issues can be traced to either server availability or host name record configuration. The simplest DNS resolution test is to use the PING command and check for name resolution. For example, Figure 7.4 shows the PING command against an IP address and the resulting name resolution. The –a switch tells PING to do name resolution. Figure 7.4 shows local resolution, and it works the same with a functioning DNS server providing name lookup. You can also ping the host name directly and, if it is able to locate the device and return results then name resolution has been successful as in Figure 7.5.

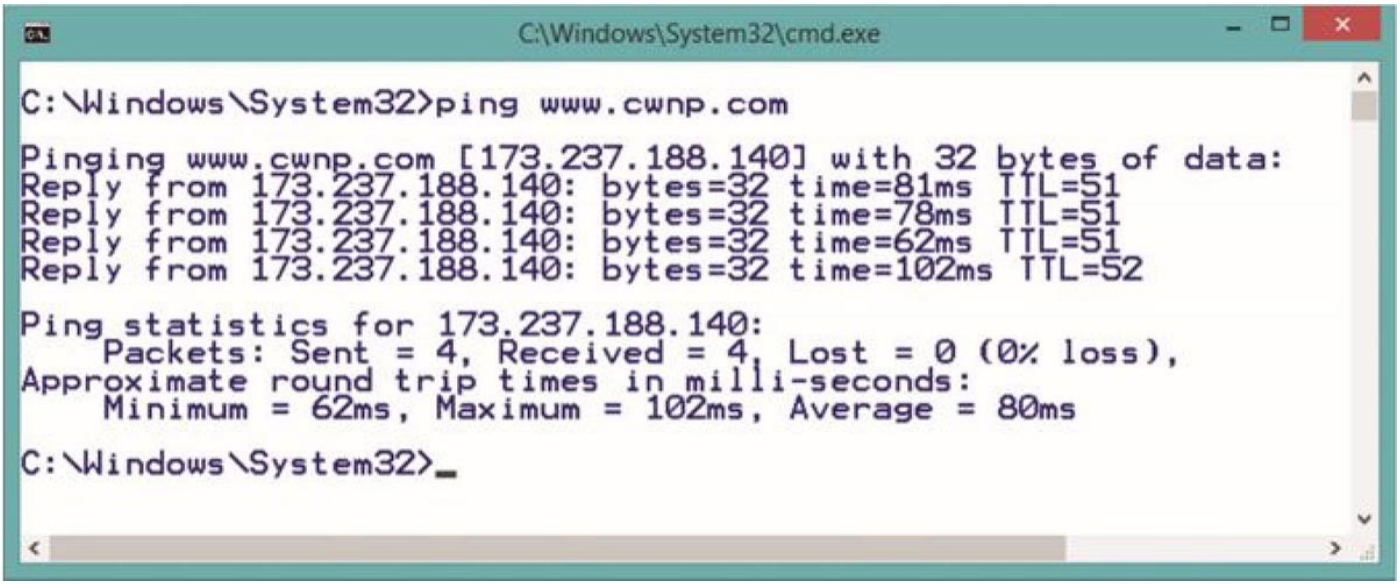


Figure 7.5: PING-based Name Resolution Testing Forward Lookup

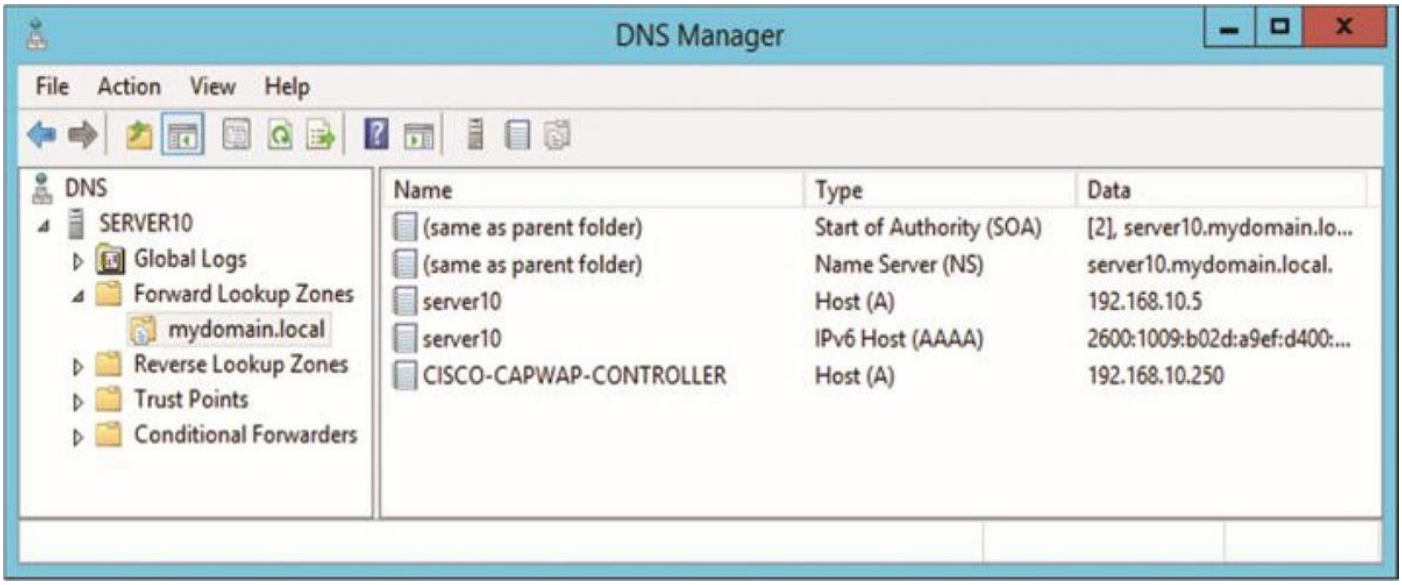


Figure 7.6: Windows Server 2012 R2 DNS Manager

If you have access, you can also inspect the DNS records in the DNS server itself. Figure 7.6 shows the Windows Server 2012 R2 DNS management interface with an entry for a Cisco WLAN controller (CISCO-CAPWAP-CONTROLLER.mydomain.local). The entry is a simple host record entry, and it should be configured to return the IP address of the controller.

An additional tool commonly used for DNS troubleshooting is the NSLOOKUP command. NSLOOKUP is the name server lookup utility, and it can be used in batch

mode or in shell mode. In batch mode you pass a full command set to NSLOOKUP as command line parameters. In shell mode (or console mode) you enter commands in a shell interface and after the results are shown you can enter further commands. You can direct NSLOOKUP to a specific DNS server or simply use the DNS server configured for use by the system on which the command is run. Figure 7.7 shows the NSLOOKUP command being used to query the CISCO-CAPWAP-CONTROLLER.mydomain.local host name.

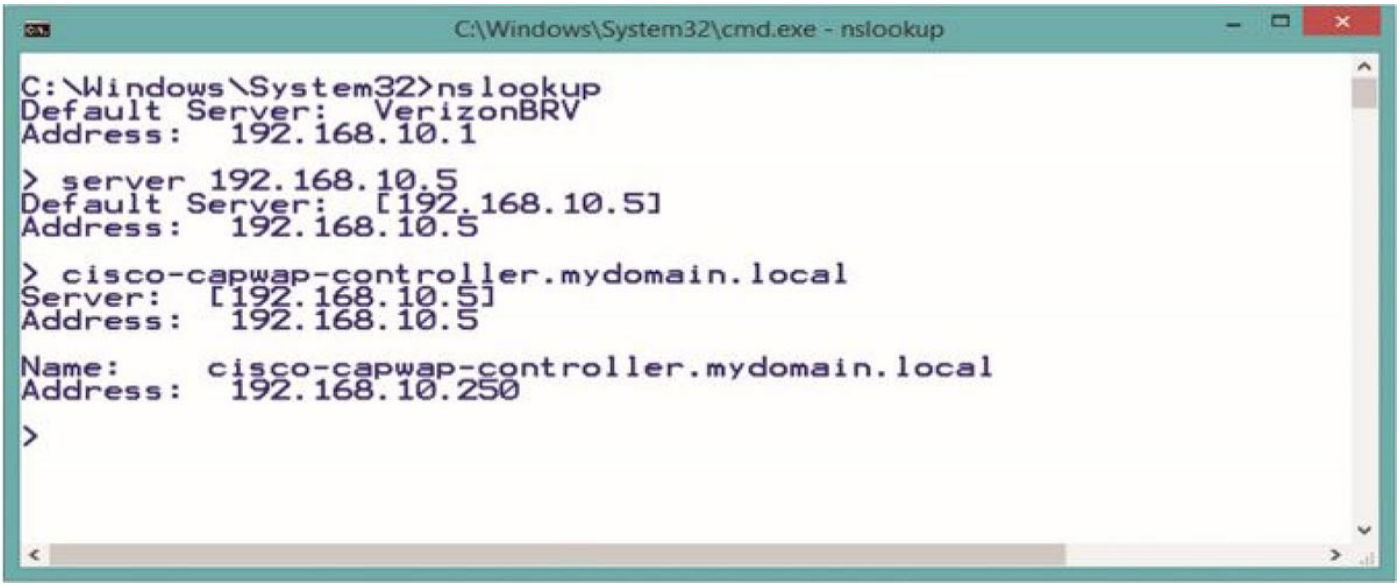


Figure 7.7: NSLOOKUP Performing a DNS Query

When DNS queries fail, verify the following:

- The server is available and reachable by the querying station.
- The host record exists in the DNS tables.
- The host record is properly configured.

If you wish to analyze DNS processes using a protocol analyzer, place the analyzer near the querying station first. If the DNS server is not responding, or the host record is not resolving correctly, consider placing the analyzer near the DNS server to see if the query is reaching it. If you determine that the query is not reaching the DNS server, the problem exists somewhere in the path between the client and the server. Use TRACEROUTE to determine the route, and then discover where the query is being lost. In most cases these extra steps will not be required with DNS as it is an infrastructure service and access to it is typically assured in the network design. Figure 7.8 shows the results of a DNS query for a Cisco host record entry.

> **EXAM MOMENT:** The DHCP server should be configured to provide the domain name (DNS – not Active Directory, though they are often the same) to the APs. This domain name will be used when querying DNS for the WLAN controller host records.

When querying a DNS server for a host record that does not exist, the packet trace will show a respond code of 3 in the flags section. This indicates that no such name (host record) exists. When you receive this reply, the configured DNS server is available and reachable, but the error is in the host record and not the network communications. If you are provisioning lightweight APs based on DNS and you receive a response code 3 (binary

0011), check the host records table to ensure proper entry of the host name. A simple typing mistake, such as CISCO-CAPWAP-CONTROLER as opposed to CISCO-CAPWAP-CONTROLLER (note the double “L”) can result in much havoc for your APs. It’s an easy mistake to make and just as easy to resolve. Figure 7.9 shows a Wireshark capture of a DNS response when the host record is not available.

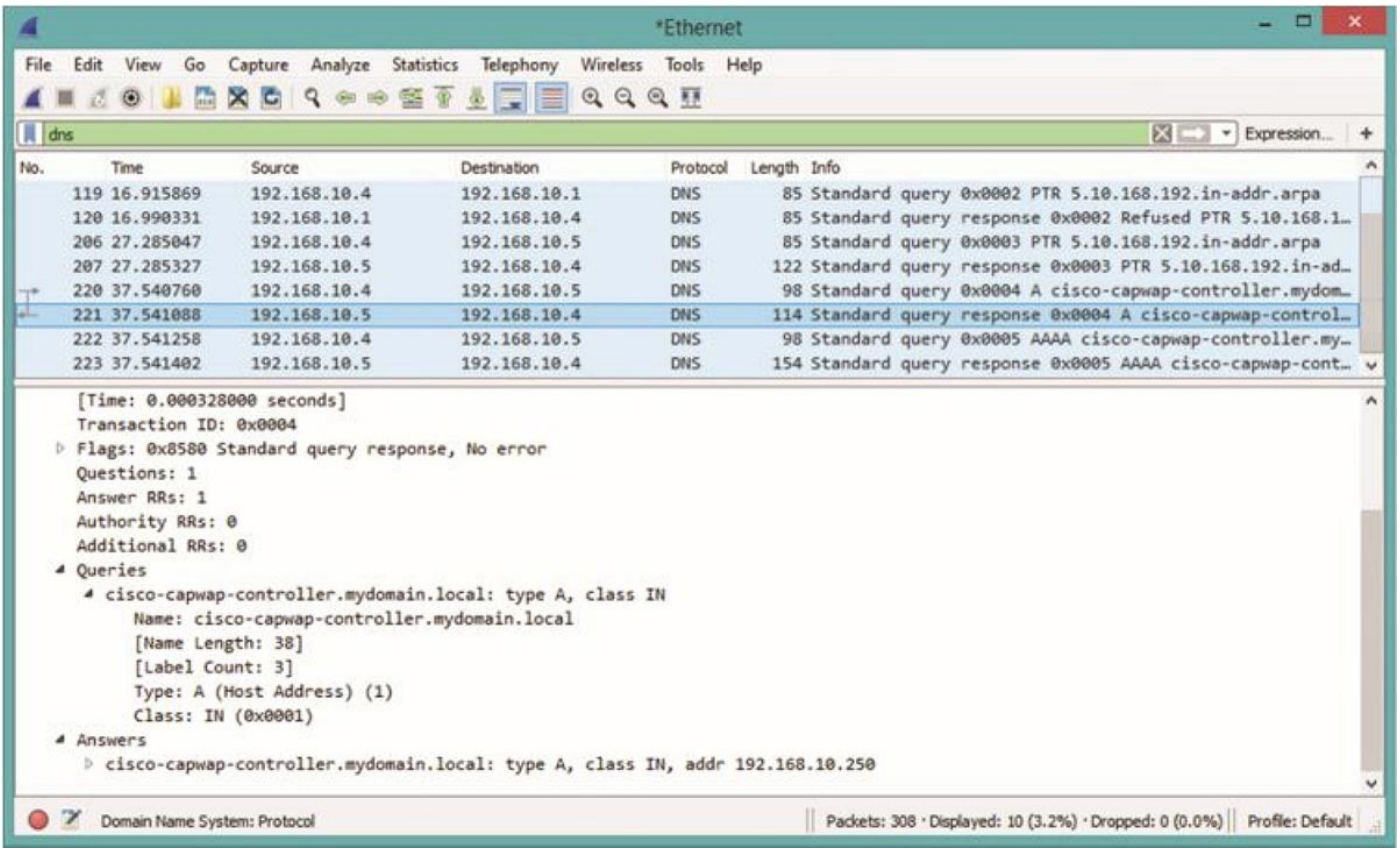


Figure 7.8: Wireshark showing DNS Query Response

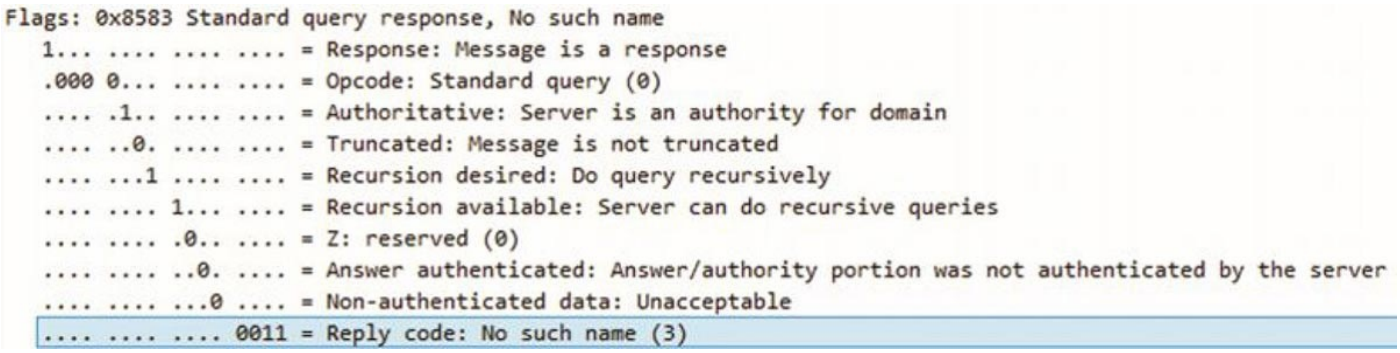


Figure 7.9: Wireshark showing DNS Query Response with No Host Record

DHCP Issues

DHCP is used by the clients on the network as well as the infrastructure devices and APs. It should provide the appropriate IP configuration settings for a given subnet and additional options as required. When DHCP is not working properly, it is typically one of three problems related to AP configuration or client access:

- DHCP location problems
- DHCP pool depletion

- DHCP configuration errors or missing information

The first problem is DHCP location. In order for any client (including an AP) to receive configuration settings from a DHCP server, it must have a DHCP server available on the local segment or a DHCP relay must be configured on the router or layer 3 switch to forward DHCP requests to a remote server. When you determine that the client cannot locate a DHCP server, verify that the server is connected to the local segment or that a relay configuration is in place and that the service is enabled on the server (which may be a router or layer 3 switch). You can determine if the DHCP server is simply depleted of addresses or unavailable entirely with a protocol analyzer.

A very common problem for WLANs is DHCP pool depletion. This occurs because many wireless clients come-and-go from the network quickly. If a client connects for only two or three minutes and the lease duration is set to multiple days (3-8 days is not uncommon), the IP address will be lost for that entire time. To resolve such issues, create more pools and reduce the lease duration to hours instead of days. Look for DHCP negative acknowledgement or server log errors to determine if the IP pool is depleted.

> **EXAM MOMENT:** DHCP pool depletion results in a DHCP negative acknowledgement sent to the requesting client from the DHCP server. It may also be shown in the server logs.

When a protocol analyzer is required, most DHCP problems can be detected by sniffing the traffic to and from the requesting device. Such monitoring will reveal the ability or inability to locate a DHCP server, the information provided by the DHCP server, and any errors of importance. For example, you can quickly determine if the DHCP server is properly returning option 43 parameters and if the client is requesting them with option 60 when required. If DHCP discovery messages are being sent but no offers are being received, this indicates that no DHCP servers are available to the local segment, or they are not responding for some reason. Additionally, on Windows Servers the Event Log will show an Event ID of 1063 when no IP addresses are available. In such cases the server may respond with a DHCP negative acknowledgement (DHCPnak) to the client, and this should be seen in the packet captures. However, not all DHCP servers respond with a DHCPnak if they are not directly contacted as opposed to broadcast-based requests. Additionally, if the DHCP server sees a response from another DHCP server, it may not send the negative acknowledgement.

WLAN Controller Issues

Other than configuration errors, the most common problem related to WLAN controllers is the lack of access by APs. When a lightweight AP is first connected to the network, it must be able to locate the controller. As stated previously, DNS, DHCP, broadcasts, and cached information may all be used to inform the AP of where the controller logically resides on the network. Therefore, when troubleshooting the inability of an AP to access the controller, the following should be evaluated:

- **DNS:** Given that many lightweight APs are configured to locate the controller based on a DNS entry, the DNS tables should be inspected to verify that the entry

is properly configured. Check the vendor literature to verify the appropriate record name.

- **DHCP:** The DHCP server should be configured to provide the IP address information to the APs, but it may also be required to pass information for option 43. Option 43 is a vendor information option and can be used for any vendor purpose. The vendor class identifier (VCI) (for example, “Cisco AP c3600”) is used with option 60 to determine the appropriate information to return with option 43.
- **Broadcast:** Ensure the WLAN controller is on the same broadcast domain as the AP if broadcast location is used.
- **Cached or Pre-configured Information:** This information must be accurate. If the AP was part of another network previously, the cached information can be removed; however, if the cached information fails, most APs will use another method to locate a controller.

```
Bootstrap Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xa219d13a
    Seconds elapsed: 0
  ▷ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 192.168.10.110
    Next server IP address: 192.168.10.5
    Relay agent IP address: 0.0.0.0
    Client MAC address: AsrockIn_0e:82:46 (bc:5f:f4:0e:82:46)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ◢ Option: (53) DHCP Message Type (Offer)
        Length: 1
        DHCP: Offer (2)
  ◢ Option: (1) Subnet Mask
        Length: 4
        Subnet Mask: 255.255.255.0
  ◢ Option: (58) Renewal Time Value
        Length: 4
        Renewal Time Value: (345600s) 4 days
  ◢ Option: (59) Rebinding Time Value
        Length: 4
        Rebinding Time Value: (604800s) 7 days
  ◢ Option: (51) IP Address Lease Time
        Length: 4
        IP Address Lease Time: (691200s) 8 days
  ◢ Option: (54) DHCP Server Identifier
        Length: 4
        DHCP Server Identifier: 192.168.10.5
  ◢ Option: (15) Domain Name
        Length: 15
        Domain Name: mydomain.local
  ◢ Option: (3) Router
        Length: 4
        Router: 192.168.10.1
  ◢ Option: (6) Domain Name Server
        Length: 4
        Domain Name Server: 192.168.10.5
  ◢ Option: (43) Vendor-Specific Information
        Length: 14
        Value: 3139322e3136382e31302e323530
```

Figure 7.10: DHCP Option 43 shown in Wireshark from a DHCP Offer Packet

> **EXAM MOMENT:** When configuring DHCP option 43, the VCI (option 60) is only required if more than one option 43 must be configured. That is, if the only use for option 43 within a scope is AP controller assistance, the VCI configuration is not required, and the single option 43 entry will be automatically passed to all DHCP clients of the scope.

If you wish to use a protocol analyzer to troubleshoot WLAN controller location issues, place the analyzer in a location where you can capture packets transmitted and received by the AP. This would typically be in the same switch as the AP with port spanning enabled. This will allow you to capture the CAPWAP broadcasts, DHCP processes, DNS queries, and all other communication attempts made by the AP to locate the controller. While you could place the protocol analyzer closer to the controller, the starting point would be near the AP. If, after capturing packets from the AP, you determine that it has received appropriate controller location information but is still not being configured, then consider capturing in or at the controller. Alternatively, you can inspect the logs on the controller to see if the AP has been rejected for some reason, and then take appropriate configuration or reconfiguration steps.

Figure 7.10 shows a Wireshark capture including DHCP option 43. In this case the server was not configured with a VCI as the only option 43 for the subnet used for APs. The IP address is shown in hex, but Figure 7.11 shows this decoded to ASCII in the decode pane.

```
◢ Option: (43) Vendor-Specific Information
    Length: 14
    Value: 3139322e3136382e31302e323530
◢ Option: (255) End
    Option End: 255

0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0110  00 00 00 00 00 00 63 82  53 63 35 01 02 01 04 ff   ......c. Sc5.....
0120  ff ff 00 3a 04 00 05 46  00 3b 04 00 09 3a 80 33   ...:...F .;...:.3
0130  04 00 0a 8c 00 36 04 c0  a8 0a 05 0f 0f 6d 79 64   .....6.. .....myd
0140  6f 6d 61 69 6e 2e 6c 6f  63 61 6c 00 03 04 c0 a8   omain.lo cal.....
0150  0a 01 06 04 c0 a8 0a 05  2b 0e 31 39 32 2e 31 36   ........ +.192.16
0160  38 2e 31 30 2e 32 35 30  ff                        8.10.250 .
```

Figure 7.11: DHCP Option 43 Decoded to ASCII showing the IP Address

An additional method for testing DHCP on a segment is to connect a laptop to the segment

and execute an `IPCONFIG /RELEASE` and `IPCONFIG /RENEW` command. A utility called DHCPTEST can also be quite useful and is available at `blog.thecybershadow.net/2013/01/10/dhcp-test-client`. This utility is shown in Figure 7.12, revealing the DHCP option 43 information received by a laptop client on the segment. When a DHCP offer is accepted, this information is stored in the Windows registry (search for `DhcpInterfaceOptions`) but it is in a binary format that is challenging to read. Therefore, the best options are either Wireshark or DHCPTEST, which are both freely available on the Internet.

Note: **To filter for DHCP-only traffic in Wireshark, use the BOOTP filter. No DHCP-named filter is available unless you are using DHCPv6.**

```
C:\Windows\System32\cmd.exe - dhcptest

C:\Windows\System32>dhcptest
dhcptest v0.5 - Written by Vladimir Panteleev
https://github.com/CyberShadow/dhcptest
Run with --help for a list of command-line options.

Listening for DHCP replies on port 68.
Type "d" to broadcast a DHCP discover packet, or "help" for details.
d
Sending packet:
  op=BOOTREQUEST chaddr=03:D5:FC:70:6A:DC hops=0 xid=765D10EE secs=0 flags=8000
  ciaddr=0.0.0.0 yiaddr=0.0.0.0 siaddr=0.0.0.0 giaddr=0.0.0.0 sname= file=
  1 options:
     53 (DHCP Message Type): discover
Received packet from 192.168.10.5:67:
  op=BOOTREPLY chaddr=03:D5:FC:70:6A:DC hops=0 xid=765D10EE secs=0 flags=0000
  ciaddr=0.0.0.0 yiaddr=192.168.10.111 siaddr=192.168.10.5 giaddr=0.0.0.0 sname=
 file=
  7 options:
     53 (DHCP Message Type): offer
      1 (Subnet Mask): 255.255.255.0
     58 (Renewal (T1) Time Value): 345600 (4 days)
     59 (Rebinding (T2) Time Value): 604800 (1 week)
     51 (IP Address Lease Time): 691200 (1 week and 1 day)
     54 (Server Identifier): 192.168.10.5
     43 (Vendor Specific Information): "192.168.10.250" (31 39 32 2E 31 36 38 2E
 31 30 2E 32 35 30)
Received packet from 192.168.10.1:67:
  op=BOOTREPLY chaddr=03:D5:FC:70:6A:DC hops=0 xid=765D10EE secs=0 flags=8000
  ciaddr=0.0.0.0 yiaddr=192.168.10.8 siaddr=0.0.0.0 giaddr=0.0.0.0 sname= file=
  11 options:
     53 (DHCP Message Type): offer
     54 (Server Identifier): 192.168.10.1
     51 (IP Address Lease Time): 86400 (1 day)
      1 (Subnet Mask): 255.255.255.0
      3 (Router Option): 192.168.10.1
      6 (Domain Name Server Option): 192.168.10.1
     19 (IP Forwarding Enable/Disable Option): "", "" (00)
     58 (Renewal (T1) Time Value): 43200 (12 hours)
     59 (Rebinding (T2) Time Value): 75600 (21 hours)
     28 (Broadcast Address Option): 192.168.10.255
     44 (NetBIOS over TCP/IP Name Server Option): C0 A8 0A 01
```

Figure 7.12: DHCPTEST.EXE Showing the DHCP Offers from a Segment

Switching and Routing Issues

For the WLAN the most common switch issue is a misconfiguration of VLANs or the switch port operating mode. Some APs will require the switch port configuration as a trunk and others will accept the default access port mode. For this reason unmanaged

switches are not typically used with APs in enterprise deployments. They do not allow configuration of the switch port modes, and all ports are simply access ports on unmanaged switches.

Lightweight APs typically connect to access ports, and autonomous APs may connect to access ports or trunk ports, depending on their requirements. Always check the vendor literature to verify proper configuration.

Note: **Some lightweight AP modes will require a trunk port configuration. For example, FlexConnect mode with Cisco APs will use a trunk port configuration on switch. It is beyond the scope of the CWAP exam to explain vendor-specific switch configuration commands. Check your vendor literature for options.**

An additional switch configuration parameter is the QoS settings. It is important to trust the AP to provide QoS parameters. For example, in a Cisco switch the `mls qos trust dscp` command (executed in interface configuration mode) can be used to trust the AP connected to the switch port in access mode. When in trunk mode, the `mls qos trust cos` command can be used. These commands are provided as examples and will not be tested on the CWAP exam; however, it is important that you know these types of commands must be used in order to accept the QoS tags from the AP and implement end-to-end QoS as discussed later in this chapter and the next.

When the client receives undeliverable errors, these can be the result of router configuration problems. Always check the access control lists (ACLs) on routers and switches to verify the allowance of appropriate traffic. ACLs can impact both the ability of clients to use network resources and the ability of APs to contact the controllers and other required services. Ensure that the following common ports are properly configured in your routers for access:

- **RADIUS:** 1812 (authentication) and 1813 (accounting) UDP
- **Older RADIUS:** 1645 (authentication) 1646 (accounting) UDP
- **NTP:** 123 UDP
- **CAPWAP:** 5246 (control) 5247 (data) UDP
- **LWAPP:** 12222 (control) 12223 (data) UDP
- **DNS:** 53 UDP
- **DHCP:** 546 and 547 UDP

When using a protocol analyzer to troubleshoot switch and router issues, the analyzer must be placed so as to capture incoming and outgoing packets on the switch or router interface. For the switch, connect the analyzer computer to a switch port and then span the monitored port to the analyzer port. For the router, determine the switch port to which the router is connected and then connect an analyzer to another port so you can span the router port to the analyzer port.

PoE Issues

PoE problems generally fall into the categories of no power or too little power. No power is typically an easy fix. Simply connect the switch end of the Ethernet cable to a PoE port, or insert a PoE injector into the path. Too little power can be a bit more difficult.

With too little power, it is either a PoE standard (as in 802.3at and af) mismatch or a power budget problem. Newer APs (802.11n and 802.11ac) often require 802.3at PoE instead of 802.3af. 802.3at provides up to 25.5 watts of power at the PD (30 watts provided from the PSE before attenuation). 802.3af provides only 12.95 watts of power at the PD (15.4 watts provided from the PSE before attenuation). If you have a newer AP, and it is either not operating or not operating with full features, verify that the Ethernet port has been provisioned with sufficient power from a switch supporting 802.3at.

The power budget problem is related to the number of PDs connected to the PSE. For example, If the PSE has a budget of 200 watts and six or seven APs requiring 30 watts are already connected, the result of connecting and attempting to provision an additional AP is usually failure. Either install an additional switch and redistribute APs, or provision the additional AP with a PoE injector instead of attempting to pull more power from the already saturated switch.

Tools like the LinkSprinter 300 can be used to evaluate PoE and the power provided on the cable. Figure 7.13 shows the web interface of the LinkSprinter 300 when connected to a PoE switch port.

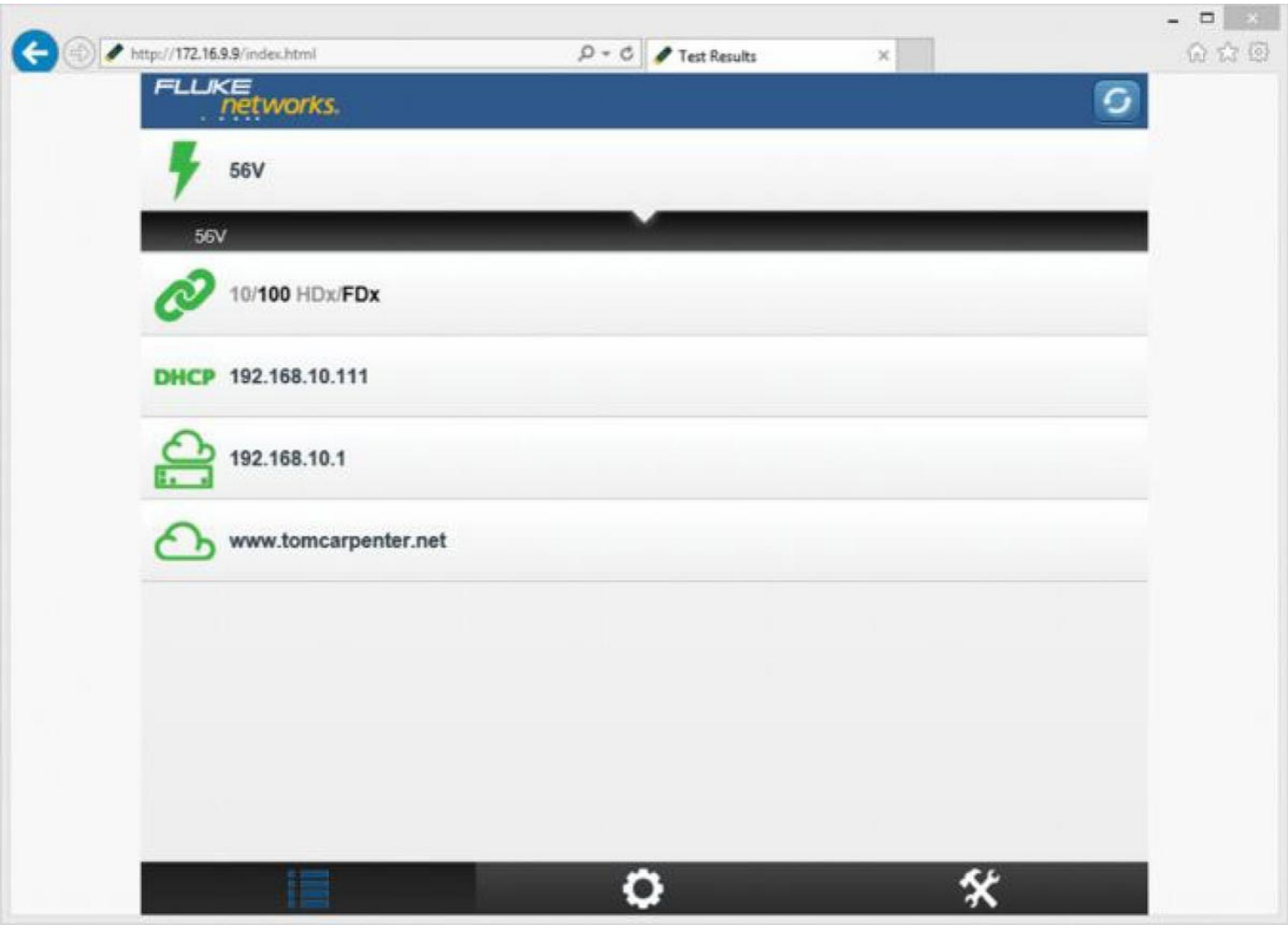


Figure 7.13: LinkSprinter 300 Showing PoE Power Reports

QoS Issues

QoS is applied at Layer 2 and Layer 3 of the OSI Model. At the Data Link layer 802.1p tags are used in the 802.1Q VLAN extension to the Ethernet frame. If you do not see VLAN information in the frame (even if a default VLAN is used), then you will not see QoS information in it on the wired side either. For wireless, as discussed in more detail in the next chapter, QoS information is provided in the 802.11 header. At the Network Layer Differentiated Services Code Point (DSCP) values are included in the IP header for prioritization. This section provides an overview of wired QoS and its interrelationship with wireless QoS.

Data is delivered on non-QoS networks in a best-effort model. This model gives no greater priority to any specific application traffic, and all traffic is treated the same. For traditional data-only networks, this model was acceptable. In modern converged networks with data, voice, and real-time video it is no longer an acceptable model. Instead, end-to-end QoS must be implemented at Layers 2 and 3 through class of service and DSCP.

The most common model used as an alternative to best effort is differentiated services. Integrated services requiring applications to request the service required before sending data is also available, but this discussion will focus on differentiated services.

The purpose of the Layer 3 and Layer 2 QoS solutions

Note: **discussed here is to tag packets and frames for classification. The switches and routers must use this information for internal queuing capabilities, which vary by vendor, and so are not addressed here in detail.**

Layer 3 QoS

Early Network Layer QoS was based on IP Precedence and later evolved into DSCP. Where IP Precedence used the 3 priority bits, DSCP uses 6 bits for a total of 64 possible priorities instead of the 8 possible priorities with IP Precedence. Today, DSCP is the more common marking in IP packets. Figure 7.14 shows the mapping of commonly used DSCP to IP Precedence values.

Examples of common values used from Figure 7.14 include (check vendor literature to see how these values are used in your equipment):

- DSCP 46 or IP Precedence 5 – expedited forwarding (EF) – typically used for VoIP
- DSCP 34 or IP Precedence 4 – assured forwarding (AF) – typically used for video conferencing and interactive video
- DSCP 10 or IP Precedence 1 – used for standard data
- DSCP 0 or IP Precedence 0 – best effort for background data

DSCP Name	Binary	Decimal	IP Precedence
CS0	000 000	0	0
CS1	001 000	8	1
AF11	001 010	10	1
AF12	001 100	12	1
AF13	001 110	14	1
CS2	010 000	16	2
AF21	010 010	18	2
AF22	010 100	20	2
AF23	010 110	22	2
CS3	011 000	24	3
AF31	011 010	26	3
AF32	011 100	28	3
AF33	011 110	30	3
CS4	100 000	32	4
AF41	100 010	34	4
AF42	100 100	36	4
AF43	100 110	38	4
CS5	101 000	40	5
EF	101 110	46	5
CS6	110 000	48	6
CS7	111 000	56	7

Figure 7.14: DSCP and IP Precedence

Various vendors may have recommendations different than those listed here. It is typically best to configure QoS according to vendor preferences, but it is essential to remember that much of IP QoS is out of the control of the infrastructure vendors as to how the IP packets are marked or tagged. For example, a VoIP phone may tag the packets, and the switches/routers must simply understand the tags and map them appropriately for routing and switching on the network.

Some QoS implementations simply use the class selectors 0-7 shown as CS0 through CS7 in Figure 7.14. This plan maps nicely to Data Link layer QoS class of service (CoS) 802.1p values as you will see in the next section. It also provides backward compatibility with IP Precedence ToS fields as they map directly to them. Notice that all of the CS0 through CS7 binary values in Figure 7.14 use only the first 3 bits of the available 6 bits. If you need the markings to be backwards compatible with some devices within the end-to-end link supporting only ToS and not DSCP, use only the class selectors when configuring QoS throughout the network.

Note: **If you've ever wondered why networks sometimes experience packet loss, it is a congestion management method. Without QoS infrastructure devices may drop any packet when the buffers are full. With QoS well-designed infrastructure devices drop lower priority packets and give favor to the higher priority packets in the buffers.**

Layer 2 QoS

At Layer 2 QoS markings are in the form of 802.1p class of service (CoS) markings or tags. CoS tags use 3 bits and range from 0 to 7. Table 7.1 shows the commonly used mapping of DSCP to CoS. CoS values are in 802.1Q Ethernet frames.

PHB (per hop behavior)	DSCP (binary value)	CoS
Default (BE also called CS0)	000000	0
Class Selector 1 (CS1)	001000	1
Class Selector 2 (CS2)	010000	2
Class Selector 3 (CS3)	011000	3
Class Selector 4 (CS4)	100000	4
Class Selector 5 (CS5)	101000	5
Class Selector 6 (CS6)	110000	6
Class Selector 7 (CS7)	111000	7

Table 7.1: DSCP PHB and Binary Values Mapped to CoS Values

The CoS bits are also called the user priority (UP) bits. The CoS value applied to an Ethernet frame may come from the switch port configuration, or they may be interpreted from the Layer 3 DSCP values. For this reason you must ensure that applications requiring priority treatment properly tag their IP packets with DSCP or at least ToS values. Many VoIP desktop applications, such as Skype, run without any QoS tagging, and if tagging is desired, it must be accomplished with something like Network-Based Application Recognition (NBAR) available from Cisco (and under other names from other vendors).

In addition to 802.1Q Ethernet frames, Inter-Switch Link (ISL) frames used between switches can also be tagged with CoS values. Figure 7.15 shows the different frames and packets in which QoS tags can be used. Notice that 3 bits are used for the UP or CoS values in both the ISL and 802.1Q/802.1p frames.

Note: **As you probably recall from CWNA studies, when an IEEE standard uses the capital letter nomenclature (such as 802.1Q or 802.1X) it is a reference to an independent standard. When the document uses the lower-case letter nomenclature (such as 802.1p or 802.11ac) it is a reference to a standard amendment rather than an independent standard. While a standard may be independent, this does not mean that it has no**

interactions with other standards. For example, 802.1Q has direct interaction with 802.3.

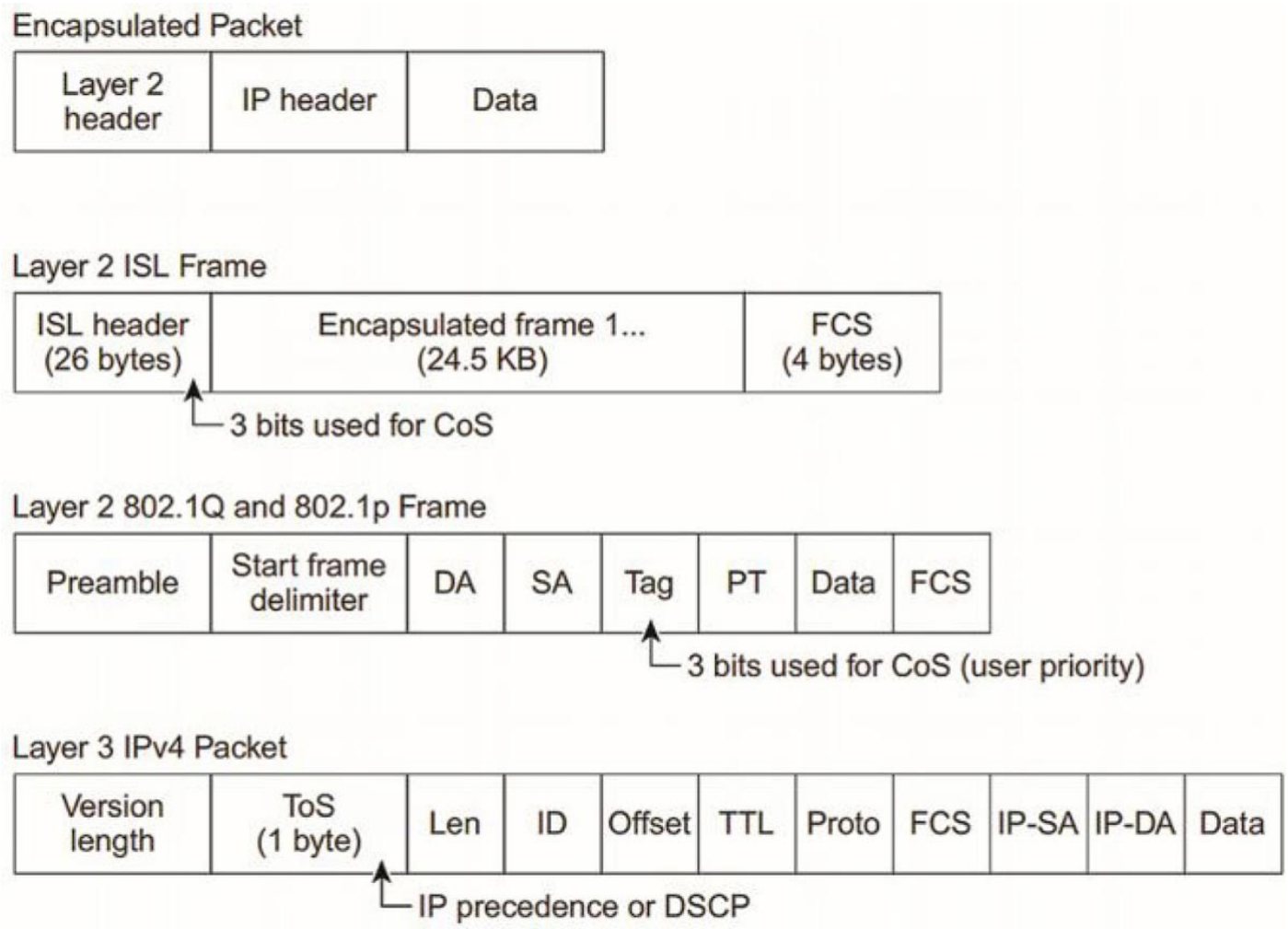


Figure 7.15: QoS Tags or Markings in Packets and Frames

End-to-End QoS

In order for QoS to work, each device on the network between the two communicating endpoints must support it. Consider the Ethernet frame format you explored earlier in this book. Remember that a destination address (DA) is part of the frame. If a frame is sent from Station A, in Figure 7.16 and is destined for Station B, it must pass through four switches and two routers. Given that the frame will first traverse from Station A to Switch 1, the first DA will be that of Switch 1. Now Switch 1 must send it to Switch 2 as well, requiring frame recreation. The new DA must be that of Switch 2. This process must continue at the LAN level, but it must also occur at the Network Layer when Router A and Router B deal with the packets. Therefore, if any of the six devices between Station A and Station B do not support QoS markings for the egress of packets or frames, the QoS bits will be stripped and the remaining portion of the route will be treated with best effort even if QoS is supported on devices further down the path.

From this explanation you should see why end-to-end QoS is so important. Many vendors now support automatic QoS features. In some cases, the automatic QoS simply implements best practices, and in others it monitors the network traffic and recommends QoS settings based on inspected communications. In either case if you do not plan to configure QoS on each device individually, enabling automatic QoS can make a

significant improvement on many small and large networks.

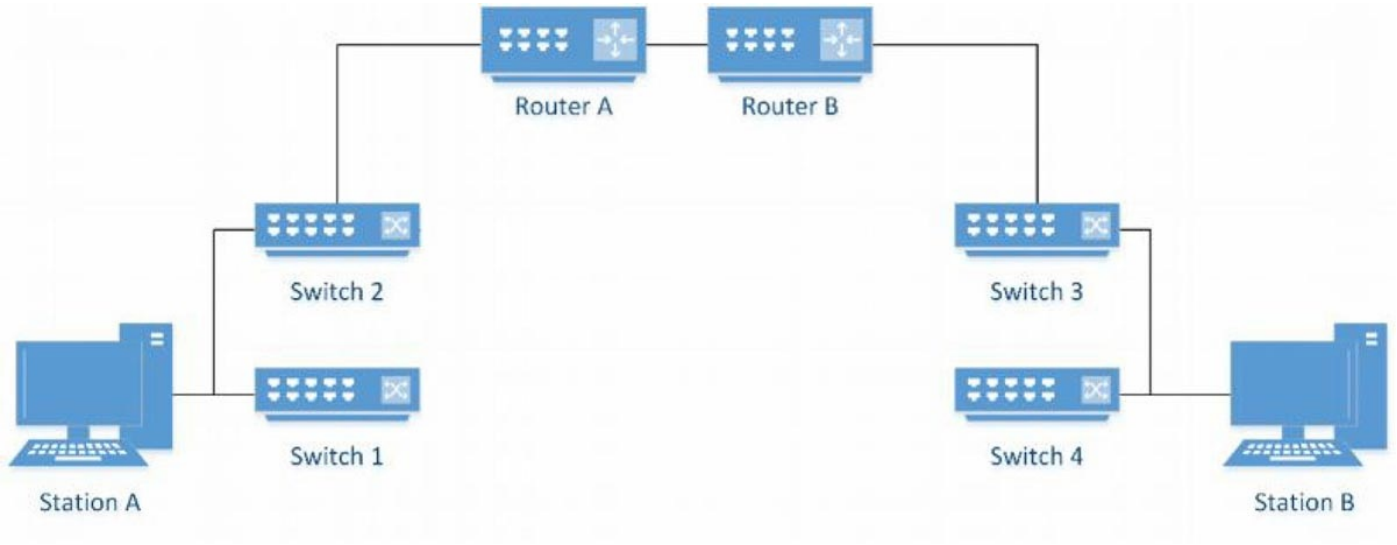


Figure 7.16: Sample Network for QoS Discussion

Troubleshooting Wired-Side QoS

Now that you have a basic understanding of wired QoS, it is important to know how to troubleshoot it. First, know that 802.11 QoS ultimately depends on properly configured wired-side QoS. Without it the 802.11 frames may get priority access to the wireless medium, but the frames and packets will be treated with best effort processing on the wired-side. Given that many high priority traffic classes require low delay (less than 100–150 ms one-way), it is important to have QoS properly configured on both the wired and wireless networks. Wireless QoS is discussed more in the next chapter.

The most common problems with QoS are as follows:

- Lack of an end-to-end implementation.
- Applications do not tag packets properly.
- Local departments assume that unmanaged switches are just as good.

The third problem will be addressed first. It is amazing how frequently local departments or branch offices will purchase equipment online or at a local electronics store and assume that they will work just fine. When first installed they may appear to function well, but as soon as users begin utilizing their computer-based video conferencing software, they find that performance is suffering. This is because most unmanaged switches do not properly support QoS. If the device tagged the 802.3 frame with a CoS value, the unmanaged switches will often remove them. Needless to say, this is a big problem and can easily be resolved by using only managed switches that support QoS implementation.

Note: **Some unmanaged switches will "honor" Layer 2 QoS tags; however, this does not allow you to enforce them if the device originating the transmission does not create them. On managed switches you can typically configure the switch port with a specific CoS tag based on the fact that you know a VoIP phone is connected to the port. Unmanaged switches do not offer this capability.**

When the end-to-end implementation of QoS is not contiguously functional between the source and destination hosts, it’s up to you to locate the point at which it is broken. You can easily test for end-to-end implementation by placing a protocol analyzer near the destination station and capturing its incoming packets. If they started with Layer 2 and Layer 3 tags but have reached the destination without them, somewhere in the path the QoS is broken. In most cases it is where an additional switch or router has been implemented (possibly as a replacement), and the installer simply forgot to configure QoS.

Finally, when applications do not tag packets properly, you have two options:

- Contact the vendor and ask them to update the application. If you have thousands of users running the application, this method may work. For smaller organizations it is seldom an effective option.
- Implement port-based QoS and NBAR (or its counterpart in a non-Cisco network). This allows tagging of CoS bits at the switch, and NBAR can also apply DSCP values at the Network Layer.

Additional Wired-Side Problems

In addition to the problems addressed so far, wired-side problems include cable faults, service availability, Internet connectivity (a major purpose in many WLAN connection), and home office issues. This section will address troubleshooting these areas.

Cable Faults

Cable faults are Layer 1 problems and can result from two common issues: improper wiring and cable failure. First, I’ll address improper wiring.

The most common network medium used in modern networks is the twisted pair cable. It is thinner and easier to work with than coax and works by implementing multiple conductor wires instead of just one center wire. These wires are twisted in pairs, hence the name twisted pair. Two kinds of twisted pair cable types exist: unshielded twisted pair and shielded twisted pair. Most 802.3 Ethernet networks are implemented using unshielded twisted pair cabling as the medium.

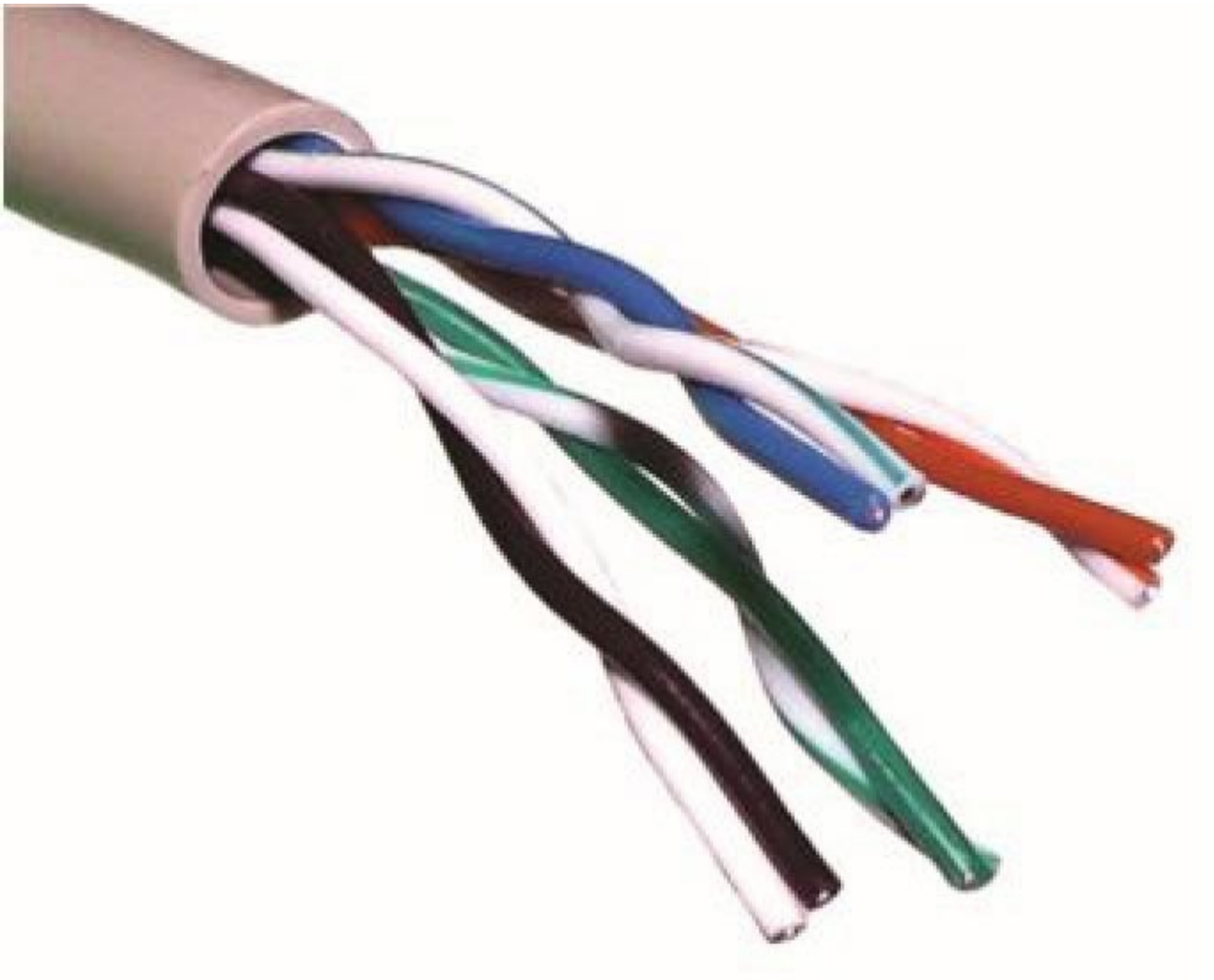


Figure 7.17: Unshielded Twisted Pair

An unshielded twisted pair (UTP) is implemented as an even number of wires twisted together in pairs and enclosed in an insulating sheath. A shielded twisted pair (STP) is implemented in the same way except the individual pairs are also insulated by a foil shield. This foil shield helps insulate the twisted pairs from each other within the STP cable. Due to the lack of standards, STP cables are rarely used. Figure 7.17 shows an example of a UTP cable, as this is the most common type implemented in IEEE 802.3 Ethernet networks.

UTP cables are classified in different categories and use wire pinouts (or connection patterns) that are defined in the Electronic Industries Alliance (EIA)/Telecommunications Industries Association (TIA) 568 Commercial Building Wiring Standard. Table 7.2 provides a listing of the categories that are defined in the EIA/TIA 568 standard. Note that these categories are often read or written as, for instance, CAT4 for category 4 or CAT5 for category 5.

Category	Application
Category 1	Traditional telephone connections. This is considered voice grade cabling and is not recommended for data.
Category 2	Provided rates of up to 4 Mbps and includes four pairs of wire (eight total wires). This category is rarely used due to its limited bandwidth.
Category 3	Provide bandwidth of up to 10 Mbps and includes four pairs of wire, as do all UTP cables. This category implements signaling rates up to 16 MHz and may still be seen in some 10BASE-T Ethernet implementations, though it should be considered obsolete at this time.
Category 4	This is the first category listed as data grade by the EIA/TIA and can provide up to 16 Mbps. Because it cannot provide 100 Mbps, it is not much more useful than CAT3 and is not commonly used even though it will support 10BASE-T Ethernet at 10 Mbps. This cable provides a signaling rate of up to 20 MHz.
Category 5	This is the most common UTP cable used in the first decade of the new millennium. It provides up to 100 Mbps and a signaling rate of up to 100 MHz. 100BASE-TX utilizes either CAT5 or CAT6 cabling. There is also a CAT5e cable that is useful for 1000BASE-TX connections running at 1000 Mbps or 1 Gbps, depending on the syntax you prefer.
Category 6	CAT6 is the most commonly recommended medium for 1 Gbps connections. The same jack is used for CAT5 and CAT6 cables (an RJ-45 jack), so the CAT6 cables are backward compatible. CAT6 is rated for signaling up to 200 MHz.
Category 7	CAT7 cabling contains four individually-shielded pairs contained within an all-encompassing shield. Data transmission speeds of up to 10 Gbps are supported. CAT7 cables are not backwardly compatible with CAT1-6 cables.

Table 7.2: UTP EIA/TIA Cable Classifications

Most modern networks use CAT5 (or CAT5e) or CAT6, with CAT6 or greater being used for 1 Gbps links. CAT6e is often used as a term for some manufacturer enhancements but is not a standard like CAT5e. CAT6 can also be used at speeds up to 10 Gbps.

While telephone cables usually use an RJ (registered jack)-11 connector, network cables

use an RJ-45 connector and jack as seen in Figure 7.18. This connector plugs into RJ-45 ports in network cards, switches, routers, firewalls, wall mounts, hubs, and many other networking devices.

Figure 7.18: RJ-45 Connector Used with UTP Cabling

In addition to the cabling type and connectors, it is important to remember that cables can be manufactured or assembled locally in two primary ways: straight through cables and crossover cables. A straight-through Ethernet cable is the most common type of cable used on modern networks. This cable is used to connect client computers to switches and switches to routers. Each end of the cable is wired in exactly the same way. For example, if T-568B is used on one end, it is also used on the other end when attaching the RJ-45 connector.

A crossover cable allows two devices to communicate without a connecting device, such as a switch, between them. The cable is designed so that the transmit wires on one end are configured as the receive wires on the other end and vice versa. Considering the listing for wiring RJ-45 connectors in Table 7.3, the only requirement for creating a crossover cable is that one end of the cable should be wired with pins 1 and 3 and pins 2 and 6 swapped. Crossover cables can be purchased from online stores and some local computer stores or they can be built using a crimping tool (a special tool that presses the wires into the pin connectors in the RJ-45 connector shown in Figure 7.19).

Pin	Wire Color
1	White with orange stripe (WO)
2	Orange (O)
3	White with green stripe (WG)
4	Blue (Be)
5	With blue stripe (WBe)
6	Green (G)
7	White with brown stripe (WBr)
8	Brown (Br)

Table 7.3: RJ-45 PIN connects when creating a T-568B connection

Figure 7.19: RJ-45 and RJ-11 Crimping Tool

UTP cables use the RJ45 connectors as cable ends or terminators. The UTP cable is an eight-pin cable that uses wiring standards based on the T-568A and T-568B assignments within the TIA/EIA-568-B-1-2001 standard. If you hold an RJ-45 connector as if you are

about to plug it into a port in the wall and look down at it, the pins are numbered from 1 to 8 as shown in Figure 7.20. Notice, in Figure 7.20, that the clip is on the opposite side, and this is important as a reference when creating cables. Table 7.3 lists the proper wire to pin assignment when creating the common T-568B connections used in modern networks.

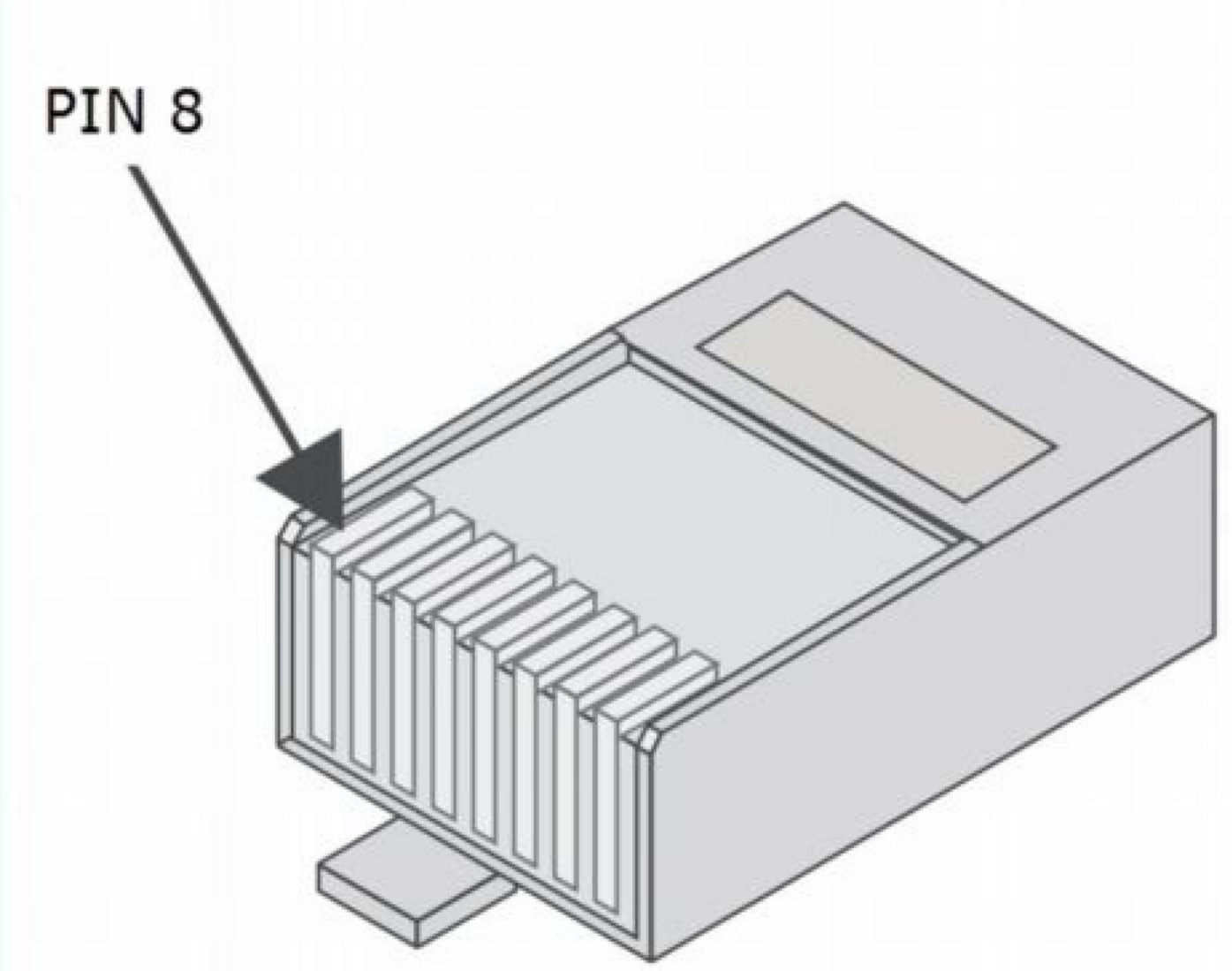


Figure 7.20: RJ-45 Connector Diagram with Pin 8 Identified

Figure 7.21 shows the T-568A and T-568B pinouts. Remember that most modern networks use T-568B, but if your network for some ancient reason uses T-568A, that should be used. Given that improperly wired cables are common problems, be sure to use this information as a guide when creating cables. In most large environments cables are created rather than purchased as the cost factor is much lower when you buy RJ-45 connectors and cabling in multi-thousand foot lengths.

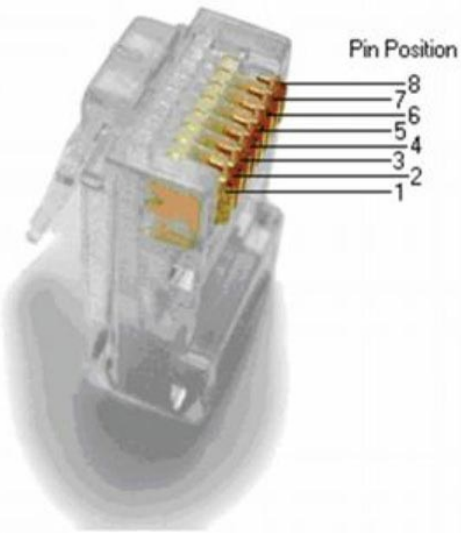
Pin	T568A Pair	T568B Pair	Wire	T568A Color	T568B Color	Pins on plug face (jack is reversed)
1	3	2	tip	white/green stripe	white/orange stripe	
2	3	2	ring	green solid	orange solid	
3	2	3	tip	white/orange stripe	white/green stripe	
4	1	1	ring	blue solid	blue solid	
5	1	1	tip	white/blue stripe	white/blue stripe	
6	2	3	ring	orange solid	green solid	
7	4	4	tip	white/brown stripe	white/brown stripe	
8	4	4	ring	brown solid	brown solid	

Figure 7.21: T-568A and T-568B Pinouts (image courtesy of www.desertelectric.com)

The second problem with cabling is cable failure. Wires break and shielding can fail. In these cases the signal cannot pass through the cable and communications falter. Cable testers can be used to verify cable functionality; however, it is important to remember that, if you are able to communicate using some higher layer protocols, but not others, the cable is not the fault. Figure 7.22 shows a wired cable tester and, additionally, tools like the LinkSprinter 300 referenced earlier in this book can be used to test a cable. If the LinkSprinter 300 is not able to gain a connection using the cable, and the switch port is determined to be operational the cable is likely at fault.

Figure 7.22: Ethernet Cable Testing Tool

The use of a cable testing tool like the one shown in Figure 7.22 is simple:

1. Connect one of the components of the testing tool to each end of the cable.
2. Power on the powered end component.
3. Verify that the wires (1–8) are lighting up as expected.

Service Availability

Service availability problems fall into two general categories: reachability and availability. Reachability is related to the switching and routing infrastructure and the IP configuration of the requesting node. Availability is related to the redundancy and performance of the service-providing device or server.

As an example, consider the NTP service. Time synchronization is very important for network devices. It impacts authentication and wreaks havoc on log files if the times on various devices are out of synchronization. Therefore, the reachability and availability of the NTP server is important. Many small businesses simply synchronize with an Internet time server, but larger organizations implement their own internal servers.

To troubleshoot reachability of a service, verify the following:

- **Proper client configuration:** Includes the IP configuration of the client and the addresses or host names of the service providers.

- **Access control lists:** Ensure that all ACLs (on switches and routers) allow connectivity to the target IP address from the source location and pass through of the utilized TCP or UDP ports.
- **Switching and routing configuration:** Ensure that switches have the proper links to other switches and/or routers. Verify that the routing protocols have converged such that all areas of the network can be properly accessed.
- **Server configuration:** Ensure that the server, if running a local firewall, allows communications with the service from the client networks. Verify that the server's IP configuration settings are accurate.
- **Hardware testing:** Ensure that all ports in the path are working properly, and that all cables are still functioning.

Availability is impacted by the performance of the servers providing the services and the number of servers providing the service. The performance of the servers is important in that it will determine the number of clients the server can attend. It is important to remember that many servers provide multiple services, and the performance of one service can be greatly impacted by the other services. Such a configuration is very common with Windows and Linux servers as opposed to dedicated network appliances. However, even with network appliances, they often perform several functions. For example, a Cisco ISR may function as a router, call manager, time server, and authentication device.

Redundancy is provided through the use of multiple serving servers or devices. Redundancy configuration can either be based on varied configurations throughout the environment (that is, different clients point to different servers) or some form of clustering or round-robin solution. A round-robin solution will sit between the requesting clients and the servers and direct some clients to one server and other clients to another. Whatever the method used, some form of redundancy is essential for many services. WLAN controllers are often configured with redundancy for this reason.

Going back to the NTP service as an example, Windows Server 2012 can act as a time server (though this is a little known fact even to long-time Windows administrators). To enable this you must first ensure that the Windows Time service is set to Automatic as shown in Figure 7.23.

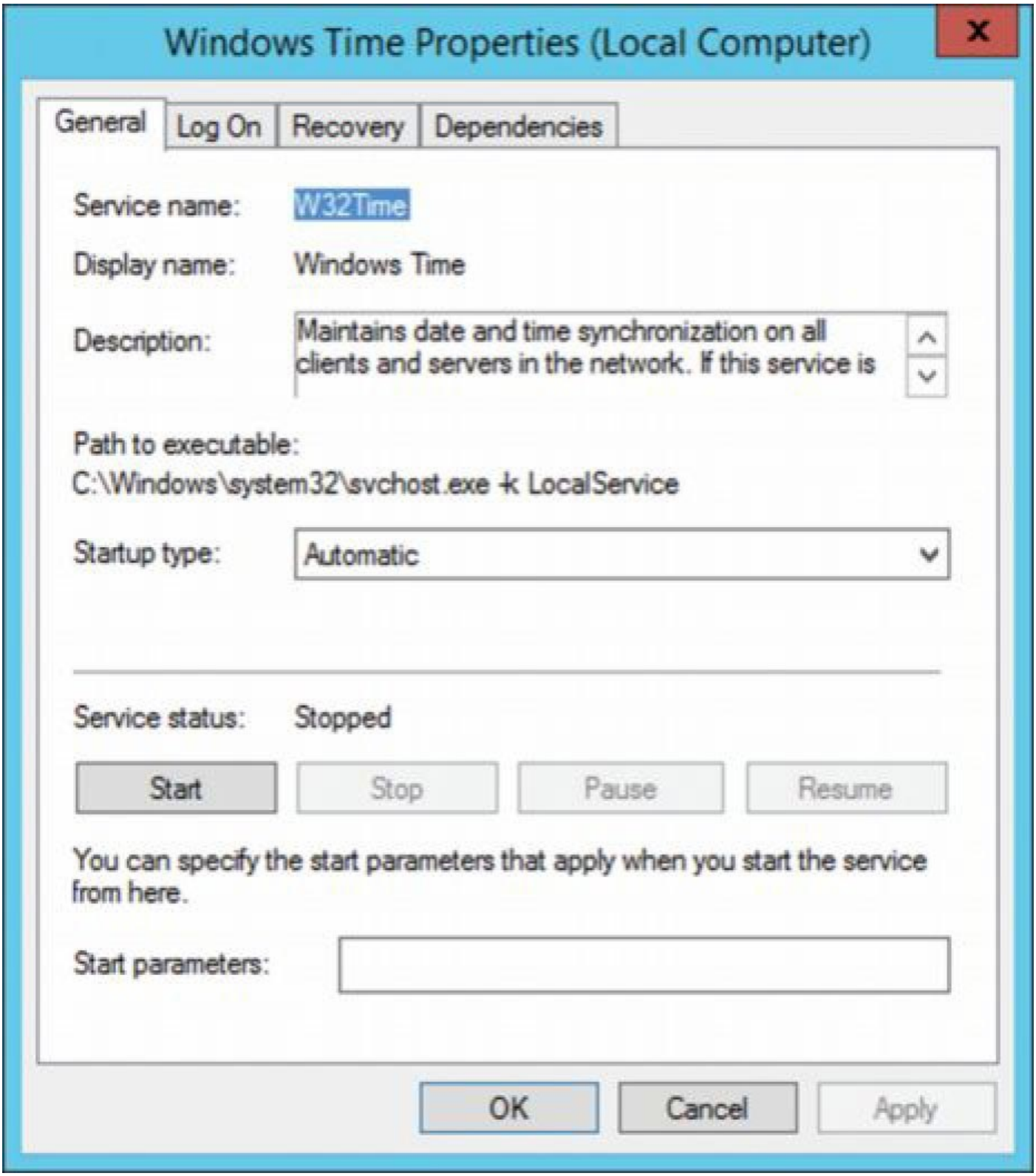


Figure 7.23: Windows Time Service Configuration

With the Windows Time service configure, you must then modify a registry entry located at:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32T
```

The actual entry is named `ENABLED`, and it should be set to the value of `1`. With these changes, the Windows Server will now respond to time synchronization requests from NTP clients. Of course, the Windows Server itself should get its time from some other source such as pool.ntp.org.

The point of this information is to show that a typical server can act in many roles. This particular Windows server may also be a domain controller, a RADIUS server, a DNS server, a DHCP server, and more. As you place more and more services on the server, performance is degraded. Using Windows tools like the Resource Monitor (shown in Figure 7.24) and the Performance Monitor, you can often track down the processes consuming the most resources. Believe it or not, a WLAN analyst is often tasked with this work as well, particularly in small- and medium-sized businesses.

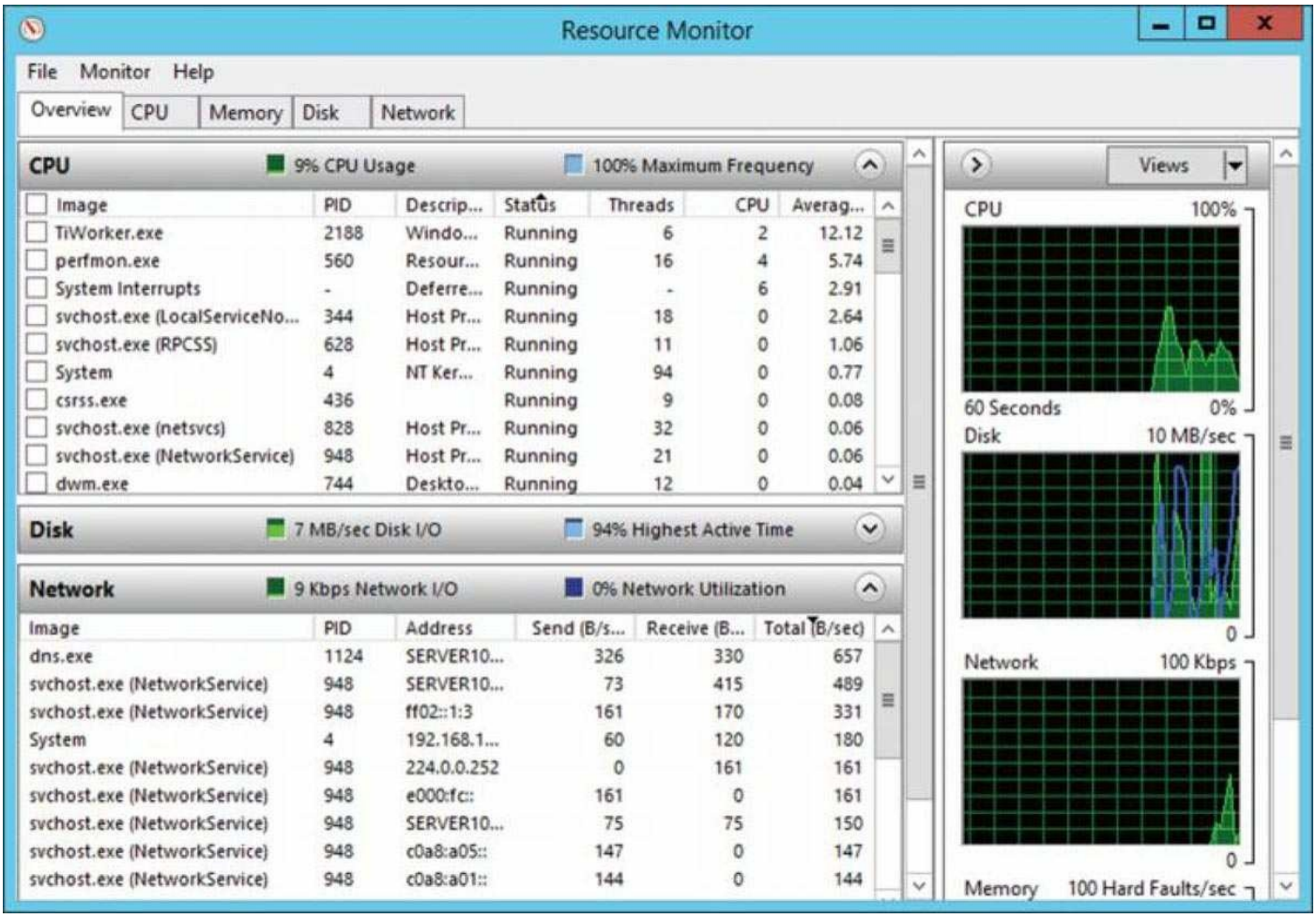


Figure 7.24: Windows Server Resource Monitor

Internet Connectivity

For guest WLAN clients the primary reason they connect to the network is usually Internet access. They often want to check e-mail, use web sites or access corporate portals across the Internet. For internal WLAN clients, Internet connectivity has become critical to many job roles. For this reason, it is important to understand the common causes of Internet connectivity problems, particularly when local resources are available, but the Internet is not.

First, many operating systems now differentiate between local access and Internet access, and they inform you when Internet access is not available. For example, Figure 7.25 shows the Windows 8.1 View Available Networks (VAN) interface with a status code of *Limited*, which typically means that the Physical and Data Link layers are working fine, but a problem exists somewhere above, typically at Layer 3, preventing Internet connectivity. Users, however, are not aware of this and will often simply report that, “the wireless network is down.” The problem is not with the wireless network but with some

service or configuration that provides Internet access.

When troubleshooting Internet access, always begin with the scale of the problem. If it is a single user, the problem is likely on that user's device or at least within the local segment to which the user is connected. If it involves many users and all other network functions are working as expected, the problem is likely with the Internet gateway (either the router or the service provider's network).

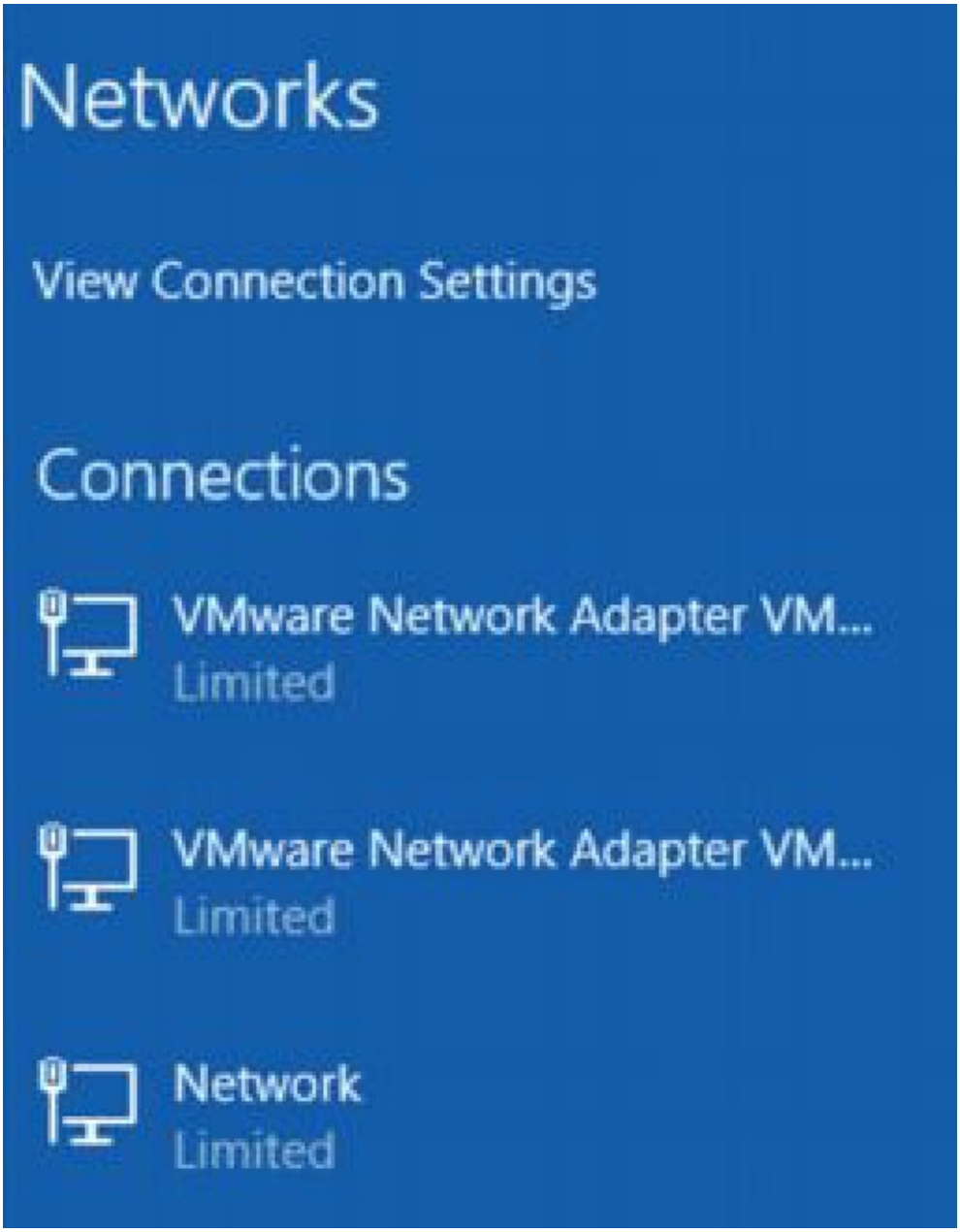


Figure 7.25: Windows 8.1 VAN

To troubleshoot Internet connectivity, consider the following points of failure:

- **Client configuration:** ensure that the IP configuration is accurate including the DNS server and default gateway and any required Internet proxy configuration settings.
- **Infrastructure:** ensure that all switches and routers along the path to the Internet gateway are configured and operating as designed.
- **Internet gateway:** ensure that the connection to the service provider is still operational and that the configuration is correct.

- **DNS:** ensure that the DNS server, if local, is configured to forward requests to a valid Internet server. Small- and medium-sized businesses often point to the Google public DNS servers at 8.8.8.8 and 8.8.4.4.
- **Captive portal:** ensure that the captive portal is responsive and configured properly. Additionally, clients often get confused over captive portals based on cached information. At times, clearing the cache (DNS and browser) may be required to reactivate the portal logon screen.

To clear the DNS cache and reset the IP stack, you can use the following two commands on Windows 8 and later:

```
IPCONFIG /FLUSHDNS
NETSH INTERFACE IPV4 RESET
```

The commands must be executed as an administrator. A reboot is suggested after resetting the IP stack. An additional command, `NETSH WINSOCK RESET`, may also be used in extreme cases.

Home Offices

The final area of troubleshooting we will explore is home offices. Telecommuters are becoming far more common today, and it is often the responsibility of the network group to support these users. The range of options for installing and managing home offices is large, and it is important to standardize on equipment and protocols if the organization will be responsible for managing and troubleshooting these networks. Four primary options exist for enabling a remote home office of enterprise employees and contractors:

- **Use of personal equipment without VPN:** The home workers use their own equipment and typically access HTTPS-based corporate sites or public cloud sites like Google drive and Microsoft Office 365.
- **Use of personal equipment with VPN:** The home workers use their own equipment and connect using a VPN client to the corporate network. Once connected, they use corporate resources as normal.
- **Use of enterprise equipment without VPN:** Like personal equipment, but the router/AP and laptop are provided by the corporation.
- **Use of enterprise equipment with VPN:** Like personal equipment, but the VPN solution may be a router-to-router VPN instead of using a VPN client solution on the computer.

As you can image, the first two options are the most difficult to support. In most cases the organization does not support hardware or software owned by the users—at least not officially. In the real world, support staff often find themselves helping the users even with their personal equipment and software.

The latter two options are easier to support as the equipment is owned and remotely managed by the organization. In this scenario remote administration of the router/AP is typically performed within a VPN tunnel and the computer(s) is supported using remote desktop solutions like Virtual Network Computing (VNC), TeamViewer, or Windows Remote Desktop.

In these scenarios, standard support processes will be used. Operating system commands and, when available, protocol analyzers and spectrum analyzers can be used. Initial installation of enterprise equipment may involve an onsite configuration. This option allows the installer to properly analyze the environment and select the best channels and configurations for the 2.4 GHz and 5 GHz radios in the remote APs.

When supporting remote office workers, consider the following best practices:

- Secure the wireless network using WPA2-Personal with a strong passphrase.
- Implement the wireless network on the best channel possible, and use 5 GHz equipment when possible.
- Use VPN solutions to encrypt all traffic between the remote network and the enterprise office.
- When using HTTP applications, ensure that HTTPS is used.

Exercise 7

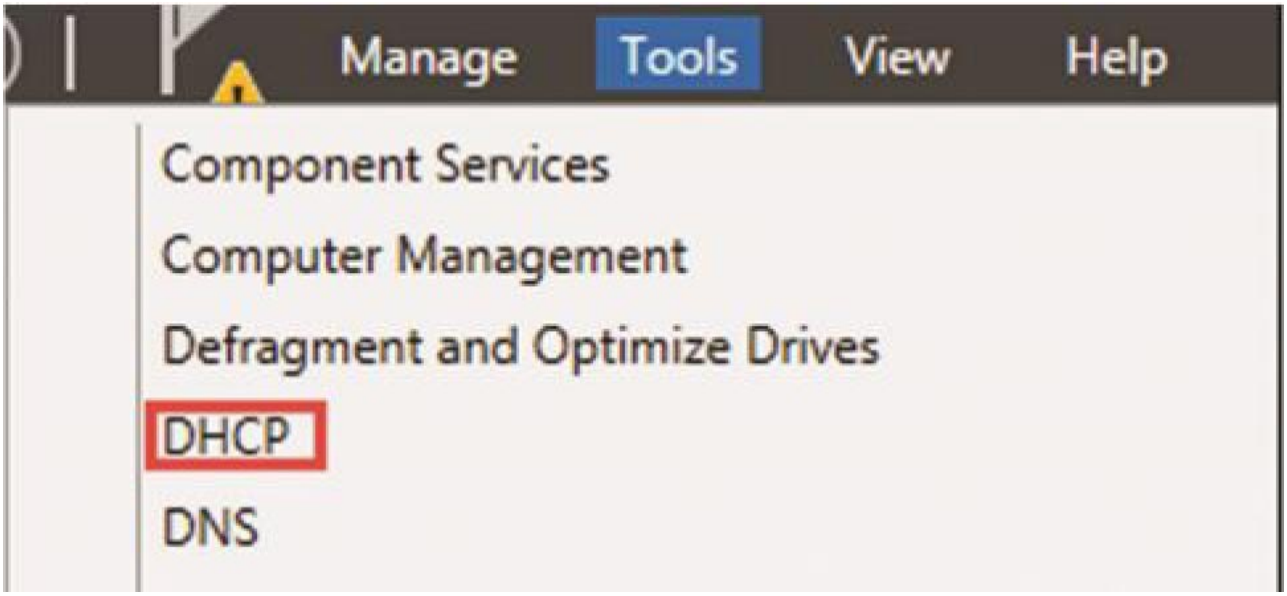
In this exercise, you will configure the DHCP server to support a Cisco lightweight AP. This involves creating the vendor class identifier (VCI) or option 60 from the client and option 43 to provide the IP address of the WLAN controller. This example uses the DHCP server service in Windows Server 2012 R2. If you do not have such a server to perform the exercise, you can view a video demonstration on YouTube by searching for "CWNPTV Configuring DHCP for the WLAN APs".

Note: **This exercise assumes the DHCP service is already installed and a scope has been created for the target segment.**

1. Log onto the Windows Server as an administrative user.
2. If Server Manager does not load automatically, load it by clicking the Server Manager icon on the Quick Launch bar.

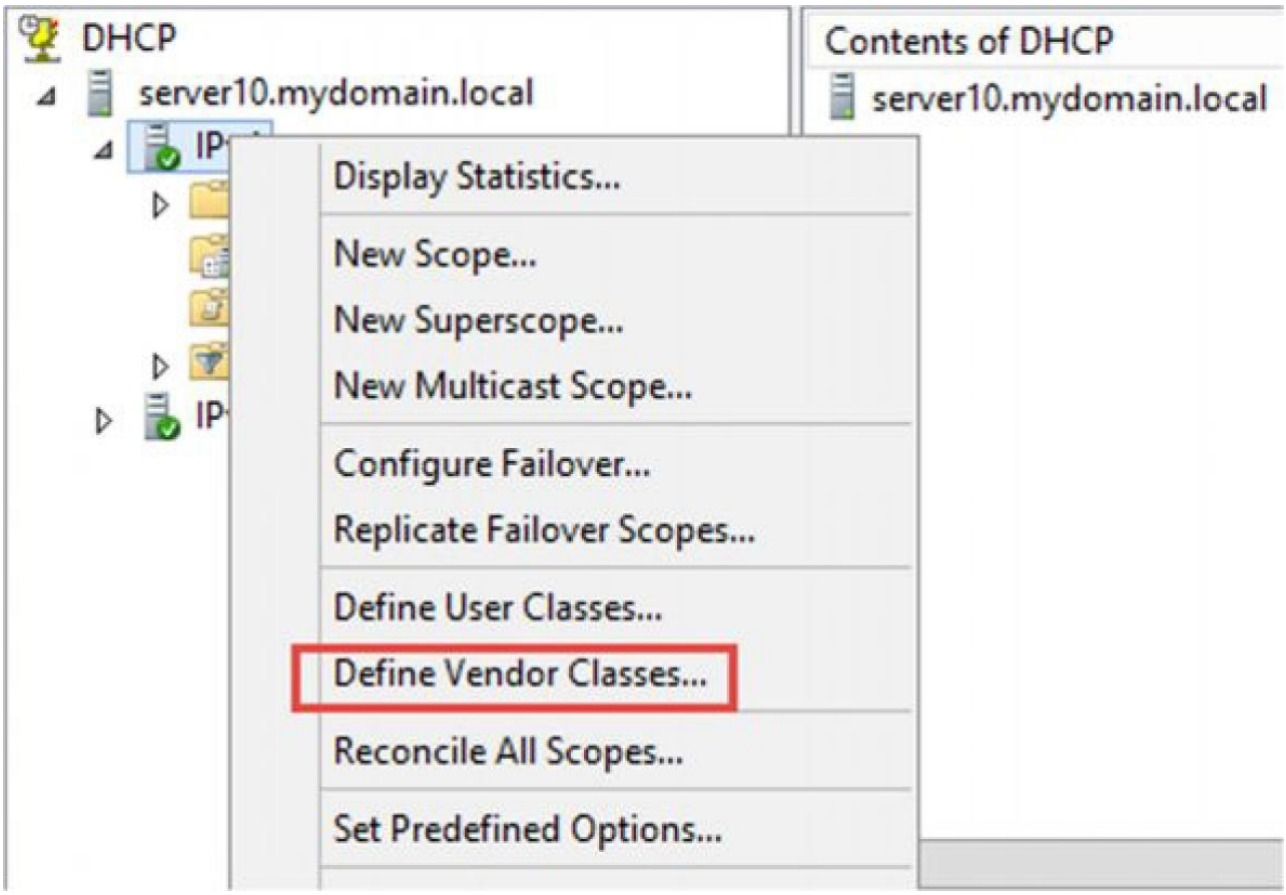
Graphic 7.1

3. In Server Manager click tools and select DHCP.



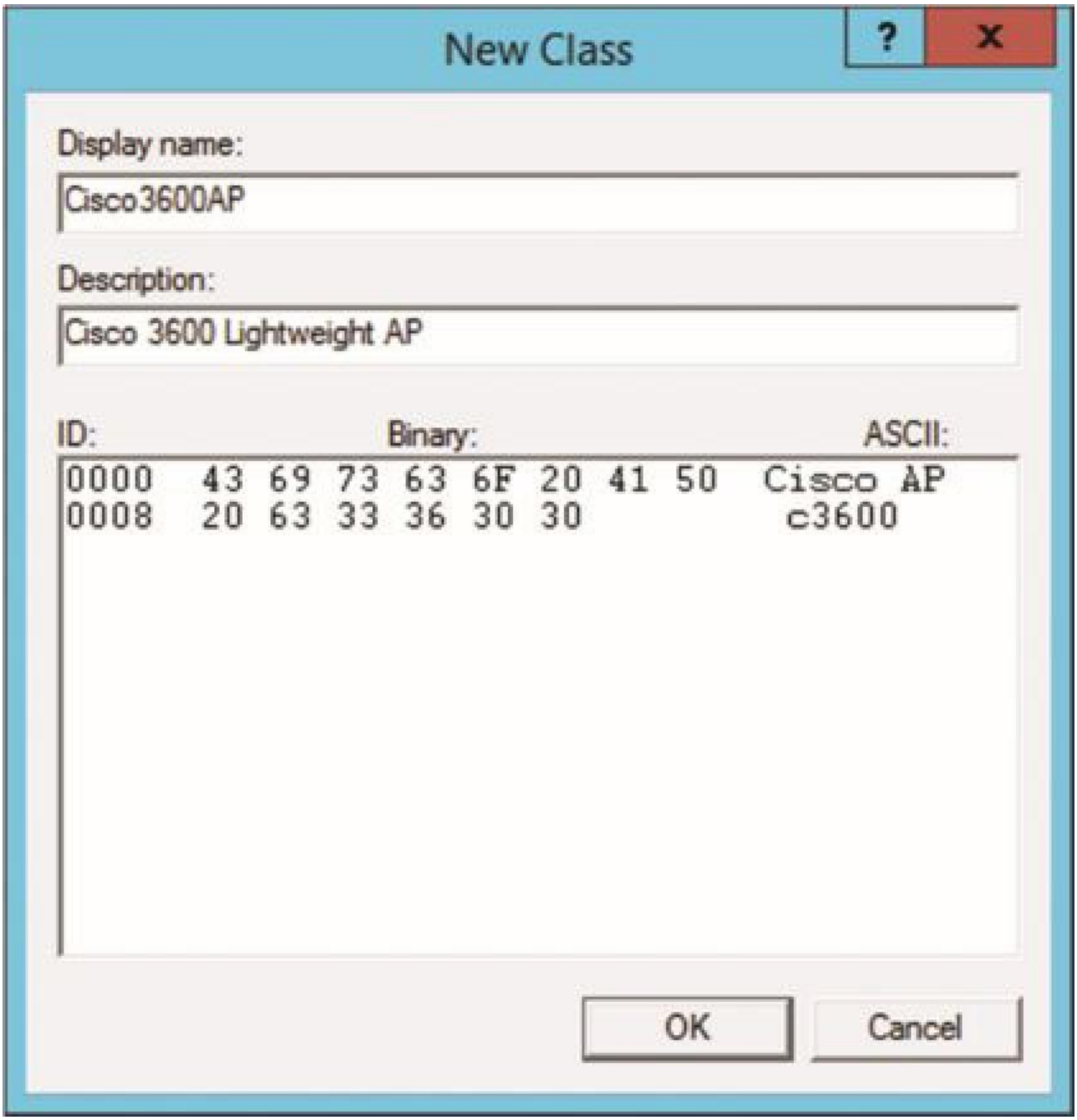
Graphic 7.2

4. Expand the appropriate domain and the IPv4 node in the left navigation panel.
5. Right-click on the IPv4 node and select Define Vendor Classes.



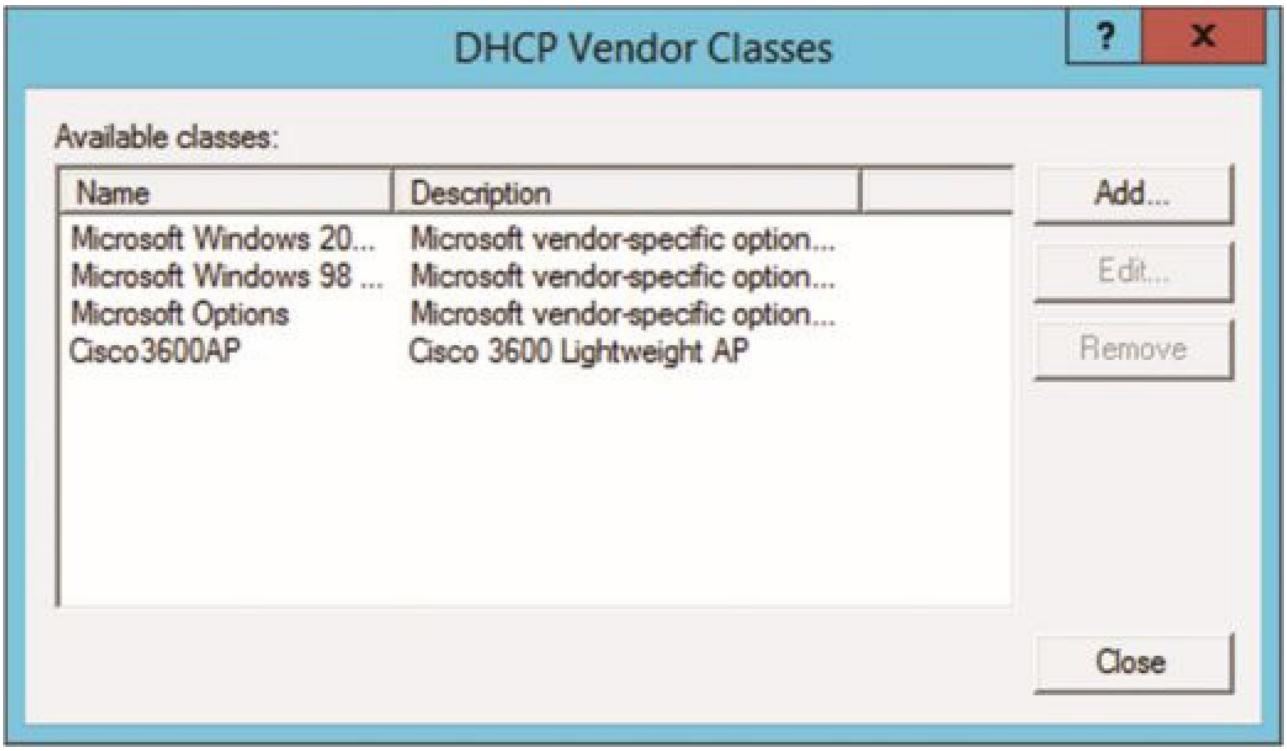
Graphic 7.3

6. Click Add to add a new vendor class.
7. In the New Class dialog enter a meaningful class name and description. Then enter the code “Cisco AP c3600” in the ASCII portion of the dialog as shown in the following graphic.



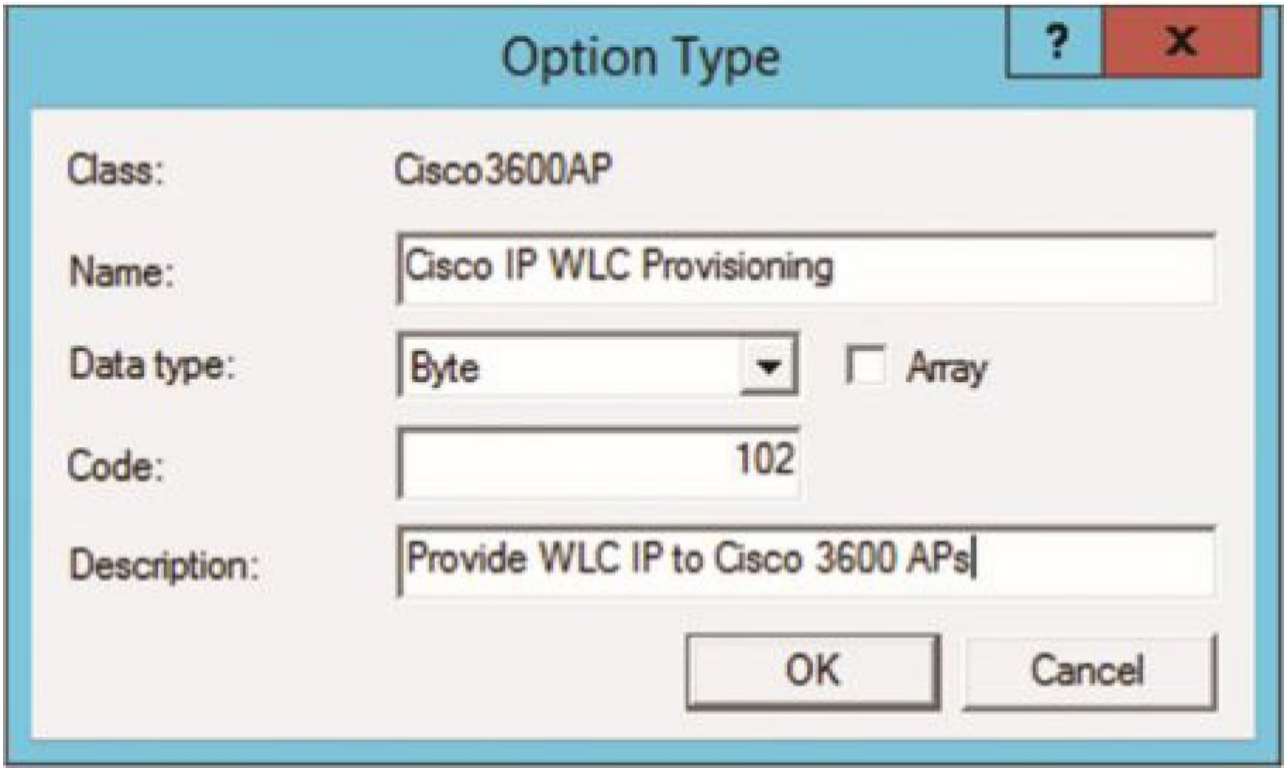
Graphic 7.4

8. Click OK to save the new VCI.
9. Click Close to close the DHCP Vendor Classes dialog.



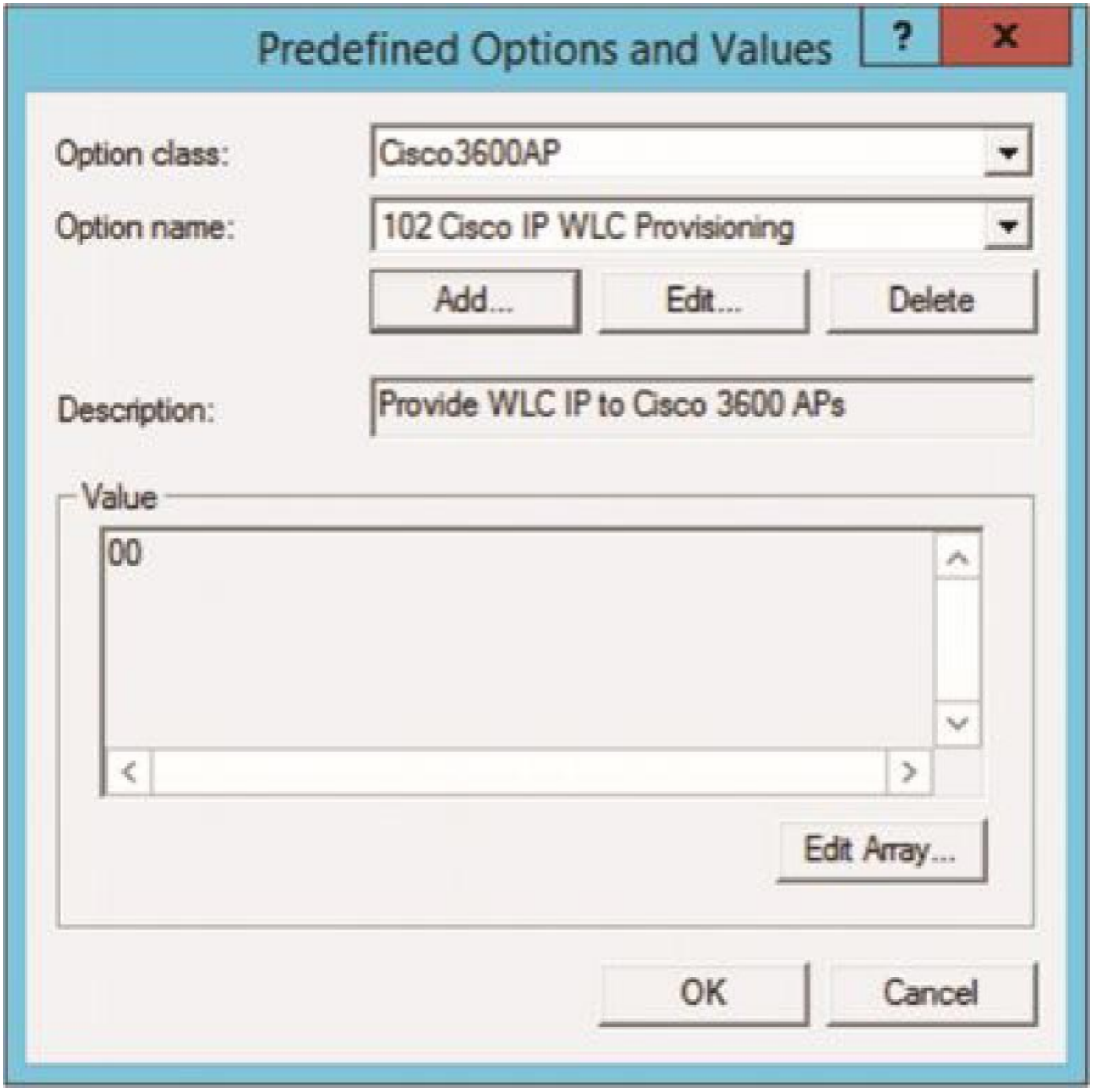
Graphic 7.5

10. Right-click the IPv4 node and select Set Predefined Options.
11. In the Predefined Options and Values dialog, select the new Cisco3600AP VCI you just created and then click Add.
12. In the Option Type dialog, enter a meaningful name and description. Set the Data Type value to Binary and the Code value to 102 as in the following graphic.



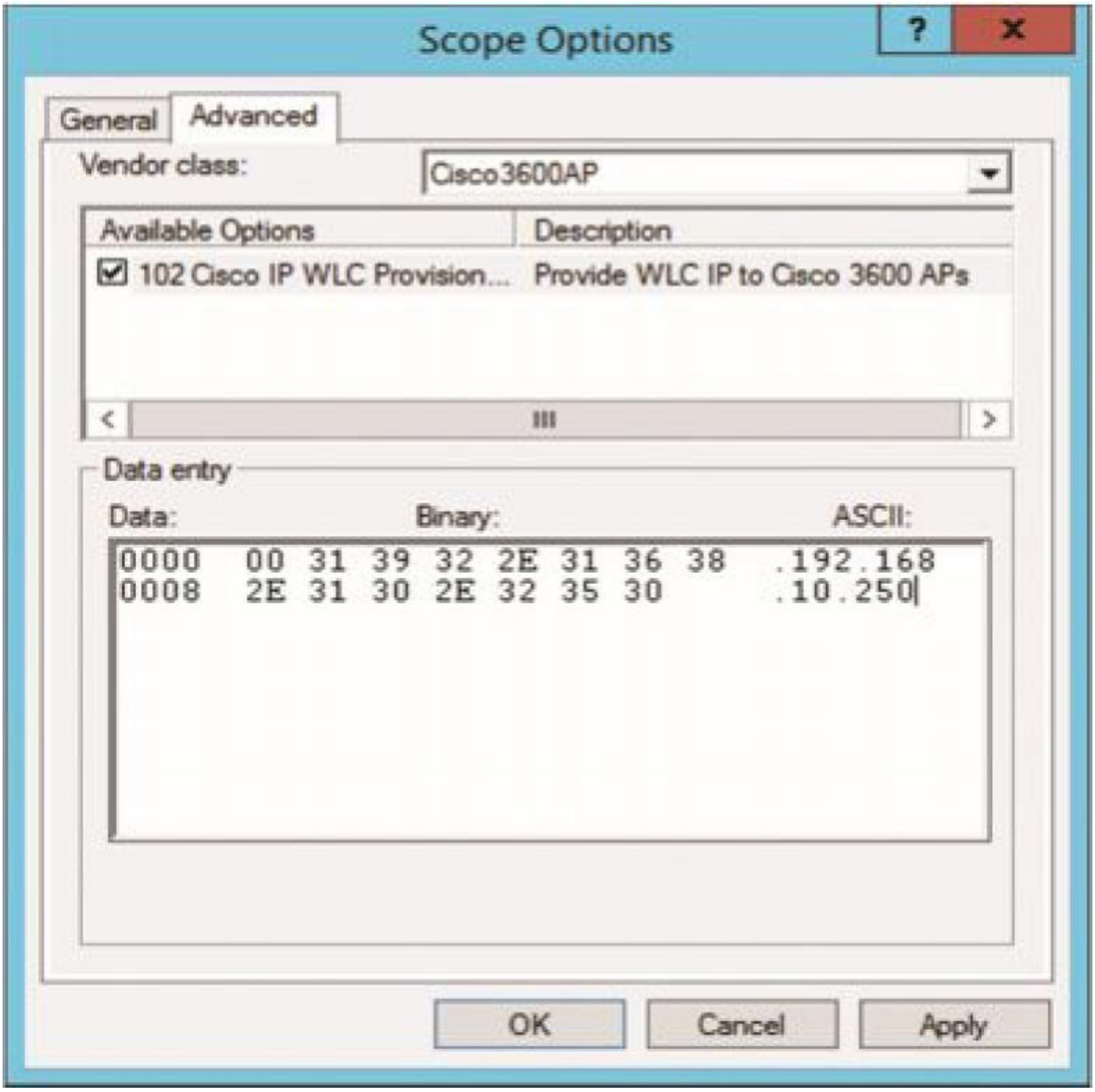
Graphic 7.6

13. Click OK to save the option type.
14. Click OK to save the cisco3600AP Option Class configuration.



Graphic 7.7

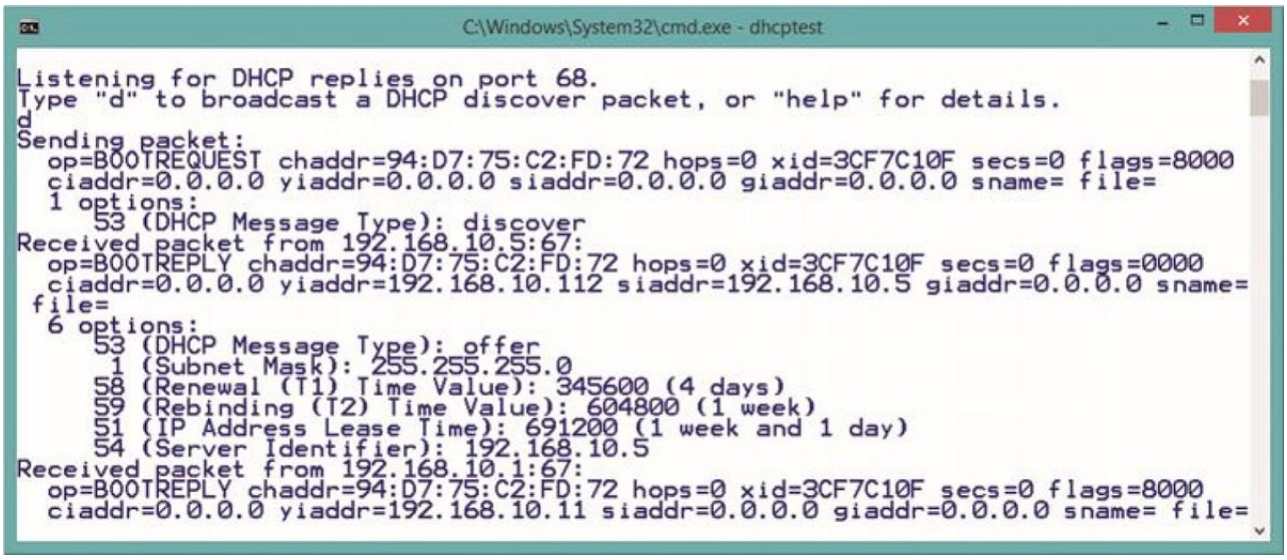
15. Expand the scope in the navigation pane.
16. Right-click the Scope Options node and select Configure Options.
17. Select the Advanced tab.
18. In the Vendor Class drop-down menu, choose the Cisco3600AP option (assuming you used that name).
19. In the ASCII portion of the dialog, simply type in the IP address of the WLC as shown in the following graphic.



Graphic 7.8

20. Click OK to save the changes.
21. Use a tool like DHCPTEST.EXE to verify proper operation of the option 43 configuration. You should not see option 43 unless you have transmitted a DHCP discover message with the proper option 60.

Note: **If you have only single model APs in the segments served by the DHCP server and no other option 43 devices, you can simply configure DHCP option 43 directly. However, realize that option 43 will then be sent to all requesting clients and not simply APs. Graphic 7.9 shows the DHCP request from a standard laptop against the previous configuration in steps 1-21. Notice the lack of an option 43 from the DHCP server at 192.168.10.5.**



Graphic 7.9

Chapter Summary

In this chapter you learned about the importance of wired-side operations to proper WLAN function. You explored important services like DHCP and DNS, and hardware such as routers and switches. In the next chapter you will focus specifically on WLAN issues that are caused by Layer 1 and Layer 2 concerns in 802.11 operations.

Review Questions

1. Which one of the following is an important WLAN function that often requires DNS operations?
    a. PHY operations
    b. 802.11 framing
    c. WLC location
    d. Autonomous AP configuration
2. What DHCP option is used by the client to request WLC IP information?
    a. 43
    b. 102
    c. 60
    d. 54
3. What DHCP option is used to provide WLC IP information to APs?
    a. 43
    b. 60
    c. 54
    d. 80
4. DHCP is an enhancement of what earlier IP provisioning protocol?
    a. CAPWAP
    b. LWAPP
    c. BOOTP
    d. 802.1p
5. What is the most common configuration used for lightweight APs in relation to switch ports?
    a. Trunk mode
    b. Access mode
    c. Spanning
    d. 802.1X
6. Which one of the following is not a method used by APs to locate a controller on the network?
    a. Broadcast
    b. DHCP

c. WINS

d. Cached information

7. What operating system command is used specifically to troubleshoot and analyze DNS configurations and problems?

   a. PING

   b. TRACEROUTE

   c. NSLOOKUP

   d. PATHPING

8. What operating system command may be used to determine the various nodes along the path between two endpoints?

   a. PING

   b. TRACEROUTE

   c. NSLOOKUP

   d. NETSH

9. For what is a tool like the LinkSprinter 300 used?

   a. To look for WLAN interference

   b. To detect CCI on the WLAN

   c. To test a cable and services available on the connection

   d. To determine jitter levels in the network

10. What kind of DNS record is created so that APs can locate a WLC?

    a. An A record

    b. SOA record

    c. NS record

    d. 45 LP

11. When in shell mode with NSLOOKUP, what command is used to specify the use of a DNS server located at 10.10.12.17?

    a. DNS 10.10.12.17

    b. SERVER 10.10.12.17

    c. 10.10.12.17

    d. QUERY 10.10.12.17

12. How does an AP know the domain name to append to the host name that is hard coded in the AP for DNS resolution of the WLC IP address?

    a. DHCP provides the domain name.

b. The domain name is guessed based on logical algorithms.

c. The AP captures DNS requests from other devices on the network and uses that information to establish the domain name.

d. All APs must use the domain name of my domain.local.

13. You have captured DNS query packets to evaluate the ability of APs to locate the WLC through DNS. You notice that the APs are receiving a DNS response with a response code of 3. What does this indicate?

    a. An error-free respond from the DNS server.

    b. The DNS server does not contain the host name required.

    c. The DNS server does not support encrypted communications.

    d. The AP requested the right domain name but did not provide the login credentials.

14. In what scenario would DHCP servers often not respond with a DHCPnak when a client requests an IP configuration but the pool is depleted?

    a. When it is not coded correctly.

    b. When the client indicates that it does not support DHCPnak messages.

    c. When a secondary pool is configured as a backup in the same segment.

    d. When the DHCP server detects that another DHCP server has made an offer.

15. What tactic can often be used to reduce DHCP pool depletion problems?

    a. Use only IPv6.

    b. Shorten the lease duration.

    c. Use only IPv4.

    d. Lengthen the lease duration.

16. In addition to looking for DHCPnak messages and simply not receiving an IP configuration, where can you look to see if DHCP pool depletion is a problem?

    a. Server logs

    b. Client logs

    c. Windows registry on the client

    d. Windows registry on the server

17. When broadcasts are used to locate the WLC, where should the APs be located in relation to the WLC?

    a. In the same broadcast domain

    b. In the same building

    c. On the same switch

d. Within three router hops

18. When is it not required to create a VCI in the DHCP server to service APs on the local segment?

    a. When BOOTP is used instead of DHCP.

    b. When option 60 has been deprecated in the APs.

    c. When one model of AP is used and no other option 43 devices are on the network.

    d. When IPv6 is used instead of option 43.

19. What filter is used in Wireshark to show only DHCP communications?

    a. DHCP

    b. BOOTP

    c. IPv4.DHCP

    d. IP.DHCP

20. In addition to setting the appropriate VLAN and switch port mode settings, what other item should be configured on all switch ports where APs are connected?

    a. IPSec

    b. 802.1X

    c. QoS trust

    d. NTP

21. What UDP ports are used by CAPWAP?

    a. 5246 and 5247

    b. 12222 and 12223

    c. 1812 and 1813

    d. 546 and 547

22. What maximum power level in watts can be provided by a PSE supporting only 802.3af?

    a. 30 watts

    b. 15.4 watts

    c. 12.95 watts

    d. 110 watts

23. When the best effort model is used, how is VoIP traffic treated?

    a. With a higher priority than email, but lower priority than control traffic

    b. With a higher priority than all other traffic

c. With a lower priority than control traffic, but a higher priority than video traffic

d. The same as all other traffic

24. What QoS solution is used at Layer 3 of the OSI Model?

a. CoS

b. 802.1Q

c. 802.1p

d. DSCP

25. To what CoS value does the CS5 class selector from DSCP map?

a. 2

b. 3

c. 5

d. 7

Review Question Answers

1. **C** is correct. Wireless LAN Controller (WLC) location often depends on DNS. A host record is created in the DNS server and is resolved by APs to locate the controller.
2. **C** is correct. While option 43 is used to return the vendor-specific information (WLC IP address for example), it is not used to query for the information. Clients will use option 60 to specify the vendor class identifier (VCI) to the DHCP server.
3. **A** is correct. Option 43 is used to provide the IP address to APs. This is a generic vendor-specific information option and can be used in a single scope to provide multiple items based on option 60 requests from the clients.
4. **C** is correct. BOOTP was used to provide IP addresses based on MAC address mappings and did not provide a dynamically allocated pool like DHCP does.
5. **B** is correct. Lightweight APs use standard access port modes in most cases (with some vendor exceptions) and establish a CAPWAP tunnel with the WLC.
6. **C** is correct. WINS is not used by any new technologies being developed today. Thankfully!
7. **C** is correct. NSLOOKUP (or DIG on Linux) is used to query DNS servers. It is useful in testing for the existence of needed host records for WLC IP address resolution by lightweight APs on the network.
8. **B** is correct. TRACEROUTE and/or PATHPING can be used to identify the nodes along the path between two endpoints. The TRACEROUTE command in Windows systems is actually TRACERT and not TRACEROUTE when executed.
9. **C** is correct. The LinkSprinter 300 is an example of a cable or line tester tool. When connected to an Ethernet cable and enabled for Wi-Fi access, you can connect to it with a laptop or mobile device and then view information about PoE, DHCP, and DNS name resolution abilities.
10. **A** is correct. An A record is created (also called a host entry or host record) in the DNS server for APs to use in the location process when discovering a WLC.
11. **B** is correct. The SERVER *ip address* command is used to indicate to NSLOOKUP that a DNS server other than that configured on the interface should be used for queries.
12. **A** is correct. The AP should receive the domain name in the DHCP offer from the DHCP discover, offer, request, and acknowledge process. Client stations, such as laptops and desktops, can be manually configured with a DNS suffix (domain name), but APs are not typically pre-staged in this way.
13. **B** is correct. When a response code of 3 is seen in a DNS query answer it indicates that the requested host name is not configured in the DNS lookup tables.
14. **D** is correct. Frequently, if a DHCP server detects that another DHCP server has provided an offer to the requesting client that send the DHCP discover message, it

will not send a DHCPnak even though the pool may be depleted. When no such detection occurs, the server should respond with a DHCPnak.

15. **B** is correct. In WLANs many stations come and go. As a result, the IP pool may be quickly depleted if the lease duration is too long. By shortening the lease duration, you can often reduce DHCP pool depletion issues.
16. **A** is correct. The server logs may contain errors indicating that DHCP requests have been made, but the server scope has no remaining IP addresses (the definition of DHCP pool depletion).
17. **A** is correct. To use broadcasts to locate the WLC, the WLC should be in the same broadcast domain as the APs. This domain may span switches by using VLANs, so existing on the same switch is not required.
18. **C** is correct. If one model of AP is used on the segment and no other non-AP devices exist on the segment requiring option 43 for configuration, the use of a VCI is not required, nor will option 60 elements be used by the DHCP server to service DHCP requests.
19. **B** is correct. No DHCP filter exists in Wireshark. Instead, the BOOTP filter is used for both DHCP and BOOTP traffic.
20. **C** is correct. By establishing QoS trust with the AP connected to the port you ensure that the switch will accept the QoS tags coming from the AP. The AP converts 802.11 QoS tags to 802.1p CoS values before sending the data on the wired side of the network. Alternatively, the controller performs this function when centralized forwarding is used.
21. **A** is correct. CAPWAP uses UDP ports 5246 and 5247. LWAPP uses UDP ports 12222 and 12223. RADIUS uses UDP ports 1812 and 1813 and DHCP uses UDP ports 546 and 547.
22. **B** is correct. PSEs supporting only 802.3af have an output power of 15.4 watts and a PD received power expectation of 12.95 watts. PSEs supporting 802.31t have an output power of 30 watts and a PDF received power expectation of 25.5 watts.
23. **D** is correct. In the best effort model no traffic prioritization is used on the network. In this model VoIP traffic is treated the same as all other traffic.
24. **D** is correct. At Layer 3 (Network Layer) Differentiated Services Code Point (DSCP) is used on all newer equipment. Older existing equipment may still use the type of service (ToS) values in the IP header instead of DSCP.
25. **C** is correct. Class specifiers in DSCP are easy to map to CoS as they usually map to the same number. For example, CS1 maps to CoS 1 and CS5 maps to CoS 5.

Chapter 8:

Common WLAN Issues

Objectives

8.1 Recognize and repair common WLAN issues including insufficient capacity, lack of connectivity, interference and QoS problems.

8.2 Diagnose and repair roaming problems including dropped VoIP calls, broken connections and lack of reconnect.

8.3 Understand and repair issues related to WLAN security including authentication, encryption and mobile device management (MDM).

8.4 Recognize and repair common client-side problems including unstable drivers, configuration errors, incompatible supplicants and operating system bugs and vulnerabilities.

It would be nice if we could implement our WLANs and then never experience problems with them. The real world is not so kind. We must understand WLAN problems and how to troubleshoot and repair them as wireless professionals. This chapter wraps up the contents of this book by discussing common issues related to WLANs, as well as specific areas of concern such as roaming, security and QoS.

Common Issues

Believe it or not, wireless communications that use RF waves have now been used for more than 100 years. From radio communications to WLANs, similar problems have been encountered along the way when trouble arises. However, WLANs introduce some new dilemmas that are not faced at the same level in radio communications such as CB and ham radio. For example, data throughput is not a real issue for these hobbyists who love to talk with people around the globe. For them, they can just turn up the power (within legal limits), buy a new antenna, and extend their operational range. There might be a little "fuzz" on the link when conditions aren't perfect, but the human ear and mind is amazingly adept at processing out the "fuzz" and retrieving the human speech.

WLAN radios are not as tolerant of interference and free space path loss-imposed attenuation. For this reason throughput or capacity management is an important part of the WLAN administrator's regular job. Additionally, scenarios exist where the administrator must determine the cause of weakened signals and find a solution. Should more APs be installed on different channels? Is RRM making output power too weak (or too strong)? Can the administrator move an AP or antenna a few feet and greatly impact the coverage area? Is the weather causing problems for the outdoor links? These questions and more will be answered in this section as we investigate the following common issues in WLANs:

- Insufficient Capacity
- Co-channel and Adjacent Channel Interference
- RF Noise and Noise Floor
- RF Interference
- Multipath
- Hidden Node
- Near-Far Problem
- Weather
- Troubleshooting voice over WLAN Issues

Insufficient Capacity

Installing a WLAN that provides access to users is only a partial solution. The access provided must be sufficient for the users' needs. This usually means providing adequate

throughput or capacity for the network clients to use the applications they require. One might suggest that there is a difference between throughput and capacity. Capacity is a linkage between throughput and the number of users that require a certain throughput in a cell. That is, as more users join the cell, at some point overall throughput is diminished. Management of capacity is simultaneous management of both overall throughput and controlling the number of stations communicating in a channel. Many different factors can affect the available throughput in a WLAN including the chosen PHY, wired-side limitations, and more. This section will introduce you to the topics you'll need to understand in order to provide your users with the capacity they need to get their jobs done efficiently.

PHY Limitations

The first choice that will impact the available throughput is the PHY or PHYs you decide to implement. There are obvious issues like the data rates supported by VHT, HT, OFDM, and ERP as compared to HR/DSSS, but there are also not-so-obvious issues like protection mechanisms.

When an AP implements the HT PHY, and an OFDM STA associates with that AP, the AP will usually implement a protection mechanism that reduces the overall throughput of the WLAN. This is because transfers that use the HT modulation must first set the NAV in all non-HT STAs that are associated with the AP or operating within range of the channel. This is done by transmitting RTS and/or CTS frames with a duration that is greater than or equal to the time needed to transmit the actual HT-modulated frame and responses. The extra overhead reduces the throughput of an HT BSS drastically and should be considered when implementing your WLAN. You can often more than double the total throughput in a BSS by ensuring that only HT-based or VHT clients are allowed to connect to any WLAN in the vicinity. Of course, in multi-tenant facilities, this will not be in your control.

Furthermore, you can force the AP to reject associations below a particular data rate so that even visiting client STAs (those that are out of your control) will not impact your BSS on an ongoing basis. As an example, in tests performed by CNet Labs (reviewed April 17, 2003 by Brian Nadel), a Buffalo AirStation WLAN router provided 19.6 Mbps of throughput in an ERP-only configuration, but this dropped to 7.9 Mbps in a mixed mode implementation with both ERP and HR/DSSS PHY-based clients (see reviews.cnet.com for more information.). The point of this older, but still relevant study is that protection mechanisms greatly reduce channel capacity. These protection mechanisms cannot always be avoided.

You must also consider the range of the PHY you select. Generally speaking, a 2.4 GHz-based BSS will have a greater range with higher data rates at a greater distance than 5 GHz-based BSSs of the same power. This is due to a limitation in antenna design that makes it less feasible to "capture" the same signal "amount" at the same distance in 5 GHz as in 2.4 GHz. However, range is not often the most important element in design in today's indoor WLANs, but rather capacity is the priority. In these modern designs installing more APs and then managing CCI (discussed more later) is of key importance.

Wired-side Limitations

You must ensure that the wired ports on your APs and WLAN routers are fast enough to

keep up with the WLAN. This includes the Ethernet port that is in the AP or wireless router and the switch port that the AP or router connects to. If the interface is a 100 Mbps port, it will not be able to keep up with the demands of the 802.11n or ac WLAN, assuming the users communicate more with devices and services on the wired LAN than they do with each other.

In most cases, you will want a minimum of a 1 Gbps port for connections to the APs and a 1 or 10 Gbps port for the uplink connection from the switch to the rest of the network. For example, you may choose to connect five APs to a switch and have an average of fifteen users associate with each AP. If the switch provides only a 1 Gbps uplink to a 1 Gbps infrastructure, the uplink port in the switch will act as a potential bottleneck that downgrades the average maximum throughput for your 5 APs. Having a 10 Gbps uplink can resolve this issue.

Note: **While this book and the CWAP exam are focused on WLANs, it is important to remember that the experience of your WLAN users will be greatly impacted by the performance of your wired LAN, as well. Some administrators make the mistake of assuming that the WLAN will be so much slower than the wired LAN that they will not have to focus on the wired side at all. This is a dangerous assumption and is the reason for Chapter 7's contents.**

Co-Channel and Adjacent-Channel Interference

One factor that can reduce throughput is co-channel or overlapping channel interference, which are really the same type of interference. It occurs when one BSS uses the same channel as another BSS that overlaps, or partly overlaps, the same coverage area. In other words, more than one WLAN or BSS is attempting to co-exist in the same coverage area on the same channel.

This concept of co-channel interference is related to system throughput in a very practical way. You can improve system throughput by co-locating APs in an area strategically configured for non-overlapping channels. For example, you can use channels 1, 6, and 11, which are often referred to as non-overlapping or adjacent channels—though they would be better referenced as less-overlapping since there is still some level of overlap. In fact, if an AP is on channel 1 and another is on channel 6 in the same area, and they both use very high output power settings, they can have a detrimental effect on each other. This would be known as non-overlapping adjacent channel interference. When channels specified as non-overlapping adjacent (2.4 GHz specify 1, 6 and 11) interfere with each other because they are too close to each other or are using output power levels that are too high, it is called adjacent channel interference (ACI), or more specifically non-overlapping ACI.

To resolve this issue, when overlapping coverage areas with co-located devices, make sure the output power is not higher than is needed. This will reduce adjacent interference.

Overlapping adjacent channel interference, for example, using channels 1 and 2, cannot really be overcome by using lower output power settings—assuming the two APs are in the same coverage area. To resolve this type of interference, you will need to remove one of the APs or change the channel so that there is more separation in frequencies. If only two APs need to be placed in a coverage area to provide the needed throughput and there are no other nearby WLAN cells, you can usually get the best results by simply setting the APs to channels 1 and 11.

ACI may be identified by large numbers of frame retransmissions. High-retry rates (above 10%) can result in significant throughput loss.

To determine if you are transmitting with too much power from an AP, use a protocol analyzer to capture frames on a channel that is 3–4 channels off from the AP and see how many frames you capture. For example, if the AP is transmitting on channel 11, capture on channels 6, 7, or 8 and see how many, if any, frames you capture from the AP. (Beacon frames do just fine.) Figure 8.1 shows a capture on channel 7 that picked up the Beacon frame from the AP on channel 11.

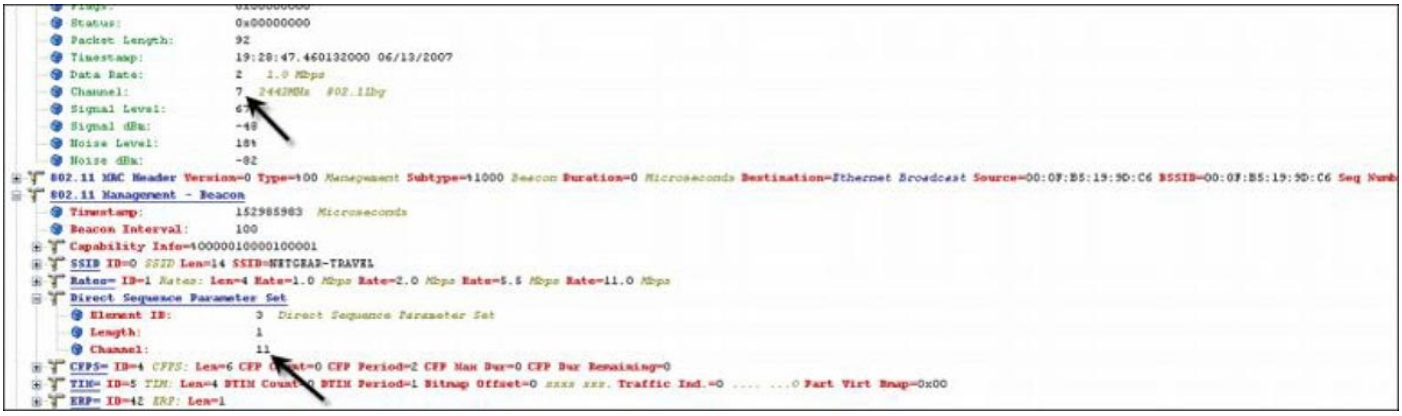


Figure 8.1: High-Output Power resulting in Co-channel Interference

With CCI, throughput is often reduced because the STAs in a BSS will accept and process duration values of received transmissions from other nearby BSSs that are on the same channel. The STAs will also process power measurements and treat the channel as busy if they detect RF energy above a specified threshold in the PHY. This results in a reduction in throughput since the STAs think the network is busy, and they do not try to transmit their waiting frames.

A key method used to reduce the impact of CCI is to reduce the number of control and management frames as much as possible. Many WLAN administrators do not consider the impact of beacon frames, but with the modern method of deploying multiple SSIDs on each AP radio, the beacon frames can add up to significant overhead.

An excellent IOS app is available that illustrates beacon frame overhead. The app is called SSID Calc and is available for free download from the Apple App Store. Figures 8.2 through 8.5 show the impact of beacon frames on CCI. Notice that we begin with 29% overhead and reduce it to only 1.83% overhead by simply disabling lower data rates and limiting the APs to 2 SSIDs instead of the starting point of 3 SSIDs.

CCI cannot be completely avoided in 2.4 GHz, so you have to live with it; however, the following suggestions can help to reduce it:

- Limit the number of SSIDs per AP radio to 2 as much as possible.
- Find the right balance between the number of APs using a channel and the total capacity of that channel within your space. This is usually from 2–3 APs maximum on a channel at a particular client measurement location.
- Disable lower data rates so that frames that are sent at the lowest data rate are sent faster.
- Stop purchasing 2.4 GHz-only client devices.

The last suggestion is important. The 5 GHz band has many more channels, and it is far easier to implement cells that have only 1–3 APs visible on the channel at a given client location. By moving as many users as possible to the 5 GHz band, you help to reduce CCI in 2.4 GHz and do not greatly impact CCI in 5 GHz in most deployments.

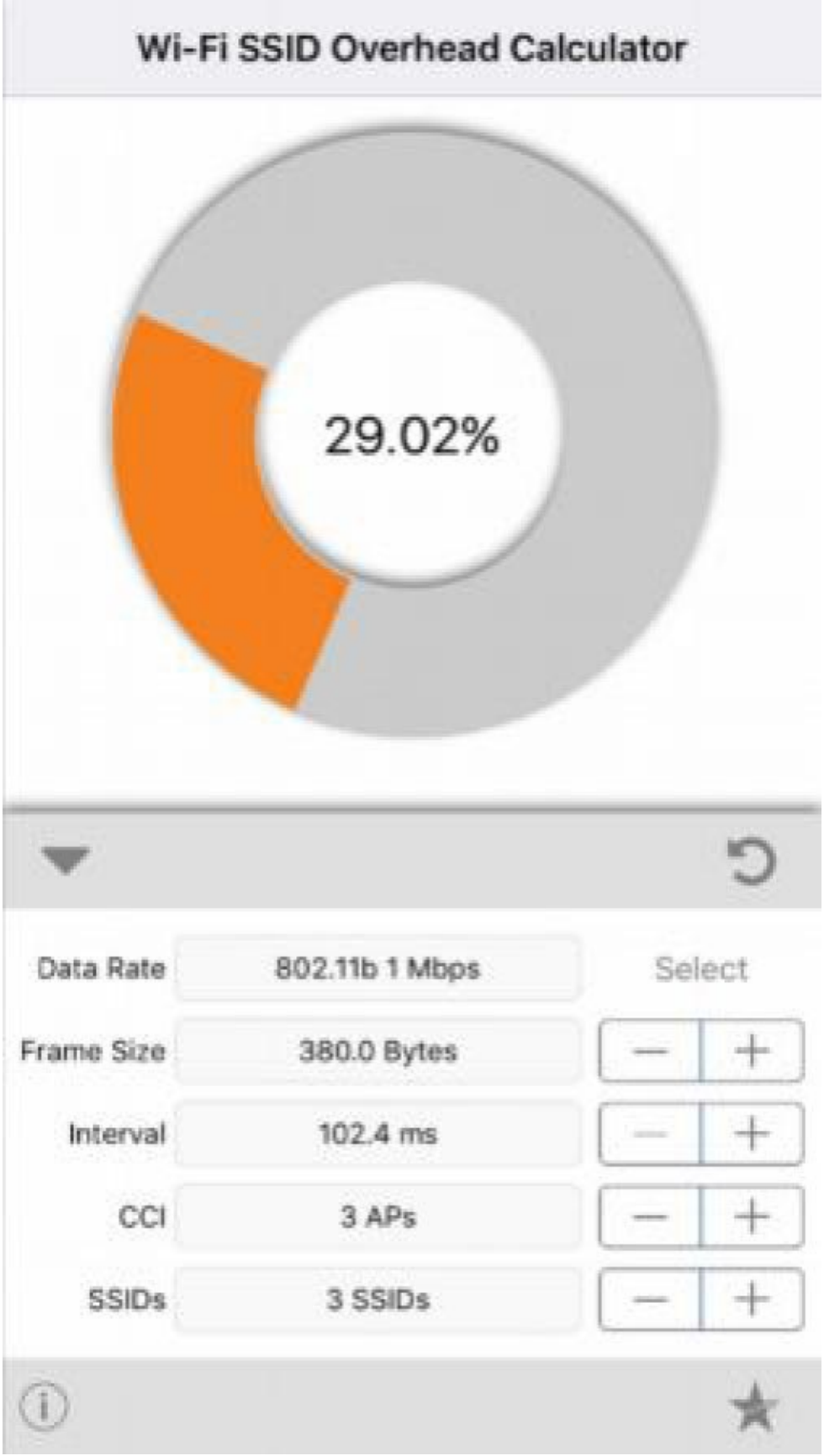


Figure 8.2: SSID Calc with three APs in a Channel and three SSIDs and a Data Rate of 1 Mbps for the Beacons

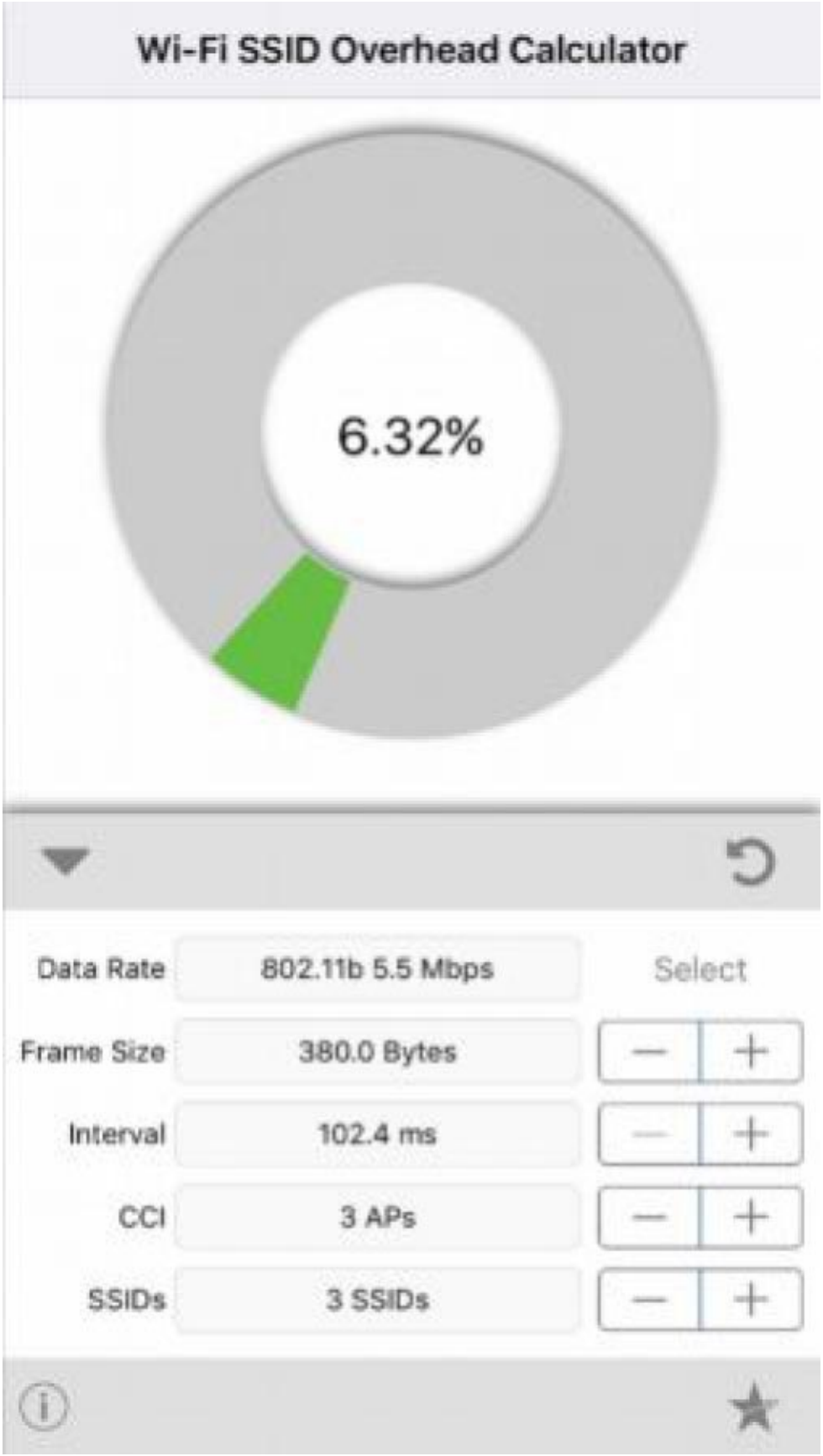


Figure 8.3: SSID Calc with the Data Rate Changed to 5.5 Mbps for the Beacons

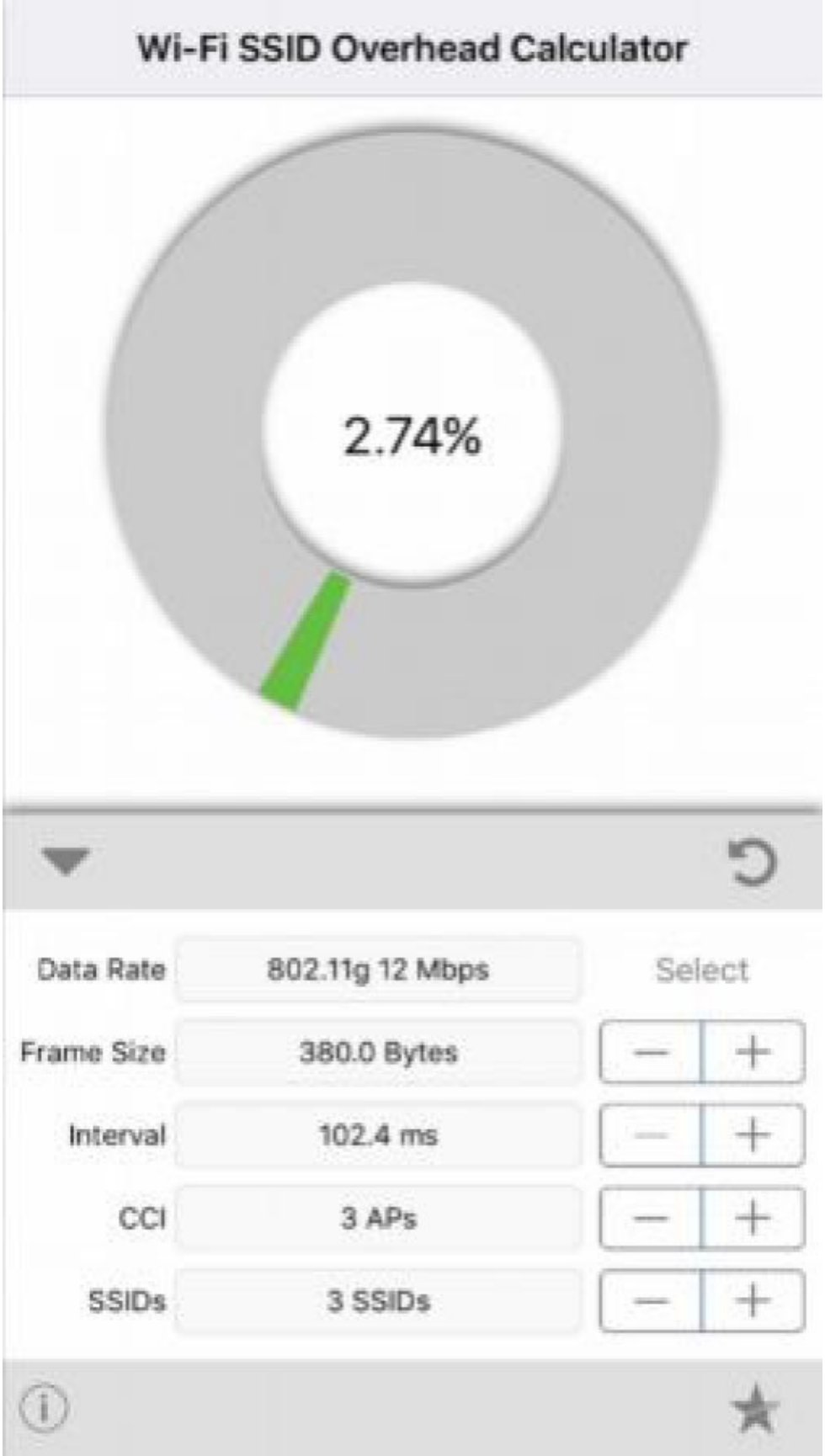


Figure 8.4: SSID Calc with the Data Rate Changed to 12 Mbps for the Beacons

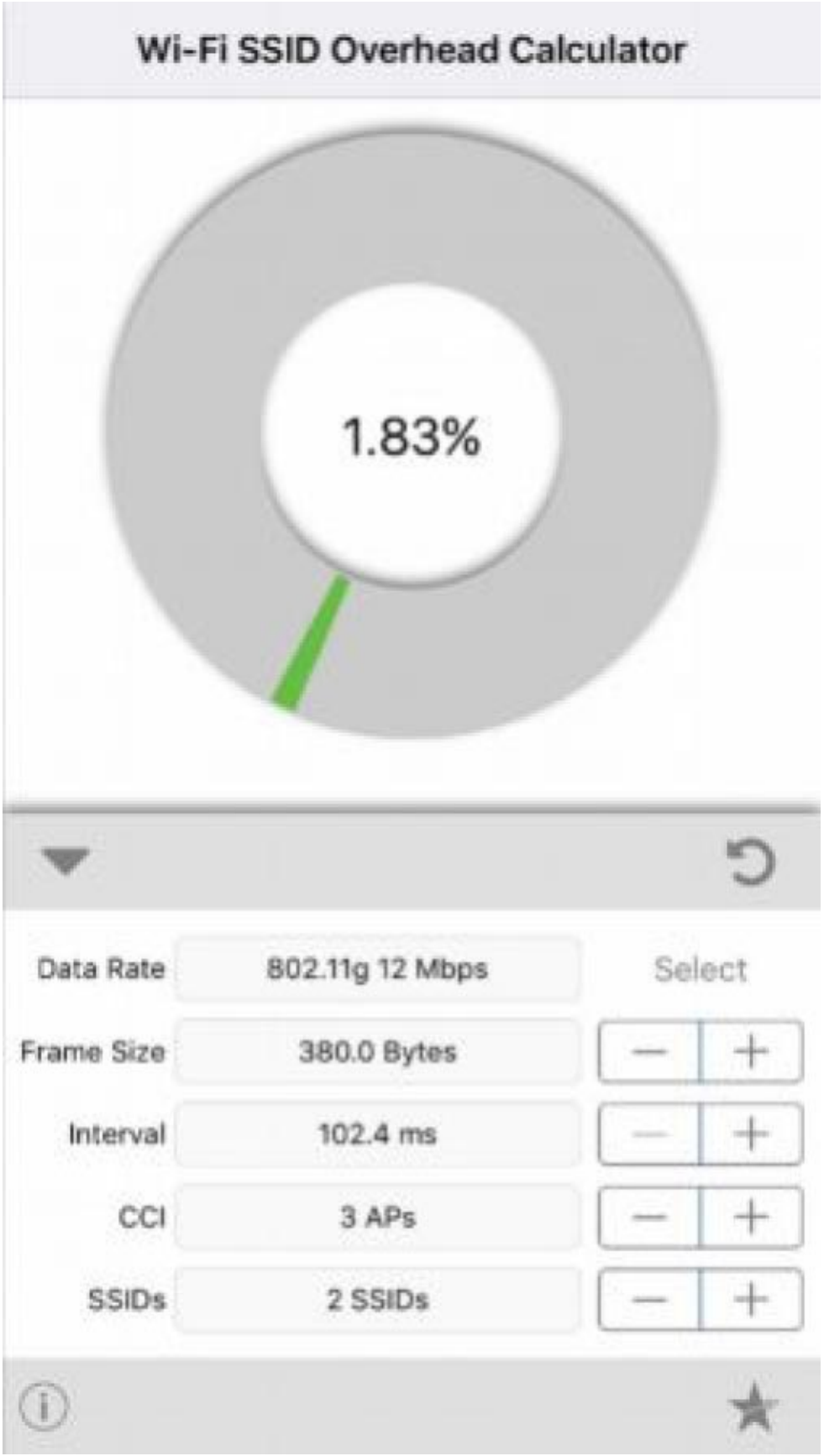


Figure 8.5: SSID Calc with the Number of SSIDs per AP Reduced to Two

When it comes to discovering potential CCI, you can use fancy protocol analyzers designed for WLAN analysis, but in many cases simple tools like Acrylic Wi-Fi Professional will do the job just fine. Figure 8.6 shows this tool revealing many APs on a single channel with signal strengths high enough to cause excessive CCI.

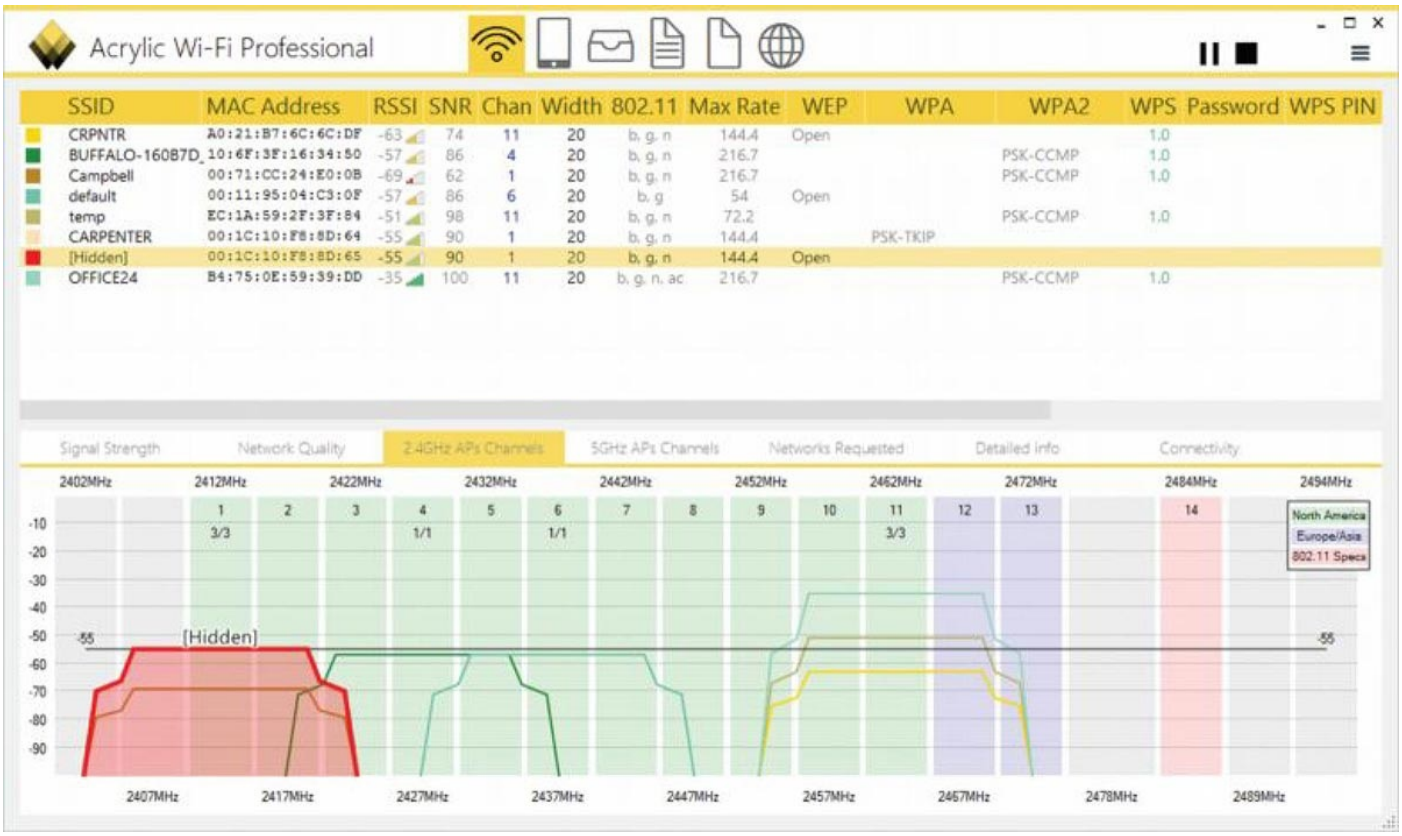


Figure 8.6: Acrylic Wi-Fi Professional Showing Potential CCI Problems

However, at times you want more detailed information. This deeper information will be provided by a dedicated WLAN protocol analyzer. Figure 8.7 shows OmniPeek revealing channel usage information.

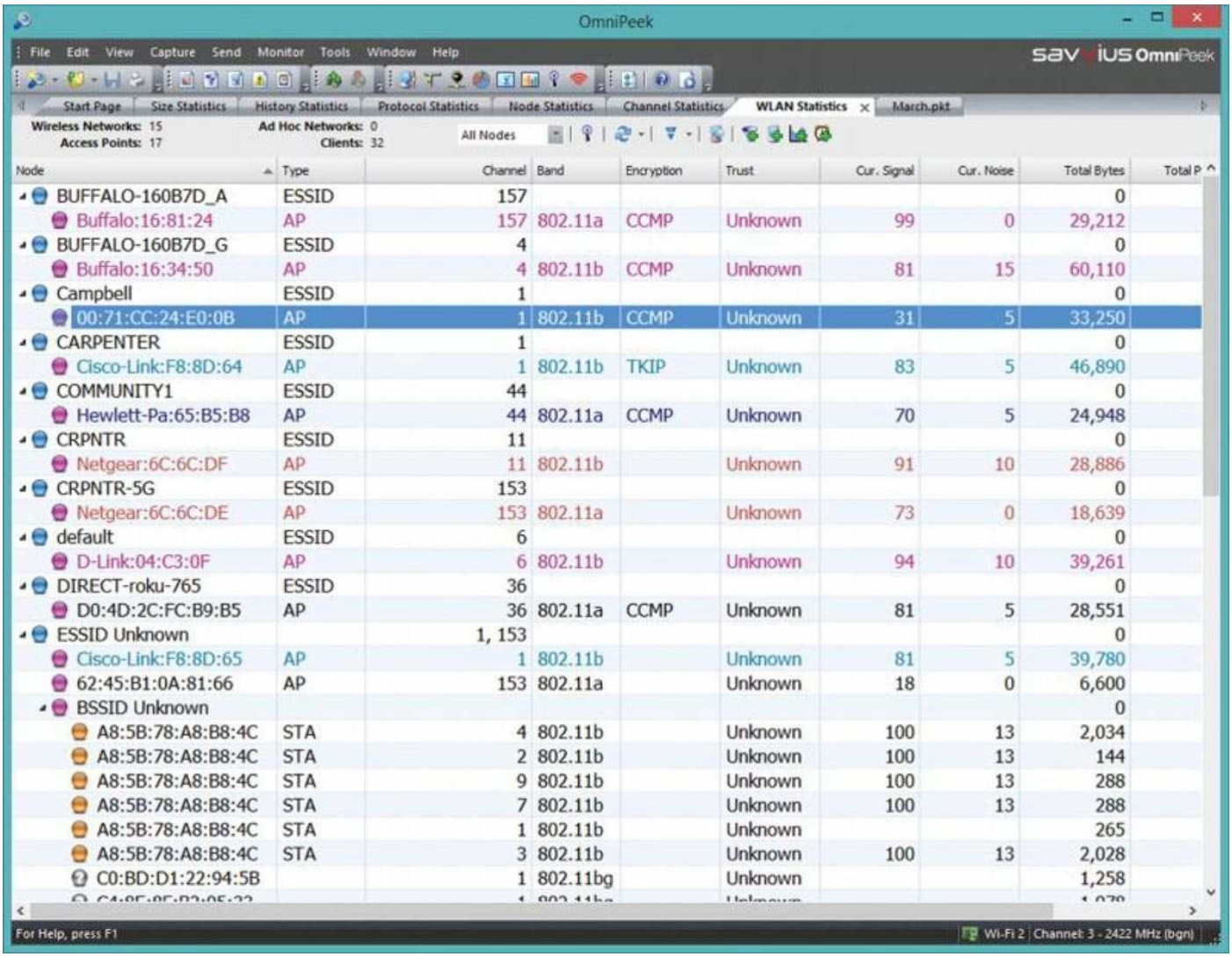


Figure 8.7: OmniPeek showing Channel Usage

Figure 8.8 Shows CommView for WiFi revealing channel usage. Notice several APs on channel 1. Utilization is not high on channel 1, so CCI is not likely to be a tremendous issue. However, this is a capture with few clients associated. Once more clients are associated and begin communicating, the utilization will go up, and then CCI will become more of an issue.

> **EXAM MOMENT:** In addition to the number of APs on a given channel, it is important to consider utilization. If several non-busy APs are on the same channel from the perspective of a client, but the utilization of most APs is very low, it will not have as much impact on the performance of the client.

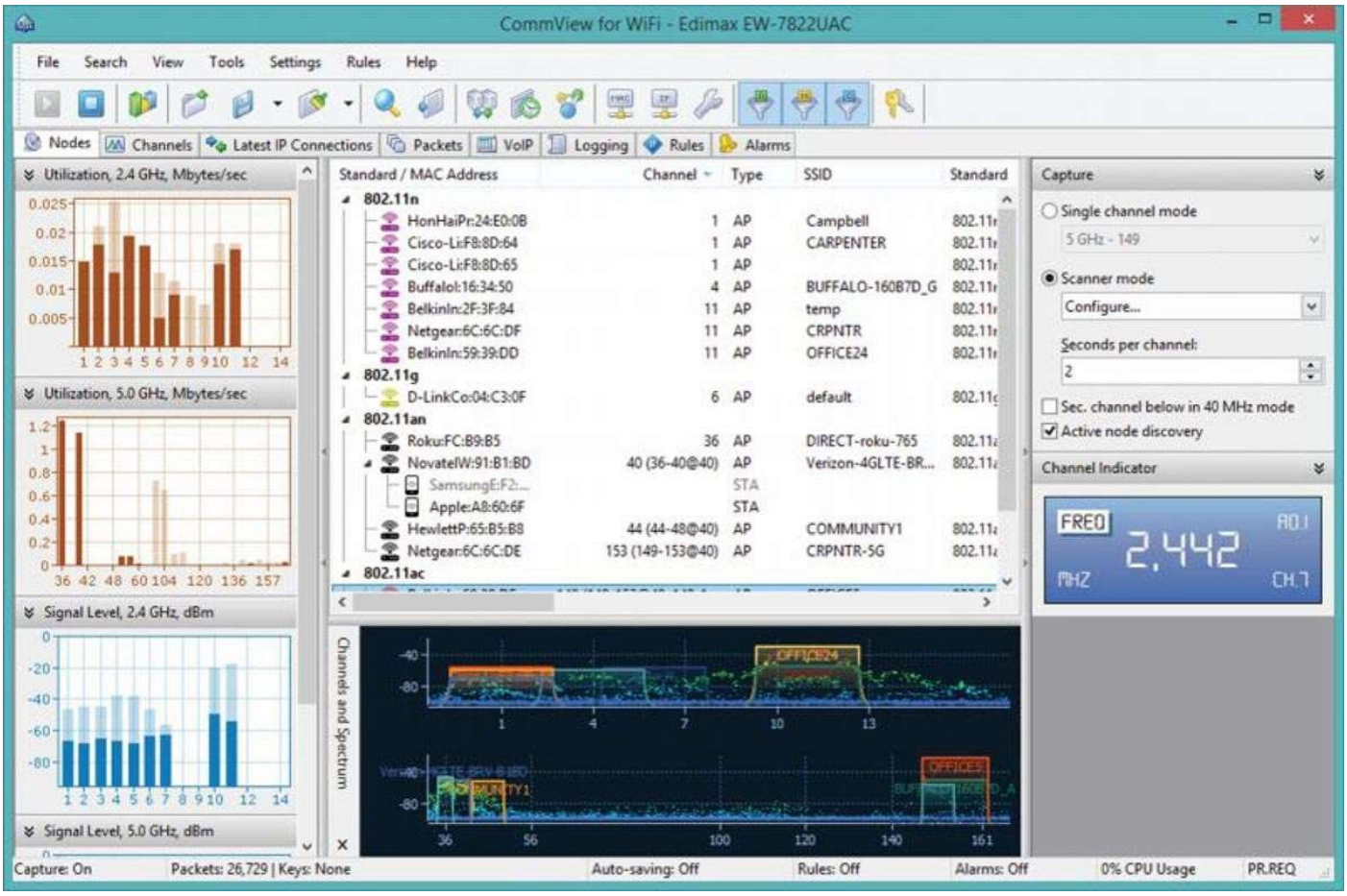


Figure 8.8: CommView for WiFi Showing Channel Usage

RF Noise and Noise Floor

RF noise may be defined as RF energy or signals generated by RF systems other than those systems with which the detecting system intends to communicate. For example, a WLAN STA configured to listen to an AP on channel 11 may consider RF signals transmitted from an AP on channel 9 at high power levels to be RF noise. This RF noise may cause corruption of frames. Interestingly, what is RF noise to one device may be the RF signal to another.

The noise floor is defined as the background level of RF noise, and the signal-to-noise ratio is the difference between the strength of the signal for which a device is monitoring and the strength of the noise floor.

RF Interference

Narrowband and wideband interference can cause corruption of data in WLANS. You can often detect that interference exists by looking at the frames in a WLAN analyzer, which may report CRC errors or corruption. When CRC errors are reported, it indicates that the signal strength was great enough to receive the RF signal, but that noise joined with the signal and corrupted the data as the signal arrived at the receiver. This results in retransmissions and, therefore, reduced throughput.

WLAN administrators can deal with these retransmissions in different ways. One way is to

reduce the data rate, which provides for more fault tolerance in the data transfer and the ability to handle more interference without losing data. Another way of dealing with the retransmissions is to fragment the WLAN frames. Smaller frames are transmitted faster, and fewer of the frames will become corrupted. The fragmentation threshold can be used to control the point at which fragmentation is utilized. A lower fragmentation threshold value should be tested when intermittent interference is suspected. If the problem is not resolved by lowering the threshold, you should immediately raise the threshold again.

If you determine that RF noise or interference is a problem in your environment, take these steps to diminish RF noise as much as possible:

- Remove or replace all RF devices that communicate on the same channels as the WLAN.
- Reduce the output power to the minimum possible to create acceptable links for all non-Wi-Fi devices.
- Replace leaky microwaves with better sealed units.
- Replace 2.4 GHz and 5 GHz phones with WLAN VoIP handsets.
- Strategically plan the channel selections in your environment to work around RF noise.

EXAM MOMENT: It is typically better to use an 802.11-based device than a non-Wi-Fi device that performs the same function. This is true because the 802.11 device will comply with contention rules, and the non-Wi-Fi device will not.

Multipath

Since WLANs have RF line of sight (LOS) instead of just visual LOS, the RF receivers can receive signals that travel directly from the transmitter to the receiver, as well as signals that reflect and diffract off or around other objects and then travel to the receiver simultaneously. Multipath is the term for signals travelling multiple paths and still arriving at the receiver. Multipath can be good for the communication link, and it can be bad for the communication. Some newer wireless technologies take advantage of multipath in order to increase the data rate and throughput of wireless communications. An example of this is the MIMO technology on which the HT and VHT PHY are based in the 802.11n and 802.11ac amendments. However, not all devices use these PHYs and some older devices may still be impacted by multipath problems.

<u>Results of Multipath</u>

As I stated, multipath can provide good and bad results. In most cases with older PHYs, the results are negative unless specific technologies are implemented to deal with them. The results include:

- Increased signal amplitude at the receiver
- Decreased signal amplitude at the receiver
- Data corruption

- Signal nullification

Increased signal amplitude at the receiver can result from multiple signal paths arriving at the receiving antenna in-phase. This is known as upfade. Of course, the signal is not stronger than when it was transmitted, and in fact will always be weaker than the originally transmitted signal. However, the signal may be stronger than it would have been at the point of reception had the upfading not occurred.

As you learned in you CWNA studies, free space path loss ensures that the received signal will be weaker than the transmitted signal. As the wave travels the wavefront broadens, and the signal strength at a given point will therefore be less.

Multipath may also cause signal reduction or a decrease in the signal amplitude. When this occurs, it is known as downfade, which should be considered during the selection of antennas at the time of the site survey. Downfade occurs when two copies of the same signal arrive at the receiver out-of-phase.

In addition, out-of-phase signals may also cause corruption of the main signal. This is because the amplitude of the received signal is reduced to such a point that the receiver can only understand part of the frame being transmitted and not the complete frame. This usually happens when the signal-to-noise ratio is very low. In other words, the RF signal is very close to the noise floor. This result of multipath usually causes a retransmission of the corrupted frame from the transmitter, and there may need to be multiple retransmissions before the frame actually makes it through.

The final result of multipath, nulling, occurs when one or more reflected waves arrive at the receiver out-of-phase with the main wave. In this case, instead of weakening the signal the main wave's amplitude is cancelled, and the signal cannot be received by the receiver. In these cases, retransmission of the frame will not likely resolve the problem unless the multipath occurred because of a moving vehicle in the area or something such as this. You may have to reposition one or both ends of the link.

Detecting Multipath

Since you cannot actually see waves as being in-phase or out-of-phase, you can only detect multipath by looking for its symptoms. These symptoms include links that should work based on standard link budget calculations that are experiencing problems, and dead spots in the RF coverage during a site survey or during the implementation of the WLAN. High retransmissions in links that should be working—based on link budgets and analysis of the RF noise floor when your transceivers are off—may also be an indication that multipath exists. Of course, remember, multipath is used to advantage in HT and VHT devices that support at least two spatial streams. Single spatial stream devices can still be negatively impacted by multipath. There are many such devices used today including tablets, mobile phones and even some laptops.

Solutions for Multipath

There are three main solutions to multipath. The first is to reposition objects, such as the receiving or transmitting antenna—or both—in order to remove the multipath (or to at least adjust it). The second is to use diversity antennas. APs and WLAN routers that have two antennas but are only ERP or OFDM PHYs (not HT PHYs) are usually diversity-

configured. This simply means that the radio will listen to one antenna and then the other at the beginning of a frame transmission, and will then receive the frame using the antenna with the best signal. Since multiple clients are being served, the AP may switch from one antenna to the other for nearly every frame, or it may use one antenna the majority of the time. There is usually no way to tell which antenna receives the most traffic.

The third solution to multipath is to use 802.11n or 802.11ac with two or more spatial streams. The 802.11n and 802.11ac devices strategically use multipath to increase the data rate and throughput of the wireless network. Since multiple antennas are used to communicate at the same time, throughput is improved over traditional simple antenna diversity.

Hidden Nodes

Hidden nodes are STAs that can be seen by the AP and that can see the AP, but they cannot see one or more other STAs and one or more other STAs cannot see the hidden nodes. Because of this scenario, the hidden nodes cannot hear at least one of the other clients communicating and so may attempt to communicate while the other nodes or nodes are active. Hidden nodes usually occur because of some large obstacle like a solid wall that’s between the STAs, or because of insufficient transmit power. For example, the AP may be placed on top of a thick block or brick wall, and clients that are lower and on either side of the wall can see the AP, but they cannot see each other.

The result of the hidden node paradigm will be collisions that cannot be avoided without the implementation of some function to clear the channel. This might include RTS/CTS.

A signature of the hidden node problem is increased corruption near the AP and increased retransmissions from the clients even though there is no increased corruption near the client. Using a protocol analyzer near the AP, you will notice frame corruptions. Using a protocol analyzer near the client STA, you will notice retransmissions approximately equal in percentage to the frame corruptions near the AP. The frames are being corrupted near the AP because that is where the signal from the one hidden node and the other hidden node “run into” each other. (Notice that both STAs are hidden nodes because they cannot see each other.)

Note: **The reverse of this description can also occur. For example, the corruptions may be happening at the client STA and not at the AP because another cell on the same channel is nearby that the AP cannot see. This is more often called a CCI problem today, but it is a form of the hidden node situation. The term hidden node, however, is typically constrained to two nodes of the same BSS that cannot see each other.**

It is important that you realize that there will almost always be hidden nodes in a WLAN (assuming it uses an omni-directional antenna and has client STAs on all sides), and that the existence of hidden nodes is not a problem in and of itself. When the hidden nodes

begin to cause too many retransmissions, it may become a performance issue on your WLAN. Use a protocol analyzer as mentioned in the preceding paragraphs to determine if 10–20 percent of the frames (from a particular client STA) are being retransmitted. If they are, you will likely need to perform one of the following steps to solve the problem:

- Use RTS/CTS
- Increase power output at the client STAs
- Remove obstacles
- Move the client STAs
- Ensure the APs and STAs transmit at the same power using IEEE 802.11h and Transmit Power Control (TPC)

Using RTS/CTS can help alleviate the overhead incurred from a bad hidden node scenario, but it should not be used as the automatic solution to a hidden node problem. Consider trying the other options first to see if they resolve your issue. If they do, they will not likely impact the WLAN's throughput as much as RTS/CTS would, and they may actually improve the throughput instead.

Increasing the output power at the nodes increases the likelihood that all or most nodes will be able to hear all or most other nodes. There are client adapters now that use power output levels as high as 300 mW which is higher than most indoor APs are capable of. Theoretically, if the AP is transmitting at 100 mW with a 7 dBi antenna, and your clients are transmitting at 300 mW with a similar or higher gain antenna, there should never be a situation where a client can hear the AP but not hear other clients. In the real world, it is not practical to think that you will use 300 mW of output power on every client, or that you will be able to use external antennas on every client. Additionally, due to absorption, reflection, refraction, diffraction, and scattering that occurs in WLANs, even with high output power, the scenario can certainly exist where two nodes cannot hear each other. Finally, using very high output power as a solution is likely to generate significant CCI for other cells using the same channel even if some distance away.

In these latter scenarios you may be able to move the nodes just a few feet or remove obstacles to resolve the hidden node problem. However, the reality is that regardless of what you do, in a WLAN with many nodes, there will most likely be hidden nodes. Your goal is to reduce the negative impact that these hidden nodes have on the overall throughput of your WLAN.

Near-Far Problem

The near-far problem is a result of a high powered STA closer to the AP drowning out a similarly powered or low powered STA farther from the AP. The farther station simply cannot get enough "talk-time" over the activity created by the closer STA. Near-far can appear as if a wireless network card has failed in the client computer. You can configure the card and be certain that the software is configured correctly, and still may not be able to authenticate and associate with the AP. Sometimes looking at the WLAN implementation plans can help, but since users and therefore STAs are mobile the plan

may not reflect the actual location of devices.

The way to identify near-far is usually to evaluate whether the inability to connect with and communicate with the AP is an intermittent problem or a consistent problem. If it is intermittent, it may be a near-far problem. To determine this, monitor the clients closer to the AP when the distant client cannot connect. Are there more clients closer to the AP each time the distant client cannot connect? If there are, near-far is the likely culprit. You can also look for retransmissions from the client and corruption of frames coming from the client close to the AP similar to the hidden node problem.

In most cases the CSMA/CA coordination functions take care of near-far without administrative intervention. In situations where they do not, the following possible solutions should be attempted:

- Increase the output power at the distant node.
- Decrease the output power of the closer nodes.
- Move the remote node closer to the AP.
- Move the AP closer to the distant node.
- Install another AP closer to the distant node.

Note: **In the real world today, near-far problems are less common as we typically deploy APs with 25 mW of power or less and simply deploy more APs.**

The easiest of these would be moving the distant node or increasing its power. The next best option is to decrease the power at the closer nodes, and then installing a new AP or repeater would be next. Moving the existing AP may cause more problems than you are currently experiencing. You should always evaluate the original site survey to determine why the AP was placed in its current location before relocating it.

Transmit Power Control (TPC), first introduced in the IEEE 802.11h amendment also helps diminish the occurrence of near-far scenarios. TPC was introduced in order to comply with regulatory requirements in some domains but provides benefits in the areas of interference and range control for WLANs.

Weather

Many of the situations I have covered so far in this chapter are related to indoor WLANs with little impact on outdoor bridge links or outdoor WLANs. Multipath is the biggest exception to this statement. Weather is probably the biggest consideration that adds great variableness to outdoor links and WLANs. Severe weather such as major thunderstorms and ice storms with very heavy wind and hail can diminish the quality of your outdoor WLAN links and even reduce the coverage area of an outdoor hotspot or standard WLAN (although I do not think I'll be outside browsing the Internet during a thunderstorm or ice storm). The two biggest factors are likely to be wind and snow build-up on trees.

When snow accumulates on trees or hilltops, it can encroach on the first Fresnel zone. This may cause reduced quality in the links or may make the links impossible to maintain. Additionally, in outdoor hotspot type WLANs that are in wooded areas such as parks, the extra snow (frozen water) can cause increased attenuation of the RF signals. Additionally, snow and ice build-up on outdoor antennas can push them out of alignment.

While wind does not impact RF waves, it can certainly misalign antennas that are not well mounted. This is why grid antennas are often better than dish antennas as they can handle more wind loading. The simple explanation is that the wind can pass through the grid instead of potentially moving the antenna.

To resolve weather-related issues, implement the bridge links with more clearance and with higher antenna gain. These two changes will provide a higher system operating margin and help add resiliency against weather-related issues.

Troubleshooting Voice-over-WLAN (VoWLAN) Issues

VoWLAN is where system capacity, throughput, and latency become a very big issue. If the VoWLAN calls are continually or even frequently dropped, users will eventually stop using them even though you may spend thousands of dollars to provide the users with the capabilities. Because of the overhead introduced by WLANs and the handoff times involved in roaming, VoWLAN implementations must be considered very carefully. When selecting equipment, it is usually best to select equipment from the same vendor for the APs, the wireless IP phones, and the infrastructure so you can be sure that they will all work together to support the same roaming capabilities, QoS features, and IEEE standard.

Common problems in VoWLAN implementations include:

- Dropped calls during roaming
- Dropped calls when staying within a BSS
- Calls not going through to the target

Dropped calls during roaming is usually a problem with the roaming procedure and not really a general problem with WLAN capacity. For an effective VoWLAN implementation, you will practically be required to use a WLAN implementation that uses APs controlled by a centralized switch or a WLAN controller that can maintain the connection as the wireless IP phone roams from one BSS to another or from one ESS to another. In the future, the IEEE standard will ratify fast roaming procedures that can be implemented in various vendors' equipment. This may provide for the ability to implement a mixture of APs, controllers, call managers, and wireless IP phones from different vendors, but we are not likely to see this for a few years. Currently, it makes more sense for the vendors to ensure their equipment works with only their own components.

Dropped calls when staying in a BSS are usually a problem with WLAN capacity, RF interference, or intentional jamming. You may have to install dedicated APs for voice over WLAN and other APs for data use, or at least install QoS aware APs that can give priority to voice over WLAN packets.

Calls not going through to the wireless target station is usually the result of the destination phone being out of the WLAN coverage area. The call will most likely fall back to voicemail in such scenarios. However, the problem may be that the intended target was in fact in in the facility, but he or she was in an area that simply lacked coverage. The solution, in this scenario, is to reevaluate your site survey and repair the network design so that the WLAN provides adequate coverage where it is needed.

VoWLAN and Roaming

The current basic roaming procedures as specified in the 802.11 standard are based on authentication and reassociation. When a STA determines that it should roam—usually based on RSSI values—it will authenticate and reassociate with the new AP. It will disassociate with the previous AP, if it is functioning well. This roaming can take a little time, and if the APs are setup in virtual LANs so that they use the same DHCP servers and/or IP subnets, the STA may even be able to keep its IP address. Since most laptop applications use TCP for data transport, there is retransmission and fault tolerance built-in to keep a connection and/or transfer going. Voice over WLAN, on the other hand, uses UDP for data transfer. Recall that UDP is connectionless and without delivery confirmation. This means that data sent (or that would have been sent) during roaming is simply lost.

The standard roaming time of the 802.11 authentication, reassociation, and dissociation process has been tested and is estimated to be between 200 and 500 ms. VoWLAN needs an end-to-end delay of no more than 150 ms. This means the WLAN roaming delay component needs to be far less than it normally is for VoWLAN. In fact many implementers aim for a less than 50 ms one-way delay. By designing wireless IP phones to scan for APs “in the background” and pre-authenticate to likely roaming targets, voice over WLAN vendors have been able to accomplish this reduction in delay. This, in addition to proprietary management of sessions using call managers and WLAN controllers, has allowed many organizations to implement effective voice over WLAN systems.

QoS Configuration Problems

In the preceding chapter, you learned about wired QoS. Now it is time to explore WLAN QoS (wireless multimedia (WMM)) in greater detail. WMM uses tagging to prioritize 802.11 frames into transmission queues on both the wireless client and APs. As mentioned previously in this book, WMM (802.11e) provides probabilistic prioritization. This simply means that the proper frames should be prioritized for delivery, but they must still contend for the medium. The AP or client station can certainly decide that the higher priority frame will be the next transmitted frame, but they cannot always gain access to the medium before a lower priority frame.

802.11 DCF is enhanced in EDCA to provide this probabilistic prioritization. Additionally, the four QoS priorities (Access Categories, or ACs) in WMM are mapped to CoS values for the wired side. Table 8.1 shows the common mapping of Layer 2 CoS to WMM ACs. This is an example mapping and some vendors may treat this differently, but most vendors comply with this one. The key is to realize the voice traffic gets the highest priority when

sent to the wired LAN, and that data traffic will have AC_BE or CoS 0 or 3 when sent to the wired LAN. WMM simplifies QoS by using only four categories, but you must ensure that your APs/controllers are configured to map the WMM ACs to the appropriate CoS used throughput your network.

WMM can be enabled or disabled in most APs or controllers and is done so using the Web-based or command line interfaces. In some interfaces you can customize the contention window parameters to impact how QoS operates in the cell. In most cases accepting the defaults is sufficient; however, in some cases you may wish to give a higher probabilistic priority to voice or video by lowering the aCWMax value for each even further than the defaults.

Layer 2 COS	WMM Access Category
1	AC_BK (background)
2	AC_BK (background)
0	AC_BE (best effort)
3	AC_BE (best effort)
4	AC_VI (video)
5	AC_VI (video)
6	AC_VO (voice)
7	AC_VO (voice)

Table 8.1: WMM Access Categories Mapped to 802.1p Class of Service

Table 8.2 lists the default parameters for the WMM ACs. As you can see, background and best effort traffic are effectively on an even playing field. Video has a massively lower aCWmax, and voice is lower even still. Given that the number is drawn randomly to begin with and that every STA is counting down the timer, the time will come when BK and BE traffic wins contention over VI or VO traffic. This is why WMM is not considered guaranteed priority, but it is more accurately described as probabilistic priority.

Access Category	aCWmin	aCWmax
AC_BK	15	1023
AC_BE	15	1023
AC_VI	7	15
AC_VO	3	7

Table 8.2: Access Category Default Values

Security Issues

When troubleshooting security issues, consider the following:

- **Roaming delays**: Roaming delays are related to security because slow roaming can break real-time communications due to the overhead of 802.1X authentication. To avoid this ensure faster roaming solutions (OPK, 802.11r FT, preauthentication, and PMK caching) are implemented as appropriate.
- **Policy non-compliance:** Using advanced tools like AirMagnet Wi-Fi Analyzer Pro, you can easily locate Wi-Fi devices operating outside of the compliance rules of your network. When discovered, reconfigure the devices to comply with the security policies of the organization.
- **Authentication:** Many problems occur related to authentication, but the most common are improperly configured pre-shared keys, incompatible EAP types, and incorrect user passwords. When authentication fails, be sure to check these factors.
- **Encryption:** The client must support the encryption and key management protocols you use. Older devices may be unable to connect because they support only WPA, while WPA2 is required of the network. In such cases you may have to implement a WPA SSID to support these older clients.
- **Mobile Device Management (MDM):** Newer WLANs now integrate with MDM solutions. Ensure that the MDM solution of choice is properly configured to identify and manage mobile devices such as iPhones, Android phones, Windows phones, tablets, and laptop computers. In many systems each device type must be configured individually.

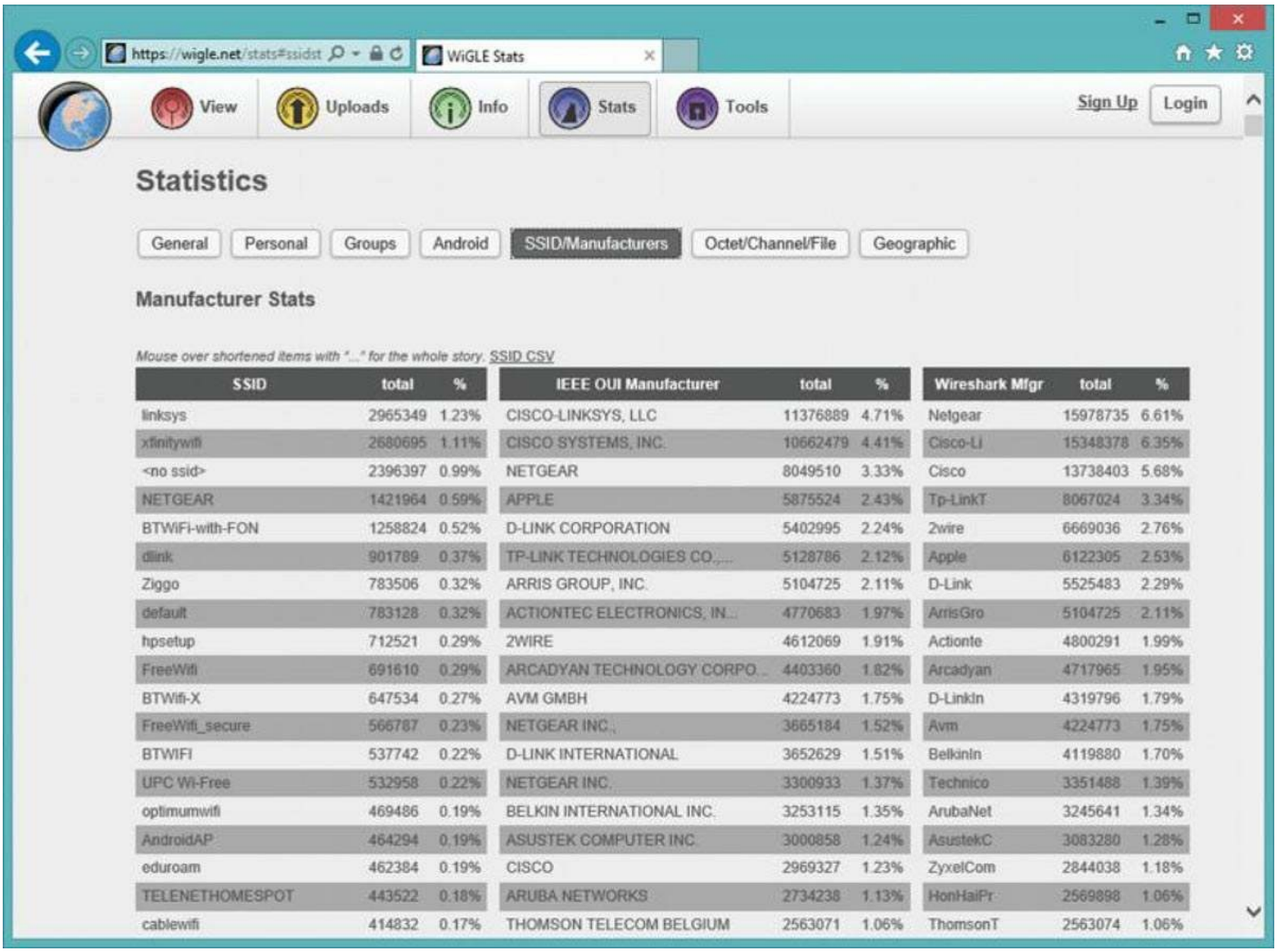
In addition to these items, the WLAN analyst should be prepared to analyze the network in search of non-compliance issues and required upgrades to comply with security requirements. A baseline threat analysis is a security study that compares the existing system with a baseline configuration. The baseline determines the minimum accepted

security settings, and the analysis ensures that the system meets the baseline requirements. The following sections provide recommendations for security baselines in 802.11 wireless networks.

SSIDs

The default SSID should be changed on all access points. The service set identifier (SSID) is meant to differentiate networks from one another. Access points are all set to a default SSID when they are first purchased. For example, most Linksys access points are set to the network name of Linksys, most early Cisco access points had a default SSID of tsunami, most Netgear access points are set to netgear, and so on. These default SSIDs are widely documented on the Internet and are well known or easily accessible by any attacker. The fact that the SSID is still set to the default is often a glaring banner to the attacker that reads, “Please attack me as I am still configured to all default settings!” Figure 8.9 shows such a list of common SSIDs available on the internet.

When access points are first installed, the SSID should be changed to something cryptic and not a string that could be used to determine the company to whom the access point belongs. This is not really a security setting, and it will have little benefit in areas where only one company exists with strong RSSI values from the APs, but it’s still a recommendation. This recommendation assumes that other companies may be nearby. If no other companies are nearby, the attacker can assume that any visible SSID with a good signal strength is the local company’s network. Changing the SSID to something meaningful such as a department name can provide an intruder valuable information. For example, if a wireless network is installed for the Accounting department, and you set the SSID to Accounting, any intruder will know there could be financial information on the network that the access point is attached to.



SSID	total	%	IEEE OUI Manufacturer	total	%	Wireshark Mfgr	total	%
linksys	2965349	1.23%	CISCO-LINKSYS, LLC	11376889	4.71%	Netgear	15978735	6.61%
xfinitywifi	2680695	1.11%	CISCO SYSTEMS, INC.	10662479	4.41%	Cisco-Li	15348378	6.35%
<no ssid>	2396397	0.99%	NETGEAR	8049510	3.33%	Cisco	13738403	5.68%
NETGEAR	1421964	0.59%	APPLE	5875524	2.43%	Tp-LinkT	8067024	3.34%
BTWiFi-with-FON	1258824	0.52%	D-LINK CORPORATION	5402995	2.24%	2wire	6669036	2.76%
dlink	901789	0.37%	TP-LINK TECHNOLOGIES CO.,...	5128786	2.12%	Apple	6122305	2.53%
Ziggo	783506	0.32%	ARRIS GROUP, INC.	5104725	2.11%	D-Link	5525483	2.29%
default	783128	0.32%	ACTIONTEC ELECTRONICS, IN...	4770683	1.97%	ArrisGro	5104725	2.11%
hpsetup	712521	0.29%	2WIRE	4612069	1.91%	Actionte	4800291	1.99%
FreeWifi	691610	0.29%	ARCADYAN TECHNOLOGY CORPO...	4403360	1.82%	Arcadyan	4717965	1.95%
BTWifi-X	647534	0.27%	AVM GMBH	4224773	1.75%	D-LinkIn	4319796	1.79%
FreeWifi_secure	566787	0.23%	NETGEAR INC.,	3665184	1.52%	Avm	4224773	1.75%
BTWIFI	537742	0.22%	D-LINK INTERNATIONAL	3652629	1.51%	BelkinIn	4119880	1.70%
UPC Wi-Free	532958	0.22%	NETGEAR INC.	3300933	1.37%	Technico	3351488	1.39%
optimumwifi	469486	0.19%	BELKIN INTERNATIONAL INC.	3253115	1.35%	ArubaNet	3245641	1.34%
AndroidAP	464294	0.19%	ASUSTEK COMPUTER INC.	3000858	1.24%	AsustekC	3083280	1.28%
eduroam	462384	0.19%	CISCO	2969327	1.23%	ZyxelCom	2844038	1.18%
TELENETHOMESPOT	443522	0.18%	ARUBA NETWORKS	2734238	1.13%	HonHaiPr	2569898	1.06%
cablewifi	414832	0.17%	THOMSON TELECOM BELGIUM	2563071	1.06%	ThomsonT	2563074	1.06%

Figure 8.9: Commonly Used SSID List

Some wireless security professionals will suggest that you set the SSID according to strong password principles. I disagree with this suggestion as it implies that the SSID somehow affords security itself. While you can give away too much information about the purpose of the network with the SSID name (such as in the Accounting department example in the preceding paragraph), you cannot really ensure security through what you might call a cryptic SSID or a strong SSID. Skilled attackers can very easily find and access a wireless network that has no security other than a cryptic SSID. In the end, I suggest you use the SSID for its intended purpose: to differentiate between networks and not to provide a false sense of security.

By default, an access point broadcasts the SSID several times per second in beacons. By listening for these beacons, intruders are provided the opportunity to gather the SSIDs of any access point within range. “Closing the system” by not broadcasting SSIDs in beacons prevents intruders from passively locating the network. Closed system features are not part of the 802.11 series of standards, and they are not supported on all access points. When SSIDs are not broadcast, operating systems like Windows XP do not automatically discover the SSID and do not configure the computer’s NIC for the hidden network. This configuration causes a potential intruder to put forth a little more effort to gain access to the network—something an intruder may not be willing to do. Unless your organization is protecting something that a cracker knows is valuable, most crackers will attack the “low hanging fruit” first, meaning that any networks that are broadcasting an SSID will be the first targets for intrusion.

Even when SSID broadcasting is disabled, the SSID can be discovered using free utilities that perform active scanning (sending probe request frames) or wireless packet analyzers (which hear all frames types). Sometimes disabling SSID broadcasting may go against business goals, such as with public wireless networks. These networks must be open to allow customers to easily find and access network resources (usually Internet access). The protection that SSIDs provide is only minimal at best, but when SSIDs are not properly configured they can present a large security hole.

Note: **Use the SSID attribute to provide organizational structure to your wireless network and as an indicator to your users as to which network they are accessing. Do not use it as a security solution.**

Default Configuration Settings

When considering the threats to your network, you must keep in mind the exploitation of default settings. These settings may include default, misconfigured, and weak passwords and settings.

Default and Weak Passwords

Default passwords are always weak passwords. This is an important principle to remember. For example, Linksys access points come with a default password of admin, and this is well known far and wide on the Internet. For this reason, the default password is weak. Even if hardware came with default passwords like b7HrT9L0, they would be considered insecure or weak. The reason is simple. It wouldn't take long until someone has an Internet site listing these "strong" default passwords, which therefore, makes them weak. Never leave a device's login name and password at their default values in a production system. Always change it to a strong password, and periodically change it as a matter of good security practice.

Default and Misconfigured Settings

Like with passwords, the default configuration settings on all access points should also be changed. To help build a useful network as quickly and as easily as possible, the manufacturer pre-configures all access points to certain default settings. As a result, the default configurations minimize security feature use. The Wi-Fi Protected Access (WPA) interoperability certification, created by the Wi-Fi Alliance, addressed shipping wireless infrastructure equipment with no security features (encryption, network authentication, management login, etc.) enabled. WPA required the person who is configuring the access point to step through a simple procedure of setting up security as part of the initial configuration. This is still the same in WPA2 and helps protect home and small business networks.

Installing an access point or bridge left in default configuration can lead to many problems, and an administrator must think specifically about infrastructure reconfiguration attacks. An infrastructure reconfiguration attack is a situation in which attackers obtain

management access to wireless infrastructure devices such as access points and bridges. In so doing, hackers are able to take down the network, change security measures or poke holes in security mechanisms to allow unauthorized network access, or even prevent authorized use of the wireless network.

When an adept hacker finds a rogue access point, the first network resource they will attempt to gain control over is the wireless network infrastructure itself. Consider that an attacker can go through a rogue access point first to get an IP address, and second to locate authorized access points on the network. The next step is to use Telnet, HTTP, SSH, or SNMP to remotely control or manage the wireless infrastructure devices. This action can have the effect of converting all authorized access points into rogues. To prevent this type of attack, the default username and password (if there is one) should be changed on all infrastructure devices before the device is installed.

Firmware Upgrades

Firmware upgrades can provide new security functionality and compatibility, but frequently they contain bug fixes or security patches as well. Periodic firmware upgrades can often prevent attackers from exploiting a well-known security hole in older firmware. There is always a chance that a firmware upgrade could introduce a new security problem, but at least most brand new security holes are not readily documented for hackers to find. Subscribing to vendor newsletters is a good way to keep up to date on what patches are available. Patches always come with release notes documenting bugs fixed as well as features added. With enterprise WLAN equipment vendors, new firmware releases may be frequent. Frequent firmware upgrades may be too time-consuming for administrators responsible for large installations. Checking the firmware release notes helps administrators reduce unnecessary wastes of time by identifying specific items of interest for a given site.

Firmware should be upgraded as necessary for the following devices:

- Access Points
- Wireless Bridges
- Client Devices
- Client or Workgroup Bridges
- WLAN Controllers

Firmware upgrades are suggested as soon as possible in order to gain any of the following security features:

- WPA2-Enterprise and WPA2 Personal support
- Kerberos support
- 802.1x/EAP (-TLS, -TTLS, -LEAP, -PEAP) support
- Advanced Encryption Standard (AES) support
- Virtual Private Network (VPN) support
- Rogue access point detection

- RADIUS or LDAP support
- Role-based access control

When performing a firmware upgrade, it is a good practice to test the end-to-end functionality of the firmware (either in a lab environment or in a non-critical production area) prior to rolling it out enterprise wide.

Rogue Equipment

Anytime rogue wireless equipment is present in a network, the incident should be considered a serious security breach. In many cases, employees who want immediate wireless connectivity at their organization install rogue access points ahead of an “official” WLAN rollout. Also, portable laptops may incorporate a WLAN client with utilities that employees feel compelled to use to create “soft Aps.”

When these employees realize that access points are very inexpensive, they can purchase and install their own onto the company network without understanding the security risks or knowing that they need permission for such installations—although this should be well documented in the corporate security policy. Certainly network administrators could lock down switches to only support a specific MAC address on each port, but a savvy network user who understands MAC spoofing could easily circumvent such a security measure and the administrative overhead of securing ports may not be deemed worth the effort.

Even the strongest wireless security solutions are rendered useless when a single rogue is added to the network. Rogues can be installed not only by company employees who want wireless access, but also by skilled attackers who want to gain access to the network without being seen. In the case of an attacker, he or she must first gain access to the premises through some type of social engineering or lack of physical security. Upon doing so, the intruder can then locate a live Cat5 or Cat6 port on a switch or hub that the access point can be connected to, preferably close to a window so the signal can be received by a client from outside the building in the typical attack scenario.

<u>Eliminating Rogues</u>

Eliminating rogue wireless equipment is a multi-step process, parts of which are ongoing to ensure the security of the network. The process includes:

- Setting Corporate Policy Regarding Rogue Equipment
- Network Administrator Training
- Help Desk & End User Training
- Intrusion Detection Systems & Audits

Would your organization allow someone—an end user or IT professional—to install his or her own DHCP server on the wired network? Such an example is the equivalent to allowing a SOHO wireless access point to be installed onto the wired segment of any corporate network. Rogue equipment installations of any kind should be clearly prohibited in the corporate wireless security policy, and offenders of such policy should be disciplined according to company policy for putting corporate assets at risk. A less-

considered topic in this area is rogue ad hoc networks. Corporate computer users should not use wireless ad hoc configurations due to the peer attack risk.

A common mistake made when an unauthorized AP is discovered is to destroy or reset the rogue access point. One should certainly control the possible damage done or being done by the access point, but the logs within the access point may provide excellent evidence of what damage has already been done. The first thing to do when finding a rogue access point is to unplug its wired Ethernet port from the network. Secondly, logs should be saved and screen captures of association tables and traffic measuring parameters made, if possible.

Proper staff training for those responsible for the wireless network is essential. It is important to note that, just because an organization does not have a WLAN, or even if they have no plans to implement a WLAN, it is still important for network security administrators to understand WLAN technology and security risks. When an attacker wants access to a network that has no wireless connectivity, it may be his first choice of attack method to place a rogue device onto the LAN. At today's low prices for wireless hardware, and the ability of anyone to buy inexpensive, non-mainstream solutions such as 900 MHz and FHSS radio equipment on Internet auction sites, network administrators must be alert to all of the techniques of a wireless attacker.

Help Desk personnel should be trained in the support of WLAN technology, security risks, and security solutions. Being able to recognize when a user is connected to a rogue device, or assisting end users with properly configuring wireless security solutions is a key part of help desk activities. End users should attend a user-level class (whether classroom-based or computer-based) if offered on how to properly implement the WLAN security solution that has been chosen by the organization. Ideally, part of this training should encompass recognizing rogue connections, understanding why not to add rogue devices to the network, and the consequences both to the organization and to the individual if network security policy is not followed.

Wireless network management includes tasks such as monitoring and auditing the network for rogue wireless devices. If an intrusion detection system (IDS, discussed later in this section) is not used, an administrator will need a wireless analyzer capable of locating any rogue devices as he walks the premises of the entire organization on a regular basis—daily or weekly. There are many such specialty hardware devices and software packages produced for this and other special purposes on the market today. Wireless packet analyzers are best suited for this type of manual procedure.

Before beginning a manual network scan, an organization must have an up-to-date inventory of which access points and bridges should be on the network and the MAC addresses and SSIDs of these devices. After the scan, a comparison can be done to compare what is actually found in the search against what should have been found. When performing this type of scan, all physical locations of the company must be searched, not just those that are supposed to have wireless access. Rogues are most likely to be added by employees in those areas that do not have wireless access already. Also, because intruders will be likely to plant rogue devices near windows so that the signal can reach the parking lot or other remote locations, the surrounding (outside) areas of the facility should be scanned regularly where an automated mechanism is not in place

One thing most inexperienced administrators miss is scanning for rogue devices in all frequency bands that WLAN equipment uses. Most administrators would search for Wi-Fi compliant devices in the 2.4-2.5 GHz and 5 GHz bands, while a skilled hacker might use a900 MHz system. Another hacker approach is to use relatively obscure FHSS systems as rogues instead of DSSS systems. An IDS would be useful in detecting and alerting administrators as to any new and unauthorized MAC addresses (access points have MAC addresses) on the network, so frequency and spread spectrum technology use would be irrelevant as long as the IDS is able to catch the rogue device.

RF Cell Sizing

Accurate cell sizing of the RF output generated by an access point or bridge can aid in preventing war drivers from being able to locate your wireless network. Configuring the output power to be greater than is required to provide the needed coverage results in easier access for outside connections. When the cell overflows far beyond the physical security parameters put in place by the organization, any war driver passing by could easily detect the signal and locate the network. Of course with the proper antenna, he or she may be able to see the network anyway, but you make it easier when the cell size is larger than required. If outdoor coverage is intentional, you accept the risk that comes with extending the WLAN beyond your walls. But there is still a balance to be had—you might want to cover a popular patio with signal but that doesn’t mean you have to blast signal beyond that targeted outdoor area.

Note: **Not all access points or bridges offer the administrator the ability to control output power. Such functionality may be one of the criteria in deciding what brand of equipment to use.**

The output power of a cell should be limited to only the coverage area that is required as defined by the site survey. Emitting more power to cover unnecessary areas only provides a war driver with a target for attack. Limiting the output power of a cell does not guarantee that a network will not be located, but the war driver must now use a more directional antenna to locate wireless networks and this may prevent casual Internet use theft, which is a frequent purpose driving the war driver in the first place.

Because administrators will not know what type of antennas a war driver may be using or how powerful they are, no assumptions should be made about security based on the size of the cell. Within a facility, part of the site survey should include the most appropriate antennas that should be used to get the necessary coverage while still considering the security risks.

Once the wireless cells have been properly configured for power output, administrators should attempt a footprint analysis to determine how easily the network can be targeted from outside the facility. This analysis involves using omni and directional antennas while walking around the facility to determine what distance a war driver would need to be from the facility in order to locate the network. In an office complex where buildings are close

together or the building in which the organization resides is open to public access, the distance for someone to pick up the signal is usually minimal. This is an area where you do your best but will seldom achieve perfect signal containment.

SNMP Community Strings

SNMP community strings should be changed or disabled if SNMP is not in use. Most enterprise class WLAN vendors ship WLAN infrastructure devices such as access points and bridges with Simple Network Management Protocol (SNMP) enabled. Default read and write passwords are clearly documented in the users' manual, with "Public" and "Private" being extremely popular default strings. Many administrators make the mistake of securing Telnet and HTTP management interfaces, but leave SNMP settings in the default configuration. This lack of configuration opens the door to attackers using SNMP management software to control these devices in just the same way as using the HTTP or Telnet interfaces. It is even possible to reconfigure the management login information for HTTP and Telnet interfaces using SNMP. SNMP management software is very inexpensive and quite powerful in controlling wireless network devices. It is important to disable SNMP access if it will not be used. If SNMP will be used, set the read and write community strings to complex, non-default values that are unrelated to the network's SSID, WEP key, or organizational information. Also, disable SNMP access from outside the corporate environment by using access control lists or firewall filtering capabilities.

Discovery Protocols

When discovery protocols are not in use, they also should be disabled. There are a few proprietary network discovery protocols on the market today. One of the more well-known discovery protocols is the Cisco Discovery Protocol (CDP). Cisco Discovery Protocol (CDP) is primarily used to obtain IP addresses of neighboring devices and to discover the platform version of those devices. CDP can also be used to show information about the interfaces your router uses. CDP is media- and protocol-independent, and runs at layer 2 on all Cisco-manufactured equipment including routers, bridges, access servers, and switches.

Whether using Cisco or another vendor, it is important to disable discovery protocols if they are not in use by the network management system or specifically used for troubleshooting by the network administrator. The reason for this security step is that an intruder who has gained administrative access to an access point may be able to map parts of the network and find vulnerabilities in firmware running on infrastructure devices by querying the access point's CDP information.

Remote Configuration

In the most stringent of high security environments, it may be necessary to disable all configuration interfaces on access points and bridges except the serial console port (if possible). When HTTP, Telnet, or SNMP interfaces are used for remote network

management, it is important to consider the possibility that those passwords or community strings may be accidentally passed across an unsecured wireless bridge link. Securing these links allows administrators to perform normal network management functions without worry that authentication information could be compromised. If manufacturer-specific feature sets allow for it, configure access points and bridges so that they cannot be configured over the wireless network segment. Make it a point where possible never to log into access points or bridges over an unsecured link or when using an unsecured protocol.

Client Security

Using client security solutions can reduce peer-to-peer attacks. Peer-to-peer attacks over WLANs are common due to unsecured operating systems. Securing wireless clients from attack is just as important as securing the network infrastructure. Many times, it is while connected to a public access network without proper protective measures in place that WLAN users are hacked. Client computers often have valuable corporate information on them, such as passwords, documents, spreadsheets, and reports. If the computer belongs to a network administrator, that machine will most likely have account information, logins, and network diagrams. Because of the value of the data that is often transported in portable computers, wireless security policy should limit any sensitive data on client machines that could damage the organization to which it belongs, and public access connectivity should likewise be limited (and protected) if not completely prohibited. One particular security weakness that is commonly exploited by hackers is file and folder sharing on workstations. Shared folders should be limited or even prohibited on unmanaged wireless client stations.

There are many tools that can be used to protect wireless clients while connected to the wireless network. Some VPN technologies, such as IPSec, when properly implemented, provide protection from peer-to-peer attacks. On the other hand, there are VPN technologies commonly used with WLANs that allow unauthenticated peer connections even when the VPN connection is enabled. Personal firewall software installed on wireless client computers can effectively thwart peer-to-peer attacks but can also introduce added administrative overhead and cost. In addition to personal firewalls, layer 2 endpoint security software can help protect your client devices. Endpoint security, in our context, is the practice of securing endpoint devices. Endpoint devices are the devices that provide connectivity to the network and network services for end users. Securing these devices may mean the use of virus protection, spam protection, and more. But for our purposes, it means protecting wireless clients from known wireless attacks.

In cases where the infrastructure to which the client is attached is secure, such as when using 802.1x/EAP solutions, peer-to-peer attacks are usually limited to authorized users attacking other authorized users. This scenario still represents a serious problem, considering that 80% of all network attacks come from authorized users. There are some implementations of 802.1x/EAP and VPN technologies that disallow peer-to-peer connectivity while an authorized connection that normally allows such connectivity is in place.

Some VPN users remotely accessing a corporate network utilize client VPN software

directly from their desktop computer. Other times, the VPN client is a hardware device such as a router doing site-to-site VPN. In cases where multiple computers reside behind a hardware VPN device, there may often be access points for mobile access. This configuration allows mobile clients collectively to use the same VPN tunnel into the corporate network. This situation presents a gaping security hole when the wireless network is not secured because unauthorized users may use the same VPN tunnel to access the corporate networks as the authorized users use if other controls are not in place.

Staging and Testing

Staging and testing should occur prior to deployment. One common mistake made when deploying wireless networks is to treat security as an afterthought instead of integrating it into the initial configuration before deployment into a production environment. When this mistake is made, the opportunity exists for an attacker to gain access to the network and to configure back door security holes that can be used for entry at a later time. This same mistake also allows the attacker to reconfigure access points, perhaps changing or adding new username/password settings for their own use. To avoid this scenario, wireless infrastructure devices should be staged and configured in an isolated environment for a secure deployment before they are installed on the network. Network administrators should use approved security configuration checklists to assure that no security holes are created due to lack of following configuration procedures. Proper staging helps not just the WLAN security paradigm, but with overall configuration integrity and consistency.

Equipment Installation

Equipment should be installed out of sight and reach, when practical. Organizations that have access points and other wireless equipment widely deployed often provide no type of theft prevention for their equipment. Access points and antennas, both of which need to be in common areas for the greatest benefit, are especially vulnerable to theft in certain environments. For example, many hospitals have access points mounted directly to the ceiling in plain view. It would take little effort for a thief to move a chair under an access point and quickly remove it.. The perpetrator might even go unnoticed if he were to wear convincing maintenance or security attire. To prevent theft of wireless network equipment, devices should be:

- Mounted out of reach
- Bolted down with tamper-proof fasteners or secured in locked steel boxes
- Kept out of plain view

Taking these precautions decreases the possibility that the devices will be stolen, replaced with a cheaper model, or reconfigured through the console port.

Client Issues

This final chapter section reviews some common client issues you must consider when

troubleshooting and analyzing WLANs, including:

- Drivers
- Adapter Limitations
- Hardware Switches
- Configuration Errors
- Supplicant Issues
- Operating System Bugs and Vulnerabilities

Drivers

802.11 adapter drivers can have a significant impact on performance and stability. If you are experiencing performance problems or lack of common features, ensure you are using the latest vendor drivers. The driver can determine the availability of key features, including:

- The use of both bands on a dual-band adapter
- Support for the latest security options
- Optimum performance of the radio chipsets
- Bug fixes

Adapter Limitations

Even with the right driver installed, you are still constrained by adapter limitations. For example, a single-band adapter simply cannot operate outside of its frequency capabilities. In most cases, single band adapters are 2.4 GHz only. Shockingly many such adapters are still sold, and many devices are still sold having only internal 2.4 GHz radios. Other limitations to consider include:

- Supported PHYs
- Supported bands
- Number of supported spatial streams
- Support for security features (typically a factor of the drivers or supplicants)
- Interface type (USB, mini-PCIe, etc.)
- Receive sensitivity
- Antenna gain
- Output power
- Support for WMM

Hardware Switches

Believe it or not, one of the most common problems you will encounter with laptop computers is the hardware switch or function key that controls the Wi-Fi adapter's off/on status. When a user reports that the wireless networks are no longer displaying on the system, always start by verifying that the hardware or software switch is turned on. Many laptops have a lighted indicator above the keyboard or on the switch itself to indicate the status of the adapter. Train the users, and then retrain them as it can take several instances of this problem occurring before many users remember to check this on their own.

Configuration Errors

Most configuration errors are related to security configurations. Mismatched pre-shared keys, improper EAP settings, wrong user passwords, and other security-related settings are frequent culprits.

Additionally, many operating systems allow for the customization of specific driver settings. For example, in Windows many settings are available that can impact the ability of the client to use the WLAN as expected. An excellent example of this is shown in Figure 8.10. Notice that 5 GHz has been disabled. While the adapter shown can support 5 GHz, if it is disabled here the device will never connect to a 5 GHz network. When in doubt, always check these settings.

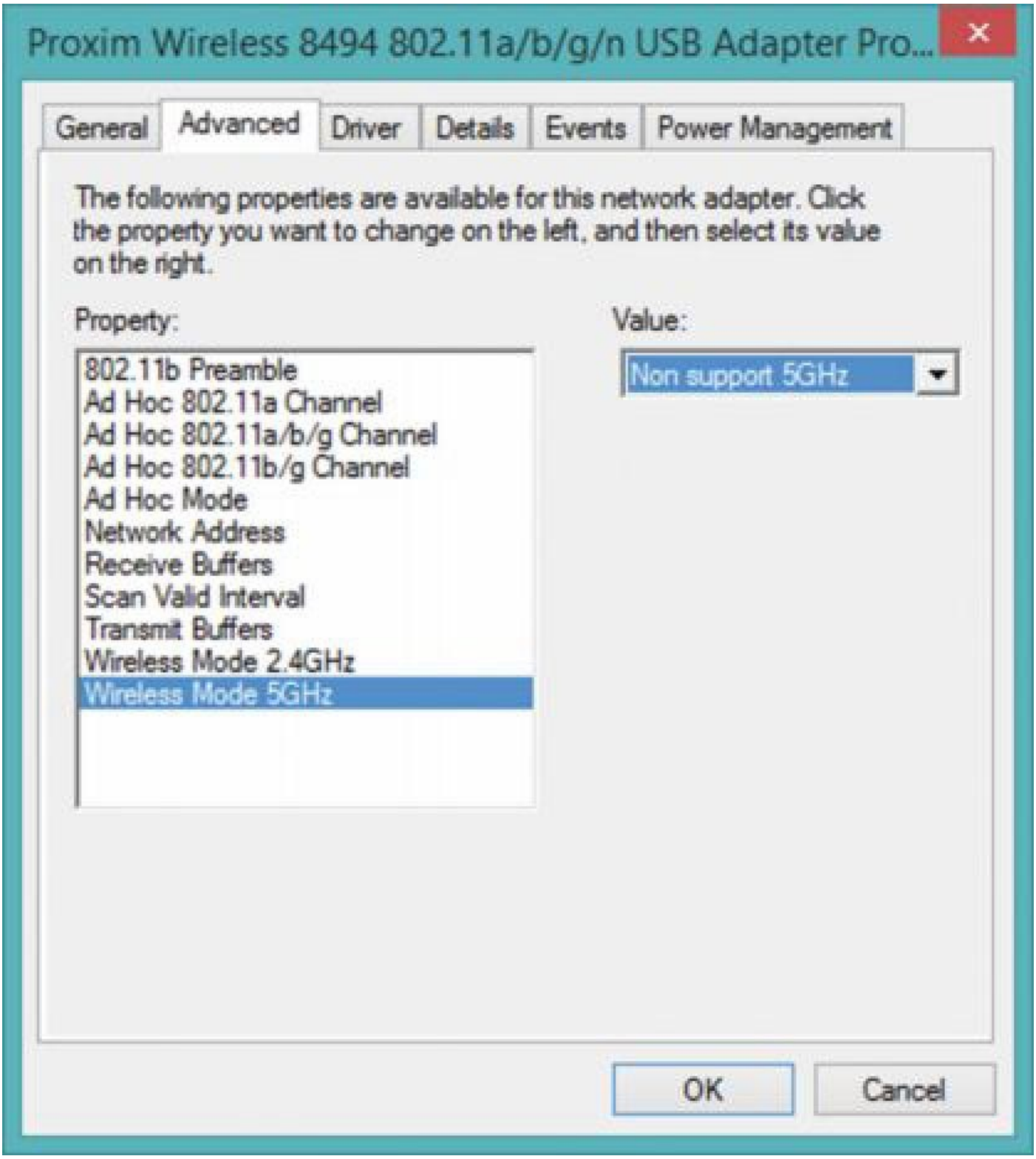


Figure 8.10: Adapter Driver with 5 GHz Disabled

Supplicant Issues

Supplicant issues are also mostly security related. However, in this case, the common problem is lack of support for a needed EAP type. Third-party supplicants may be available to provide the EAP type required; however, it is important to remember that many devices will not have the option of installing an alternative supplicant. This is true of many mobile devices.

As an example, iPhones and iPads support the following EAP types:

- EAP-TLS
- EAP-TTLS
- EAP-FAST
- EAP-SIM
- PEAPv0
- PEAPv1
- LEAP

Knowing this kind of information and the types of devices you must support can assist you in making good planning decisions related to WLAN security design and implementation.

Operating System Bugs and Vulnerabilities

Finally, you must consider operating system bugs and vulnerabilities introduced by the WLAN clients. It is important to keep up with new vulnerabilities related to your operating systems and hardware. Websites like CVEDETAILS.COM prove very useful in these scenarios. Additionally, you can visit specific vendor websites to learn about issues.

CVE stands for common vulnerabilities and exposures. Websites that report on new CVEs help you stay ahead of the attackers and maintain a patched network and device pool. Some network access control (NAC) systems will allow you to integrate with CVE providers to automatically add checks that verify particular applications or operating systems that have been updated to protect against vulnerabilities before allowing them access to the network. Whether manual or automated, staying up with security issues related to the WLAN and its clients is part of the analyst's responsibility.

Modern Issues

Some additional issues should be addressed in this text, though at the time of writing they are just coming into our environments. These include Internet of Things (IoT), Multi-User-MIMO (MU-MIMO), and new operational bands (900 MHz and 60 GHz).

IoT

Simply defined, the IoT is the collection of devices that use computing and network technology to communicate with each other and with monitoring systems. Direct human interaction may or may not occur with the IoT objects and they are frequently found in the 2.4 GHz band today, with future devices likely implemented in the 900 MHz band thanks to 802.11ah. Some studies predict nearly 50 billion IoT devices by 2020.

The expected end result of IoT, from a productivity perspective, is even greater automation than we have today. For those devices operating in 2.4 GHz, the expected end result is even more interference than we have today. IoT devices include environmental monitoring solutions (humidity, temperature, etc., healthcare applications (heart monitors, blood pressure monitors, etc.), wearable technology (smart watches, fitness monitors,

etc.), and even biological monitoring solutions (bacteria detectors, heat detectors, etc.).

The large number of devices warrants a much larger address space than we're used to with IPv4. For this reason, many expect IoT to be a major force in finally transitioning environments over to the IPv6 protocol with its 128-bit address space (as opposed to the massively smaller 32-bit address space in IPv4). This change will require the mastery of IPv6, as many have not really explored this new version of the IP protocol because of the pervasiveness of IPv4.

Note: **Some are using the phrase Internet of Everything (IoE) to reference both IoT and traditional Internet clients. More specifically, IoE is the integration of people, data, processes, and devices into the network.**

In the 2.4 GHz, the Wi-Fi Direct standard, is basically an embedded software AP in devices so that WPS can be used for security and direct setup between two devices. Many IoT devices can take advantage of Wi-Fi Direct and ensure compatibility—even from different vendors—because of the use of the 802.11 standard protocol. The downside to our existing WLANs is that these devices typically operate in 2.4 GHz instead of 5 GHz because of the cheaper hardware and greater range of reception capabilities in this lower band.

With the 802.11ah amendment, this may change. 802.11ah devices will not cause interference with 2.4 GHz or 5 GHz WLANs since they operate in the 900 MHz band, which at this time is expected to use a frequency range of 902–928 MHz. These devices will be able to communicate over sufficient distances with very low output power due to the wavelength used in the RF medium. Channels will likely range from 1 MHz to 8 MHz with data rates from 150 Kbps to 40 Mbps. Considering that many IoT devices require very low throughput rates, 150 Kbps links would be sufficient.

The issues introduces by IoT are really not new:

- Addressing potential interference problems
- Addressing design issues in 900 MHz
- Addressing communications issues across the enterprise network

However, while not new, the massive number of devices is likely to introduce greater complexity to the issues. This is particularly true with interference in the 2.4 GHz band. Ultimately, it is another driver energizing the move to 5 GHz for data WLANs.

MU-MIMO

MU-MIMO takes advantage of transmit beamforming and channel sounding to transmit to multiple client STAs at the same time. MU-MIMO is a downlink-only technology and does not support receiving multiple frames from multiple client STAs at the same time. From a troubleshooting perspective, as we see more implementations of this in the coming years, the most common task will be determining its effectiveness in operations.

To implement MU-MIMO, the AP creates groups that can receive streams at the same

time. A group may include only two receiving STAs, or it may include more if the AP supports more. For example, a 4x4:4 AP could transmit to a maximum of 2 STAs supporting 2 spatial streams at the same time.

The AP vendors should provide reporting information on the status and operations of MU-MIMO. These reports should include information on the groups in use, the efficiency gains through the use of MU-MIMO, and concerns such as retries or CRC errors. How this is reported and what information is provided will be up to the vendors.

Note: **Future versions of the CWNA certification will cover MU-MIMO in greater depth. The CWNA-105 version simply references it as a feature introduced in 802.11ac. The current CWAP exam does not cover it in-depth because it is not implemented in production environments in early 2016. Future exams will address it from a troubleshooting perspective.**

New Operational Bands

802.11 has supported the 2.4 GHz and 5 GHz bands since 1999 with the release of 802.11a. Two new bands have been added in recent amendments or drafts. The 802.11ad amendment supports operations in the 60 GHz band. This is mostly used for in-room high data rate communications, such as video over wireless. The 802.11ah draft (in early 2016) specifies use of the 900 MHz band and will be used mostly for IoT devices.

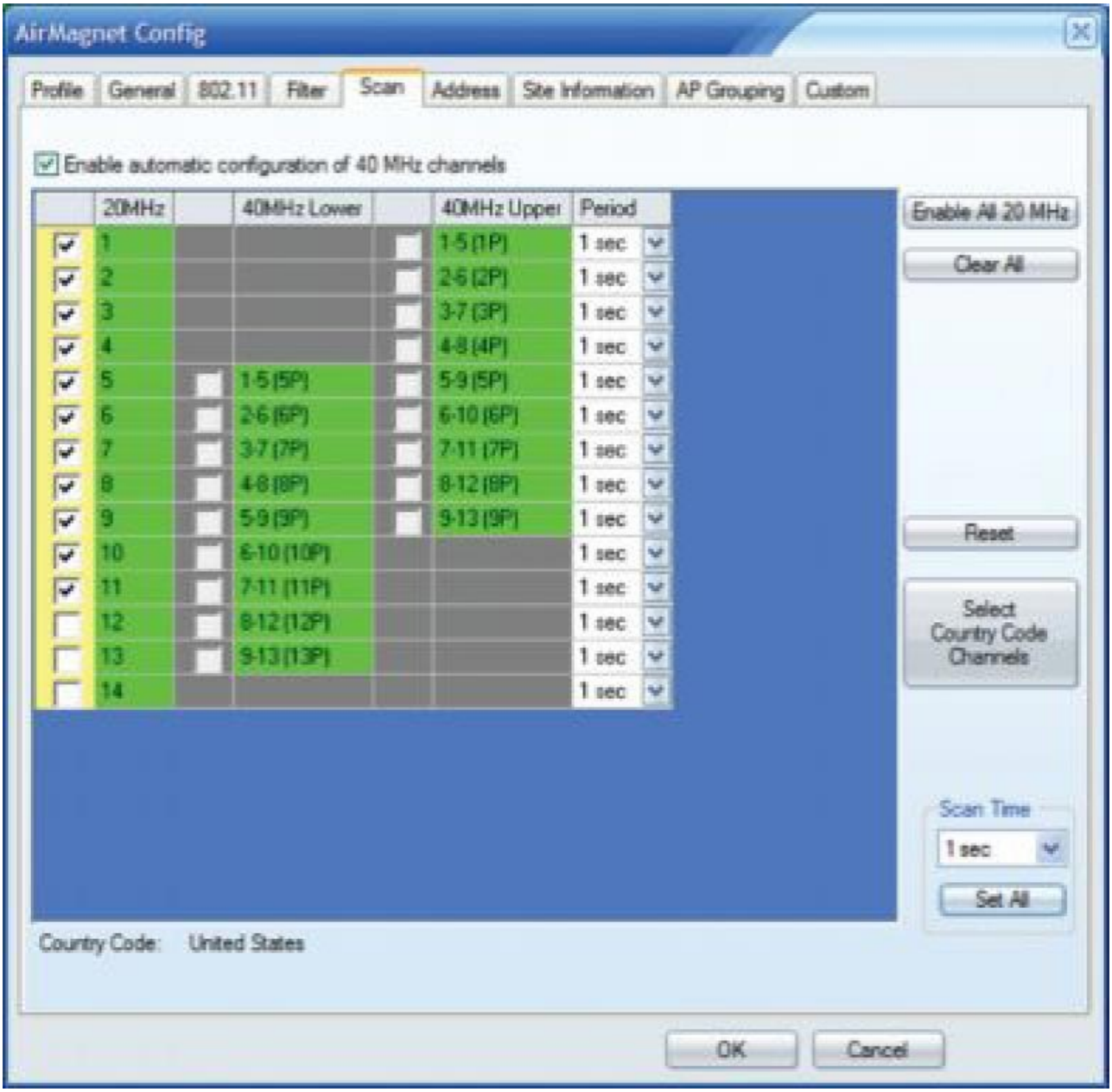
As these new bands see more use, new tools will be required including:

- **Spectrum Analyzers:** A spectrum analyzer is designed in hardware to monitor specific bands. Most wireless engineers today use adapters that work in 2.4 GHz and 5 GHz only. New devices will be required to monitor 60 GHz and 900 MHz frequencies.
- **Protocol Analyzer:** Like spectrum analyzers, wireless engineers use 802.11 devices that can capture frames in 2.4 GHz and 5 GHz. To capture frames in 60 GHz and 900 MHz, new adapters will be required and must be supported by the capture engine used.
- **Survey Software:** Site survey software (or planning software) falls into the same category as spectrum and protocol analyzers, and many packages support both capabilities. Therefore, adapters that work with the site survey software will have to be acquired to perform surveys in the software. Simulated planning can still be performed without additional hardware once the site survey software supports the additional bands.

Exercise 8

In this exercise you will use AirMagnet Wi-Fi Analyzer Pro to evaluate the performance of WLANs operating in 2.4 GHz. If you do not have access to an adapter (such as the Proxim Orinoco® 8494 as was used in this case) and the software required to perform this exercise, you can view a video demonstration by going to YouTube and searching for "CWNPTV AirMagnet Performance Monitoring".

1. Insert the Proxim adapter that is compatible with Wi-Fi Analyzer Pro.
2. Ensure that the appropriate driver available from MyAirMagnet is installed.
3. Launch Wi-Fi Analyzer Pro.
4. Select File > Configure, and navigate to the Scan tab.
5. In the lower-right corner select 1 sec for the scan time and choose Set All.



Graphic 8.1

6. Click OK to save the changes.

7. In the drop-down band selector choose 2.4 GHz to scan only that band.

Graphic 8.2

8. Click the red Stop button and then the green Start button to reset all packets and stats.

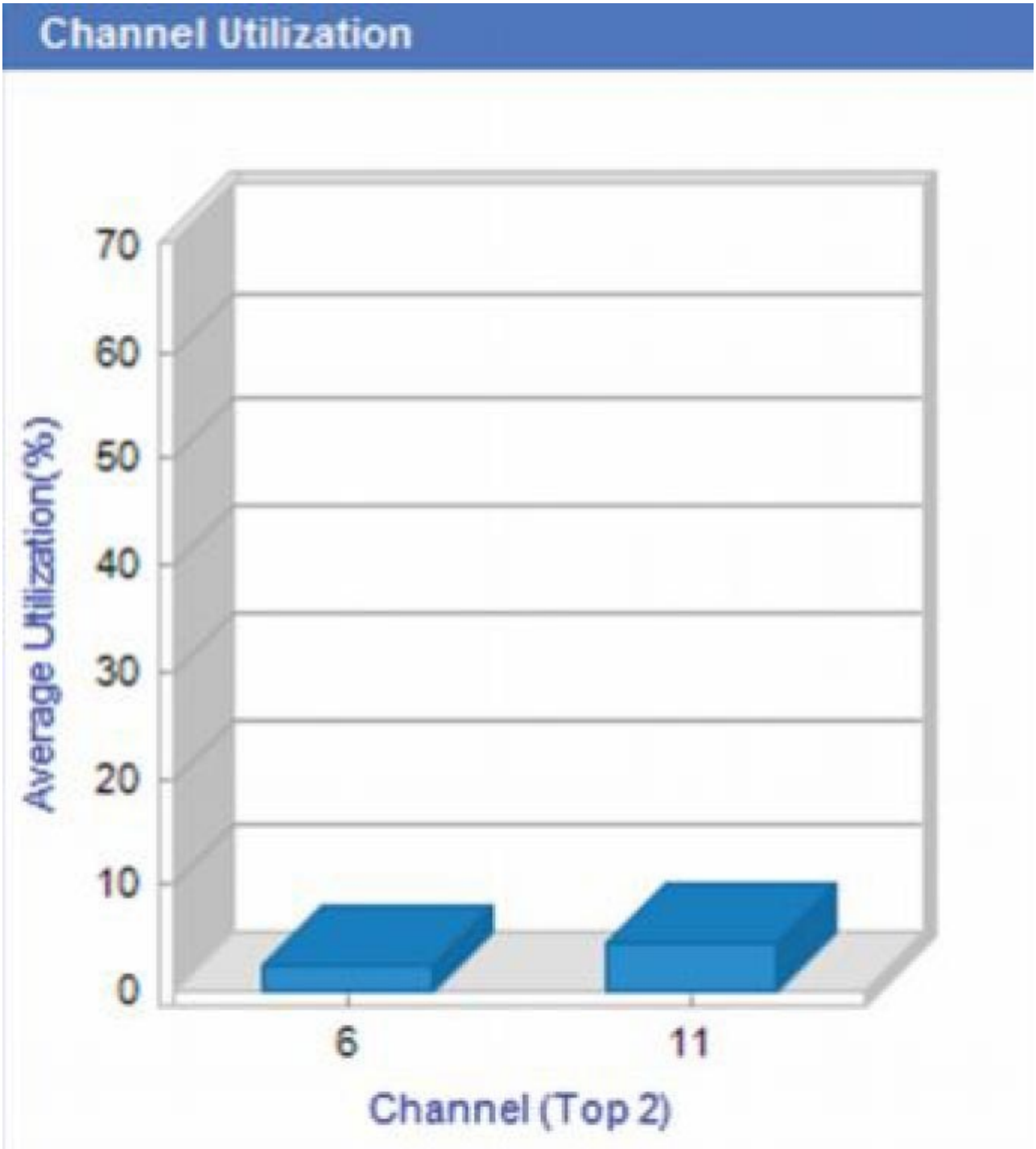
9. Allow the protocol analyzer to run for several minutes to gather sufficient evaluation information.

10. Note the channel monitor in the upper left corner of the Start screen. Click the down arrow in the upper-right section to view more information as shown in the following graphic. Important information includes the signal level, noise level, and signal-to-noise in dB. The interference score indicates CCI and number closer to 10 are worse than numbers closer to 0. If integrated with Spectrum XT, the interference score will also factor in non-Wi-Fi interferers.

Signal Level(dBm)
2.4GHz(802.11b/g/n)
-10
-100
1 2 3 4 5 6 7 8 9 10 11 12 13 14
Noise Level(dBm)
-10
-100
1 2 3 4 5 6 7 8 9 10 11 12 13 14
Signal/Noise(dB)
80
0
1 2 3 4 5 6 7 8 9 10 11 12 13 14
Interference Score
10
0
1 2 3 4 5 6 7 8 9 10 11 12 13 14
802.11 Information
SSID (9)
Ad-Hoc
Infrastructure
AP (8)
STA (4)
Computer (3)
Smart Device (1)
AirWISE Advice
Security IDS/IPS (13,23,10,0)

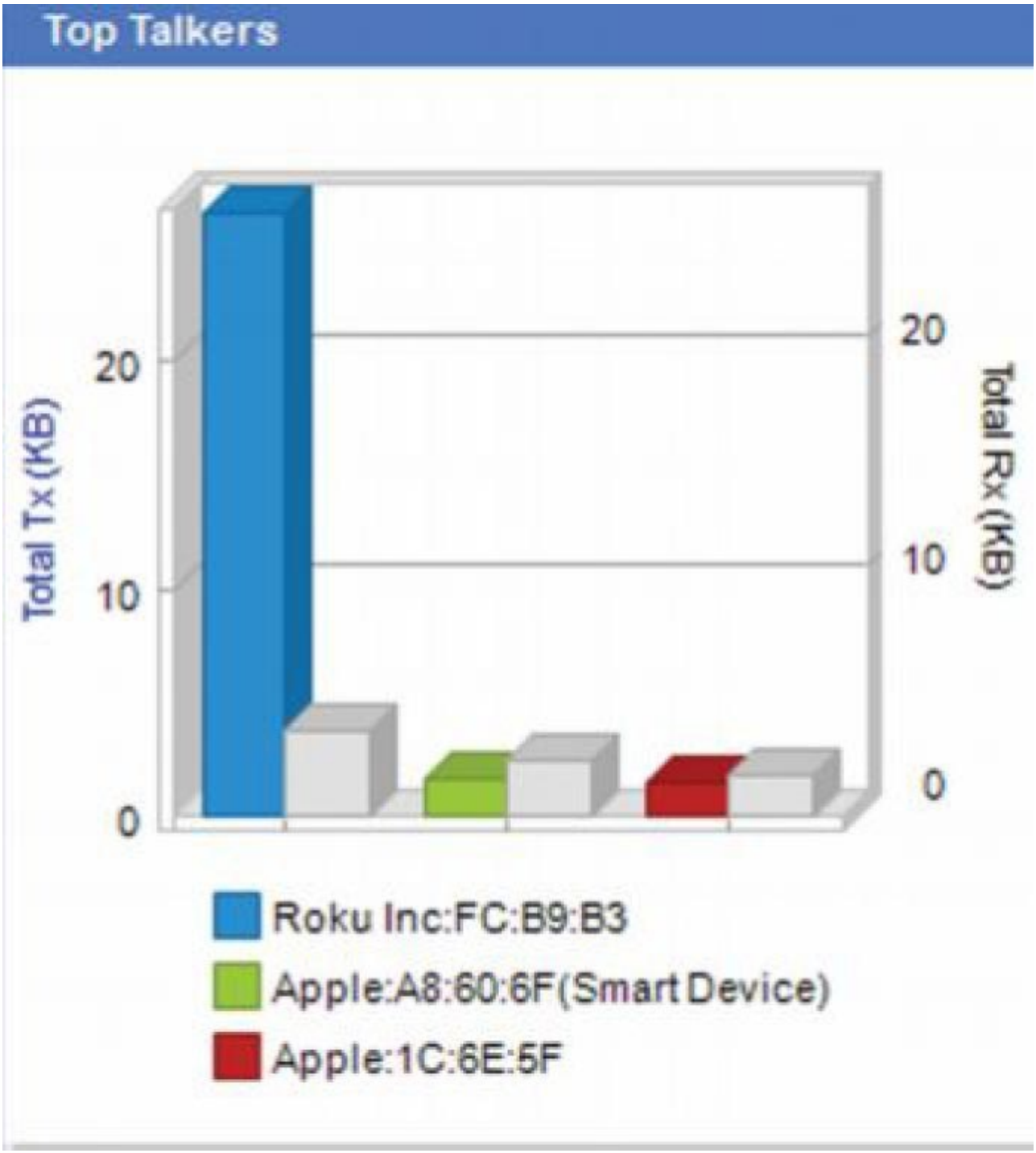
Graphic 8.3

11. The Channel Utilization view shows the top channels based on utilization. In the image here utilization is very low and not indicating oversaturation at all. When utilization is close to 70%, it is time to begin considering expansion of the WLAN or upgrading to newer PHYs with greater data rates.



Graphic 8.4

12. The Top Talkers view can be useful in locating busy devices that may be causing performance problems on the WLAN.

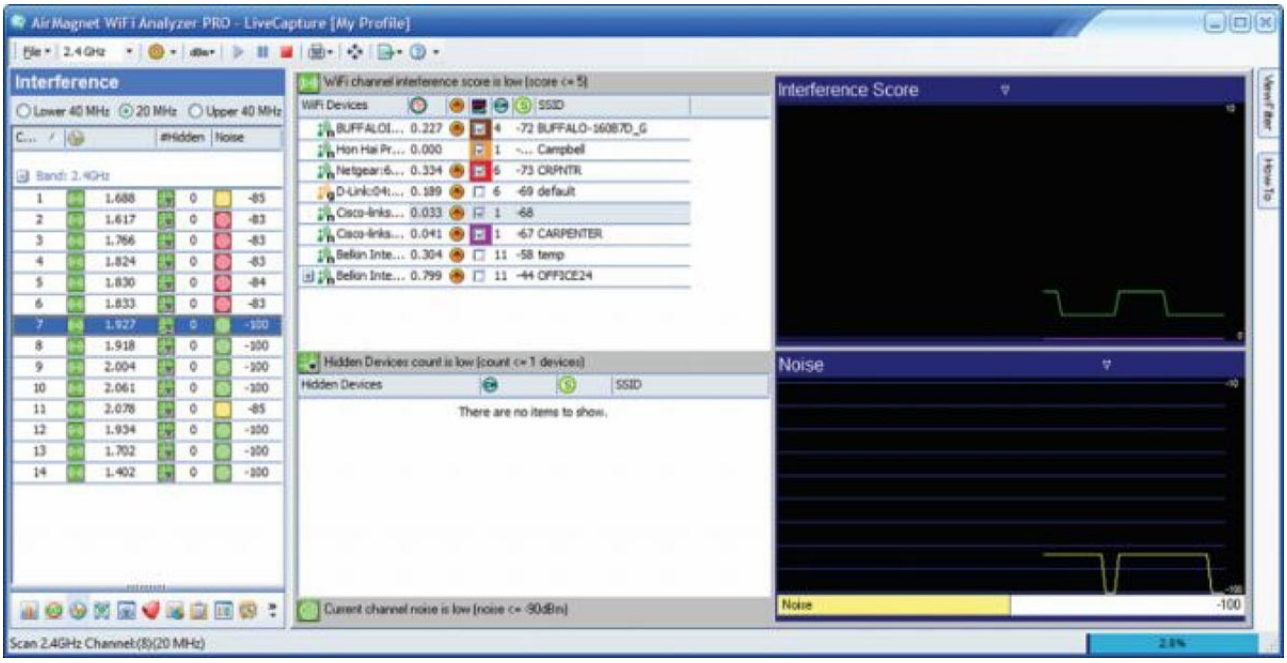


Graphic 8.5

13. The Channel view allows you to investigate a specific channel and see utilization as well as the number of STAs and APs on the channel. Too many APs on a channel can result in excessive CCI particularly when they are close together or at a client location where their signals are equally strong.

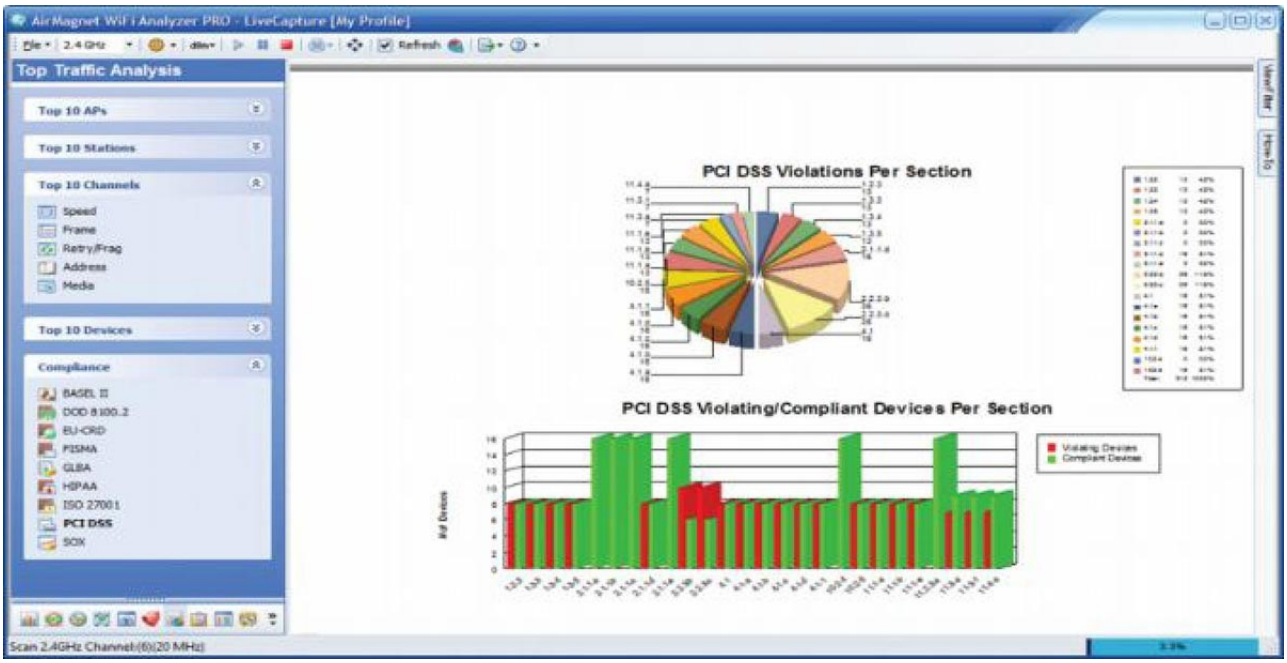
Graphic 8.6

14. The Interference view allows you to see channels that may be experiencing interference problems.



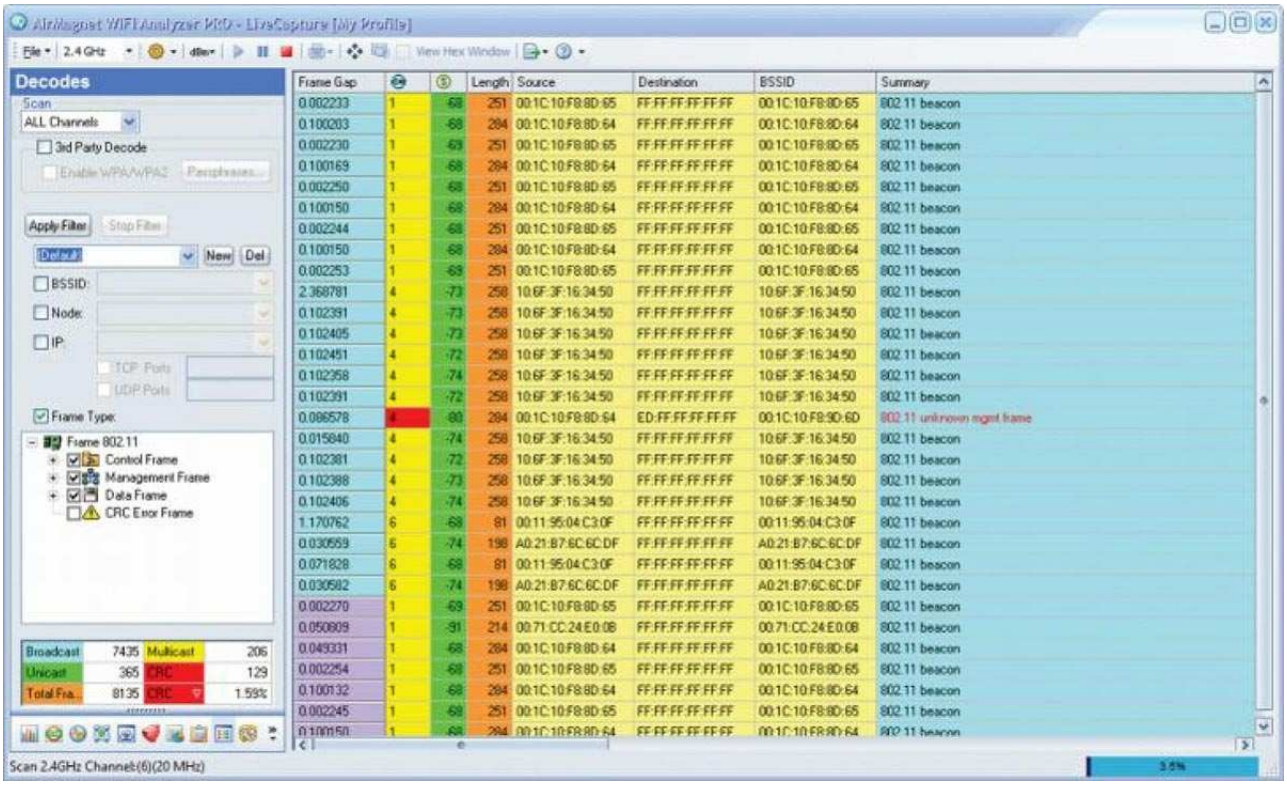
Graphic 8.7

15. The Top Traffic Analysis view allows you to see the top APs, STAs, channels and devices by speed, frame type, retries, and more. It also allows you to compare the network against various compliance requirements. The following graphic shows PCI DSS analysis.



Graphic 8.8

16. Finally, the Decodes view allows you to inspect the actual frame captures for low-level analysis.



Graphic 8.9

Chapter Summary

In this chapter we explored common problems in Wi-Fi networks and various methods to resolve them. You considered client issues, security issues, QoS issues, and various types of interference. In the following Appendix instructions are included for installing several different protocol analyzers so that you can gain experience using these tools. (The more you use them, the stronger your analysis skills will be.) This Appendix is followed by a glossary of terms to help you master these WLAN analysis topics.

Review Questions

1. In addition to the data rates supported what other factor of the various PHYs has a significant impact on capacity?
    a. Protection mechanisms
    b. Preamble
    c. PLCP header
    d. IP Precedence
2. What is the minimum Ethernet port speed needed in modern APs?
    a. 100 Mbps
    b. 1 Gbps
    c. 10 Gbps
    d. 10 Mbps
3. What can you do to reduce the impact of beacon frames on CCI and channel utilization?
    a. Disable SSID broadcasting
    b. Use frame aggregation
    c. Use fewer SSIDs per radio
    d. Use WPA2 encryption
4. When you capture frames on a channel but see frames from another channel, of what is this an indicator?
    a. CCI
    b. ACI
    c. Non-Wi-Fi interference
    d. A microwave oven
5. Why does disabling lower data rates reduce CCI?
    a. Frames that must be sent at low data rates use less air time.
    b. It prevents VHT clients from connecting.
    c. It reduces the range of the PHY preamble and header.
    d. It reduces intersymbol interference.
6. When using a protocol analyzer to evaluate CCI, what should be considered about a channel in addition to the number of BSSs seen on that channel?
    a. Utilization
    b. The frequency used

c. The number of non-Wi-Fi devices detected

d. The use of RIFS

7. Why is it best to use Wi-Fi devices for various functions instead of non-Wi-Fi devices in the same frequency space?

a. Wi-Fi devices always use narrower channels,

b. Wi-Fi devices always have higher gain antennas,

c. Wi-Fi devices always use lower output power levels,

d. Wi-Fi devices will comply with contention rules,

8. What is one method used to detect hidden nodes?

a. Corrupt frames at the AP and retries at the client

b. High retry rates at the AP for all clients

c. Large walls near the AP

d. Large walls near the client

9. If you attempt to use a high output power client to alleviate hidden node issues, what new problem are you likely to create?

a. Increased retry rates in the associated BSS

b. Increased CCI

c. Removal of encryption from the link

d. Decreased throughput on the link

10. Why are near/far problems not as common in modern capacity-based WLANs?

a. Clients have directional antennas.

b. Clients have higher gain antennas.

c. APs use low output power settings.

d. All APs now use omni antennas.

11. What kind of WLAN links are most impacted by snow and ice buildup?

a. Indoor WLAN links

b. Warehouse WLAN links

c. Outdoor bridge links

d. Indoor high-gain antenna links

12. What is a common cause of dropped calls for users with mobile Wi-Fi handsets?

a. The use of open WLANs

b. Slow roaming times

c. Lack of data rates about 150 Mbps

d. Lack of data rates below 5.5 Mbps

13. As the WLAN analyst for your organization, you must locate all wireless networks detectable on a given channel. What utility can be used to perform this operation without complicated training classes or long learning curves?

    a. A Wi-Fi scanner

    b. A spectrum analyzer

    c. A protocol analyzer

    d. WLAN controller interfaces

14. What is the one way delay time required for VoIP transmissions?

    a. 50 ms

    b. 150 ms

    c. 200 ms

    d. 300 ms

15. To what are WMM access categories mapped by autonomous APs before sending the frame on the wired link?

    a. DSCP

    b. IP Precedence

    c. CoS

    d. DiffServ

16. To what CoS is AC_VO mapped?

    a. 1

    b. 0

    c. 7

    d. 3

17. What is the default aCWmax for AC_BK?

    a. 7

    b. 15

    c. 1024

    d. 1023

18. What access category has a default aCWmin of 3?

    a. BE

    b. BK

    c. VI

d. VO

19. What tool can be used to check for security policy compliance in an environment that does not run an intrusion prevention solution?

    a. Spectrum analyzer

    b. Protocol analyzer

    c. Throughput tester

    d. NETSH

20. Why should the default SSIDs not be used?

    a. They immediately inform an attacker with no real effort of the vendor device in use.

    b. They cannot be used with WPA2-Enterprise.

    c. They cannot be used with WPA2-Personal.

    d. They reveal the password automatically

21. What is a good reason to apply a firmware update to an AP?

    a. To enable new security features and patch vulnerabilities

    b. To enable more spatial streams

    c. To disable lower data rates

    d. To enable the short-guard interval

22. What is the first step to eliminating rogue devices on a network?

    a. Disable rogue device detection in all authorized APs.

    b. Scan for rogue devices and reprimand users who have installed them.

    c. Create a clear policy against the installation of unauthorized devices.

    d. Build a list of the MAC addresses of all unauthorized devices.

23. Why might a VoIP frame not get transmitted on the wireless medium before a data frame from another STA even when WMM is used properly?

    a. Because WMM is a probabilistic QoS.

    b. Because WMM does not prioritize VoIP.

    c. Because many devices have a VoIP blind spot.

    d. Because WMM is reservation-based QoS.

24. Why does limiting the output power of an AP not guarantee that an attacker at some unexpected distance cannot connect to the WLAN?

    a. Because attackers have the ability to do things network administrators do not.

    b. Because the attacker may have an old FHSS device.

c. Because the attacker can use high output power.

d. Because high gain antennas can be used.

25. What is a good way to prevent the theft of wireless APs?

a. Mount them on the roof.

b. Mount them out of reach.

c. Mount them in the floor.

d. Cover them with aluminum casings.

Review Question Answers

1. **A** is correct. When RTS/CTS is enabled it requires an additional set of frames to be exchanged for every useful frame. This results in extra management overhead and reduced throughput.
2. **B** is correct. Even with 802.11ac 4x4:4 devices a 1 Gbps port will typically suffice due to the use of only 20 and 40 MHz channels in business deployments.
3. **C** is correct. Each SSID requires a beacon frame. If you have five SSIDs on a radio, the radio will transmit roughly five beacon frames every second. This adds significant overhead, often as much as 20% more.
4. **B** is correct. ACI can be detected when you are capturing on one channel but seeing frame from another channel.
5. **A** is correct. When you remove lower data rates, beacon frames and any other frames that must be sent at the lowest data rate allowed in the BSS will utilize less air time.
6. **A** is correct. The number of APs seen on a channel at usable signal levels is not the only factor. The utilization of the channel is also key. With low utilization a single channel may accommodate 2–4 APs at usable data rates on the same channel, though this is not preferred.
7. **D** is correct. When Wi-Fi devices, such as video transmitters and phones, are used they comply with contention rules and typically cause less interference (or degradation of throughput) than non-Wi-Fi devices operating on the same frequencies.
8. **A** is correct. Hidden nodes within the same BSS are often detected by corruption (CRC errors) at the AP and retries at the client. This is because both clients can properly hear the AP, but they cannot hear each other.
9. **B** is correct. When you enable high output power on a client device, it will increase the size of its contention domain or contention boundary.
10. **C** is correct. Because most modern business WLANs use APs with 50 mW or lower output power, near/far problems are not as common since a closer AP is typically available for the client that might traditionally suffer from this problem in a coverage design as opposed to a capacity design.
11. **C** is correct. Outdoor bridge links can be significantly impacted by snow and ice buildup as the buildup may encroach on the Fresnel zone.
12. **B** is correct. Slow roaming times can result in dropped calls because the delay time becomes too great, and the other end of the call link assumed the connection has been lost.
13. **A** is correct. A Wi-Fi scanner such as Acrylic Wi-Fi Professional or inSSIDer can be used to locate all BSSs detectable on a given channel and act as a starting point in analyzing CCI.|

14. **B** is correct. Most VoIP vendors suggest a one-way delay of 150 ms or less for effective call quality and link stability.
15. **C** is correct. WMM is a Layer 2 QoS solution so the access categories are mapped to Layer 2 class of service (CoS) values.
16. **C** is correct. AC_VO is a voice category, and it is typically mapped to wither CoS 6 or 7.
17. **D** is correct. 1023, the maximum possible, is the default aCWmax for the background (AC_BK) access category.
18. **D** is correct. AC_VO (voice) has the lowest aCWmin value by default of 3. VI uses a default of 7, and BE/BK uses a default of 15.
19. **B** is correct. Some WLAN protocol analyzers have built-in security compliance analysiseven to the point of reporting against such standards as DoD policies and PCI-DSS.
20. **A** is correct. Among the answers given, the fact that default SSIDs quickly reveal the vendor equipment type is a reason to not use default SSIDs. Additionally, using default SSIDs can be confusing to users, and SSIDs should be created to assist the users in selecting the appropriate WLAN.
21. **A** is correct. Firmware updates are often applied to provide new security features and to patch discovered vulnerabilities. They cannot add any chipset dependent features in most cases as these features are either in the chipset or not.
22. **C** is correct. As with any security measure, it is important to begin by creating security policies against which security configurations can be audited.
23. **A** is correct. WMM is probabilistic and not guaranteed. Therefore, at any moment, a standard data frame may gain access to the medium before a VoIP from another station can. However, it provides increased statistical probability that the voice frames will gain access to the medium more often than lower priority frames.
24. **D** is correct. An attacker can utilize a high-gain antenna and connect to a WLAN well beyond the point where a standard client device may be able to gain access. Remember, as you learned earlier in this book, the SNR impacts the available data rates, and a higher gain antenna will result in a better SNR at a given location due to the gain given to the signal by the antenna before it enters the radio.
25. **B** is correct. It is important to mount APs in proper locations, which mean not on the roof or in the floor (except in some unique high-density deployments) or in aluminum casings. But mounting them out of reach will diminish theft due to the lack of ease of access.

Appendix A:

Installing WLAN Analysis Software

Installing Wireshark

Wireshark is one of the most popular open source network packet analyzers, which enables the network engineer to capture and analyze network data packets to understand network performance details and troubleshoot common problems. The Wireshark packet analyzer has multiple uses, such as:

- Troubleshooting network problems
- Examining network security problems
- Learning about network protocols
- Debugging protocol implementation

Wireshark is available for both Linux and Windows operating systems and enables you to perform the various functions, some of which are given below:

- Capture live packet data from various types of network interfaces.
- Open packet files that have been captured using various other packet capture applications, such as tcpDump or Windump.
- Import packets from text files.
- Export packets to various packet-capture formats.
- Display detailed protocol information from the packet.

System Requirements:

For Windows installation you will need the following;

- Any version of Windows operating system, such as Windows 10, 8, 7, Vista, Server 2012 R2, Server 2012, Server 2008 R2, and Server 2008.
- Any modern 64-bit AMD64/x86-64 or 32-bit x86 processor.
- 400 MB available RAM, as larger capture files require more RAM.
- 300 MB available disk space, as capture files require additional disk space.
- 1024×768 (1280×1024 or higher recommended) resolution with at least 16-bit color.
- A supported network card for capturing both Ethernet and 802.11 packets:
    - For Ethernet, any card supported by Windows should work.
    - For 802.11, refer to the Wireshark wiki page. Capturing raw 802.11 information may be difficult without special equipment.

To install Wireshark (both source and binary files), the latest version can be downloaded from the following web page:

1. Click the `www.wireshark.org/download.html` to display the web page as shown in the following figure. The web page displays the current stable release.

Figure A-1: Download Wireshark Webpage

2. Click on the link to download the installation files for the platform you want (Windows or OS).

   The system starts to download the latest installer package, such as **Winshark-win64-2.0.0.exe**, for the operating system you have selected. The installer package contains the WinPcap functionality that is used for packet capture.

   The system saves the Wireshark installer package at the location you have specified.

3. Start the installation by double-clicking the **Wireshark-win64-2.0.0** installer package, as shown in the following figure.

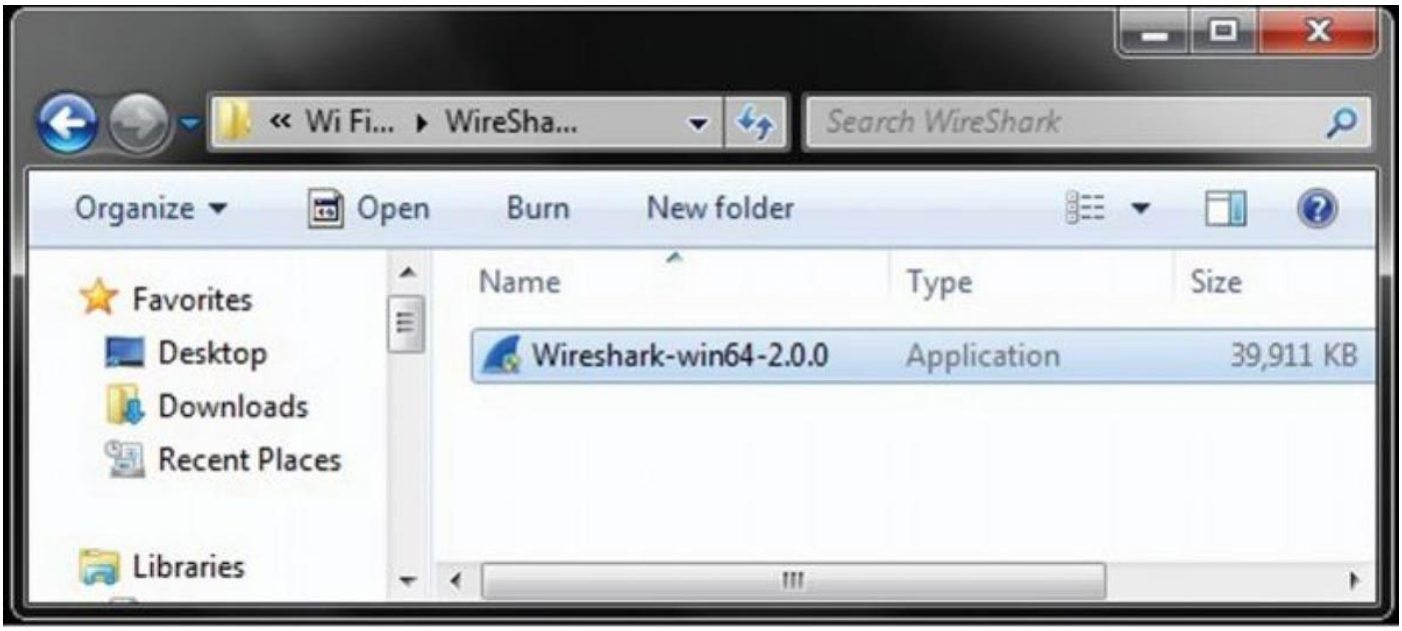


Figure A-2: Wireshark Installer Package

The system starts the Wireshark installation wizard and displays the **Welcome to the Wireshark 2.0.0 (64 bit) Setup Wizard** screen, as shown below.

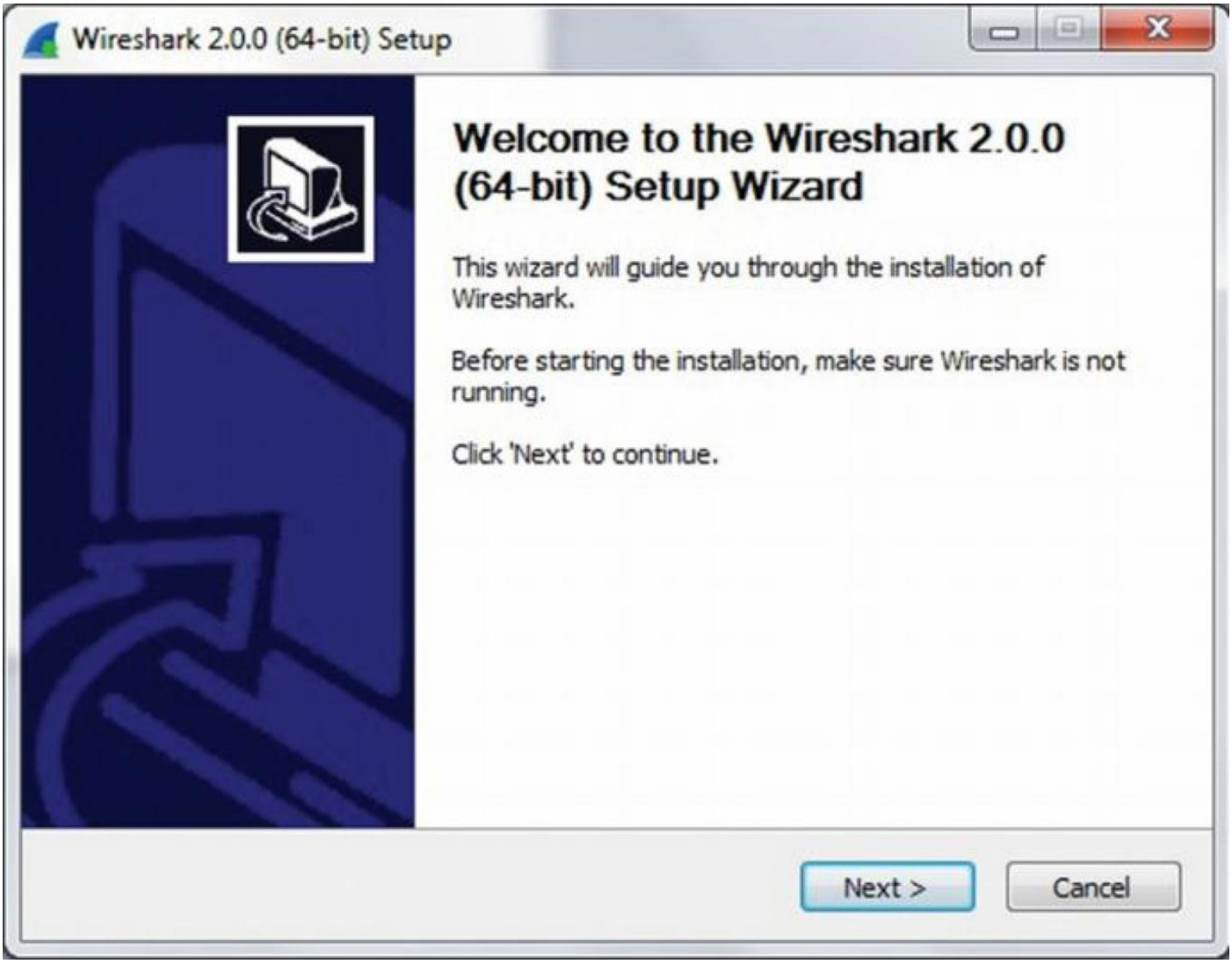


Figure A-3: Welcome to the Wireshark 2.0.0 (64 bit) Setup Wizard Screen

4. Click the **Next** button to display the **License Agreement** screen, as shown in the following figure.

Figure A-4: License Agreement Screen

5. Click the **I Agree** button to accept the license terms and conditions associated with the installation and use of Wireshark application. Clicking the **I Agree** button displays the **Choose Components** screen, as shown in the following figure.

Figure A-5: Choose Components Screen

6. Select the required components, as explained below in this table, from the **Choose Components** screen of the installation wizard, and click the **Next** button.

Component	Description
Wireshark	The network protocol analyzer.
TShark	The command-line network protocol analyzer.
Wireshark 1 Legacy	The previously used (GTK+) user interface.
Plugins & Extensions	Extra functionalities for the Wireshark and TShark dissection engines: ■ Dissector plugins (plugins with some extended dissections) ■ Tree Statistics plugins (for extended statistics) ■ Mate (Meta Analysis and Tracing Engine, which is a user-configurable extension(s) of the display filter engine) ■ SNMP MIBs (For a more detailed SNMP dissection)
Tools	The tools that you can use to work with capture files: ■ Editcap (reads a capture file and writes some or all of the packets into another capture file) ■ Text2Pcap (reads in an ASCII hex dump and writes the data into a pcap capture file. ■ Reordercap (reorders a capture file by timestamp) ■ Mergecap (combines multiple saved capture files into a single output file) ■ Capinfos (provides information on capture files) ■ Rawshark (Raw packet filter)
User Guide	Wireshark user guide.

7. Click the **Next** button to display the **Select Additional Tasks** screen, as shown in the following figure.

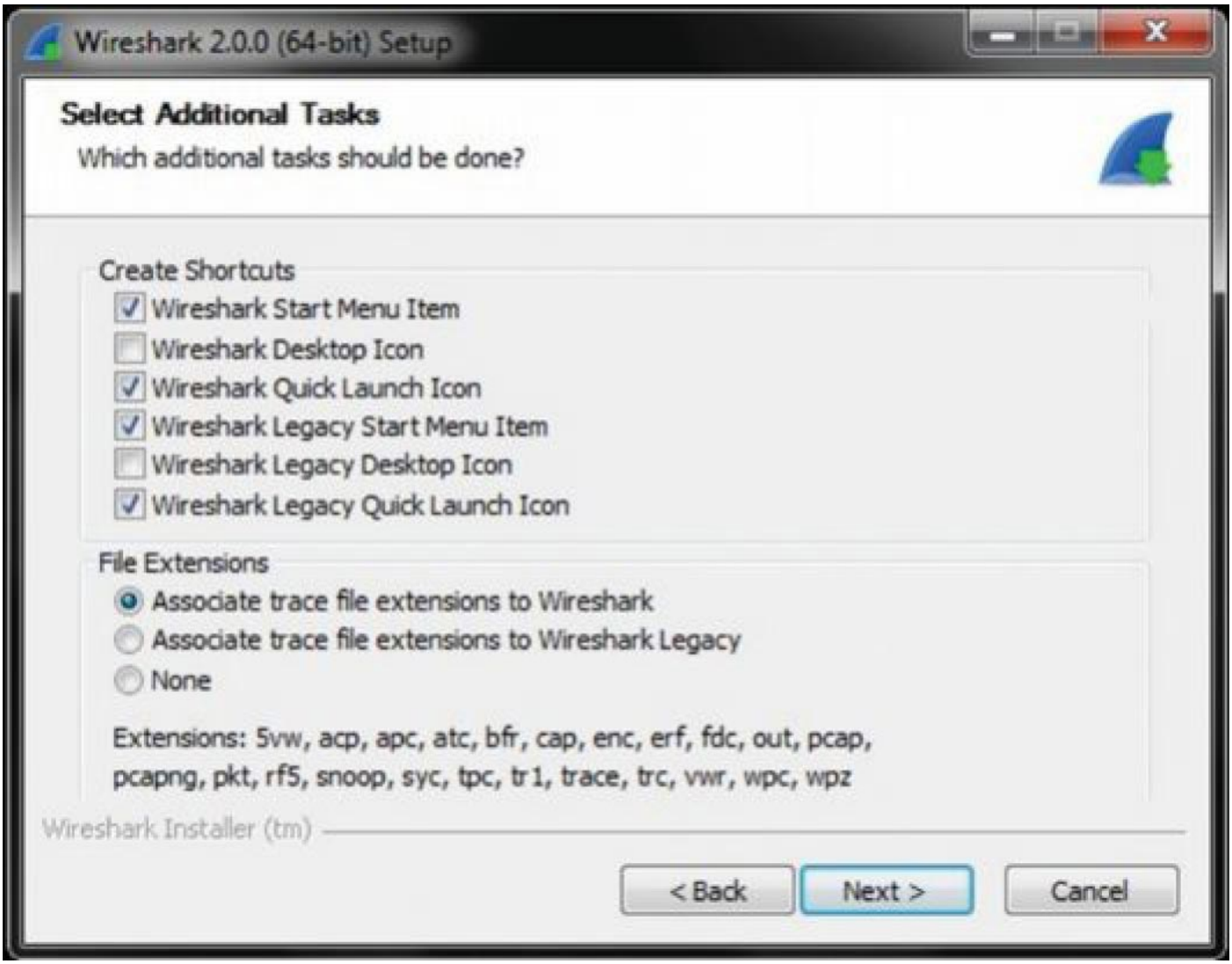


Figure A-6: Select Additional Tasks Screen

Select the required shortcuts you want the system to create, and select the required option for the file extensions. Some of the shortcut types are selected by default, as shown in the above figure.

8. Click the **Next** button to display the Choose Install Location screen, as shown in the following figure.

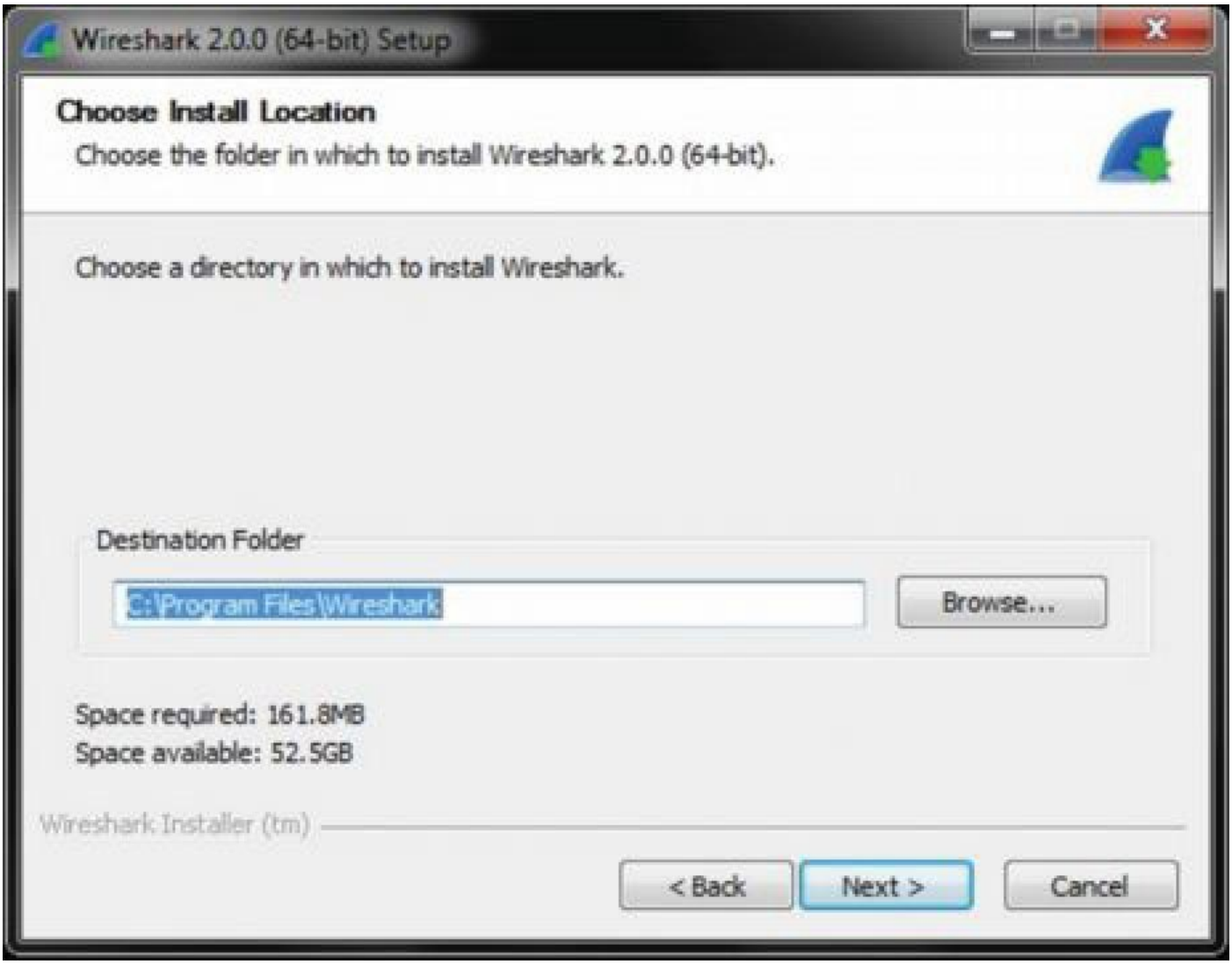


Figure A-7: Select Additional Tasks Screen

Specify the folder and the path to install the Wireshark application, in the **Destination Folder** text box. Alternatively, you can click the **Browse** button to select the folder and the path to install the Wireshark application.

9. Click the **Next** button to display the **Install WinPcap ?** screen, as shown in the following figure.

Figure A-8: Install WinPcap ? Screen

The **Install WinPcap 4.1.3** checkbox is selected by default. If you do not want to install this application, uncheck the **Install WinPcap 4.1.3** checkbox.

10. Click the **Next** button to display the **Install USBPcap ?** screen, as shown in the following figure.

Figure A-9: Install USBPcap ? Screen

Select the **Install USBPcap 1.1.0.0-g794bf26** check box to install the USBPcap application.

11. Click the **Install** button to display the installation process of the Wireshark application, as shown in the following figures.

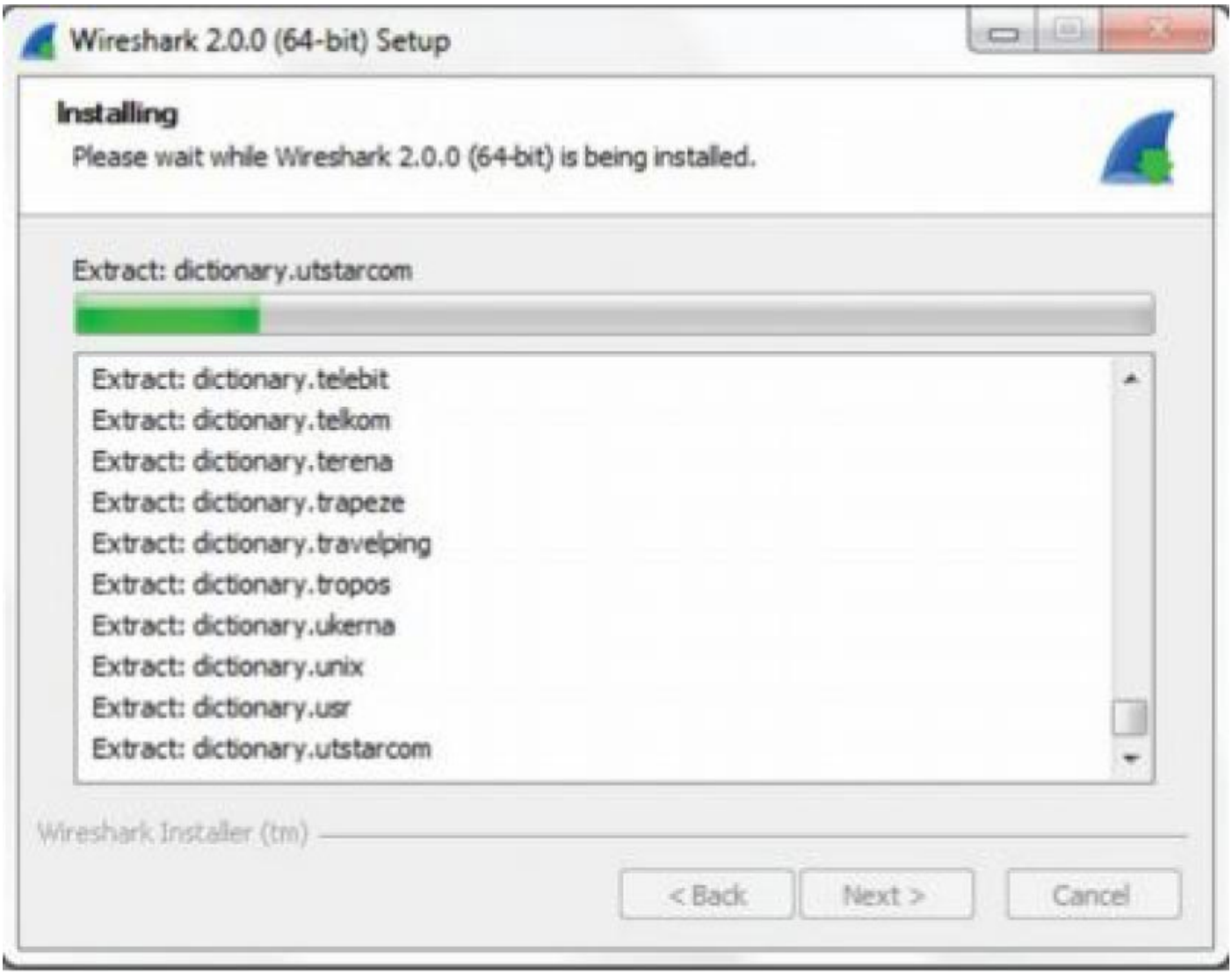


Figure A-10: Installing Screen

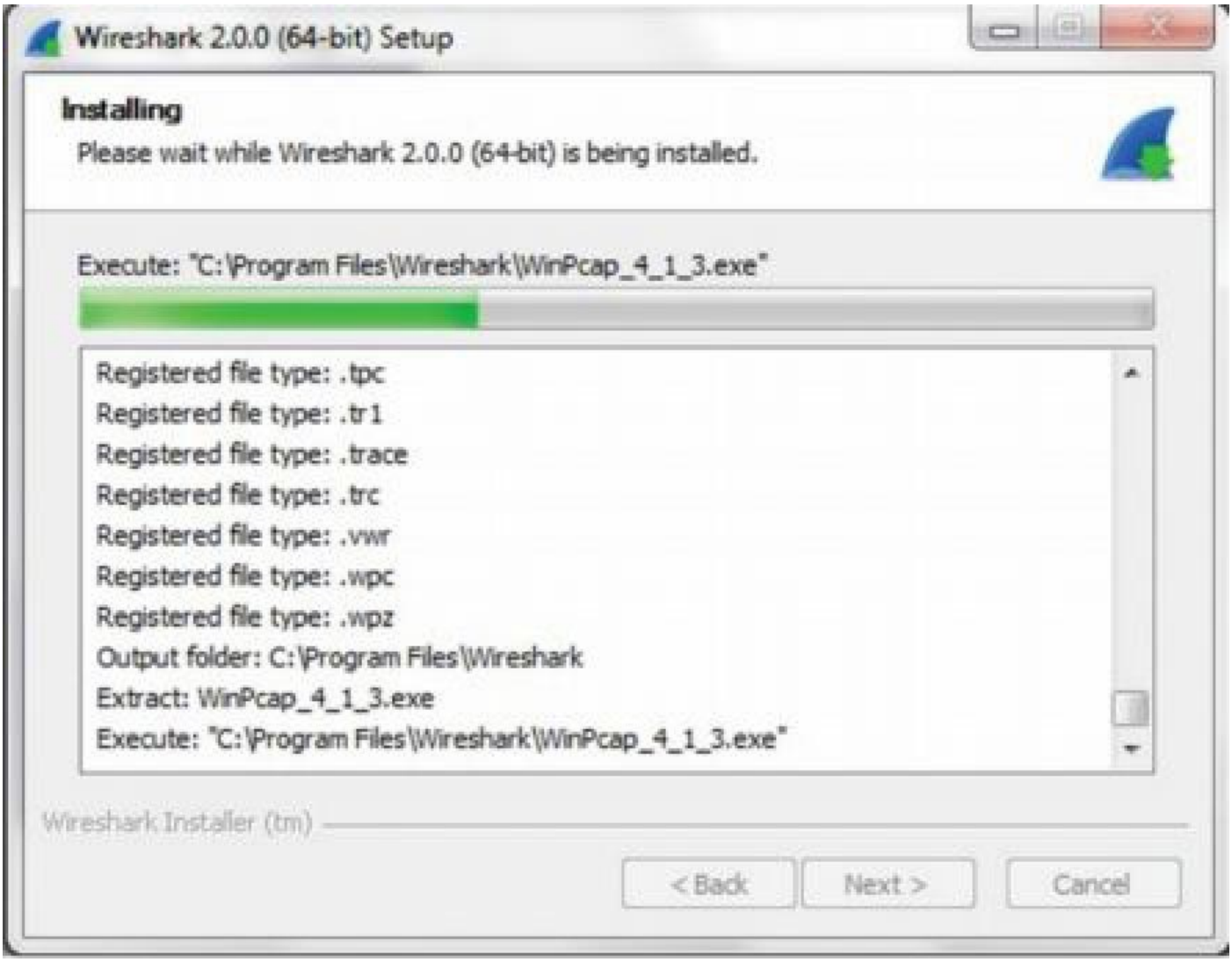


Figure A-11: Installing Screen

The Wireshark installation process automatically starts the installation of the WinPcap 4.1.3 application and displays the **Welcome to the WinPcap 4.1.3 Setup Wizard** screen, as shown in the following figure.

Figure A-12: Welcome to the WinPcap 4.1.3 Setup Wizard Screen

12. Click the **Next** button to start the installation of the WinPcap application. Clicking the **Next** button displays the **License Agreement** screen, as shown in the following figure.

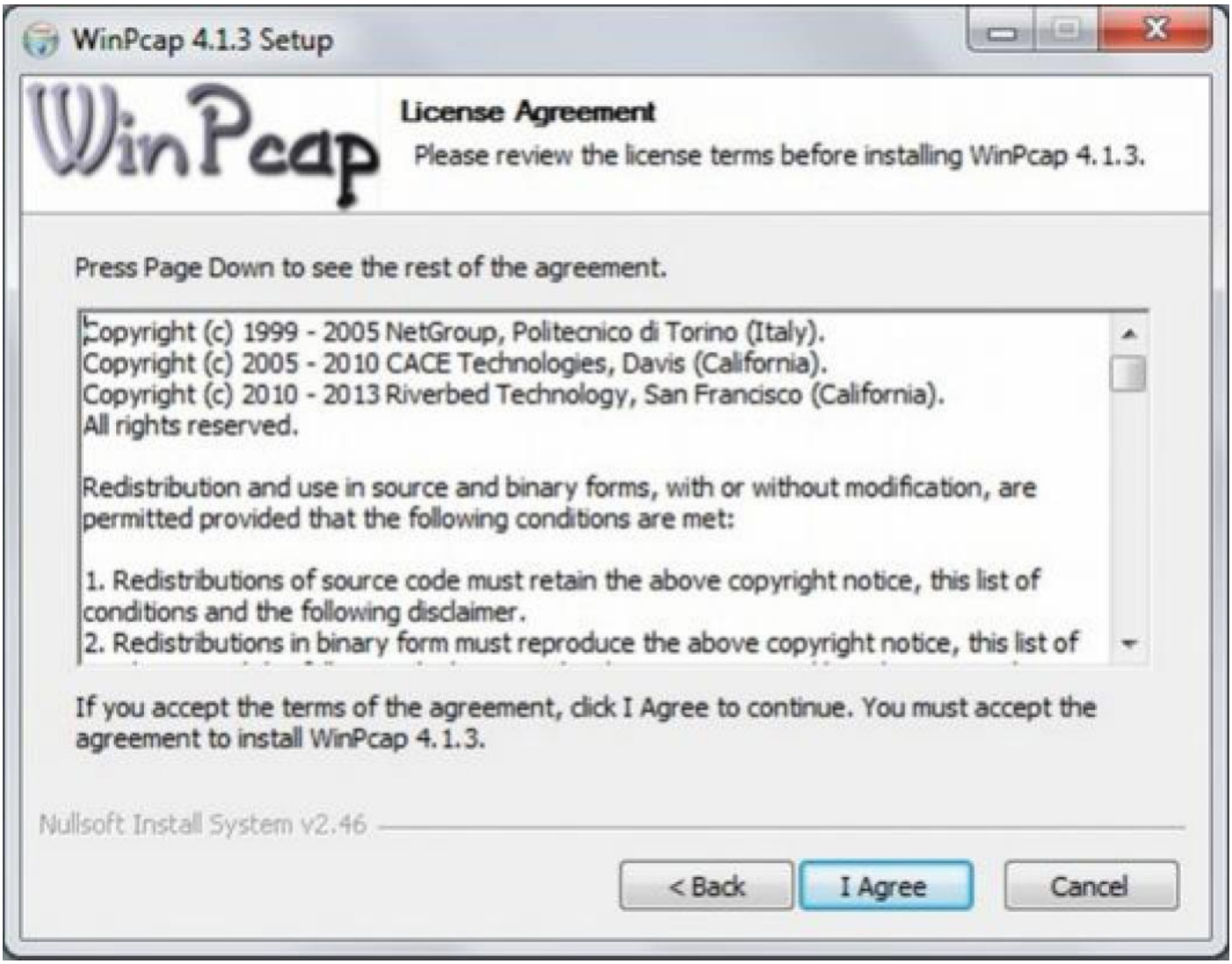


Figure A-13: License Agreement Screen

13. Click the **I Agree** button to accept the license terms and conditions and to start the installation of the WinPcap application. Clicking the **I Agree** button displays the **Installation options** screen, as shown in the following figure.

Figure A-14: Installation Options Screen

Click the **Install** button to start the installation process, and to display the **Installing** screen, as shown in the following figure.

Figure A-15: Installing Screen

The **Installing** screen displays the progress of the WinPcap installation process. After the WinPcap installation process is complete, the system displays the **Completing the WinPcap 4.1.3 Setup Wizard** screen, as shown in the following figure.

Figure A-16: Completing the WinPcap 4.1.3 Setup Wizard Screen

14. Click the **Finish** button, and the system automatically returns you to the Wireshark installation processes and displays the **Installation Complete** screen, as shown in the following figure.

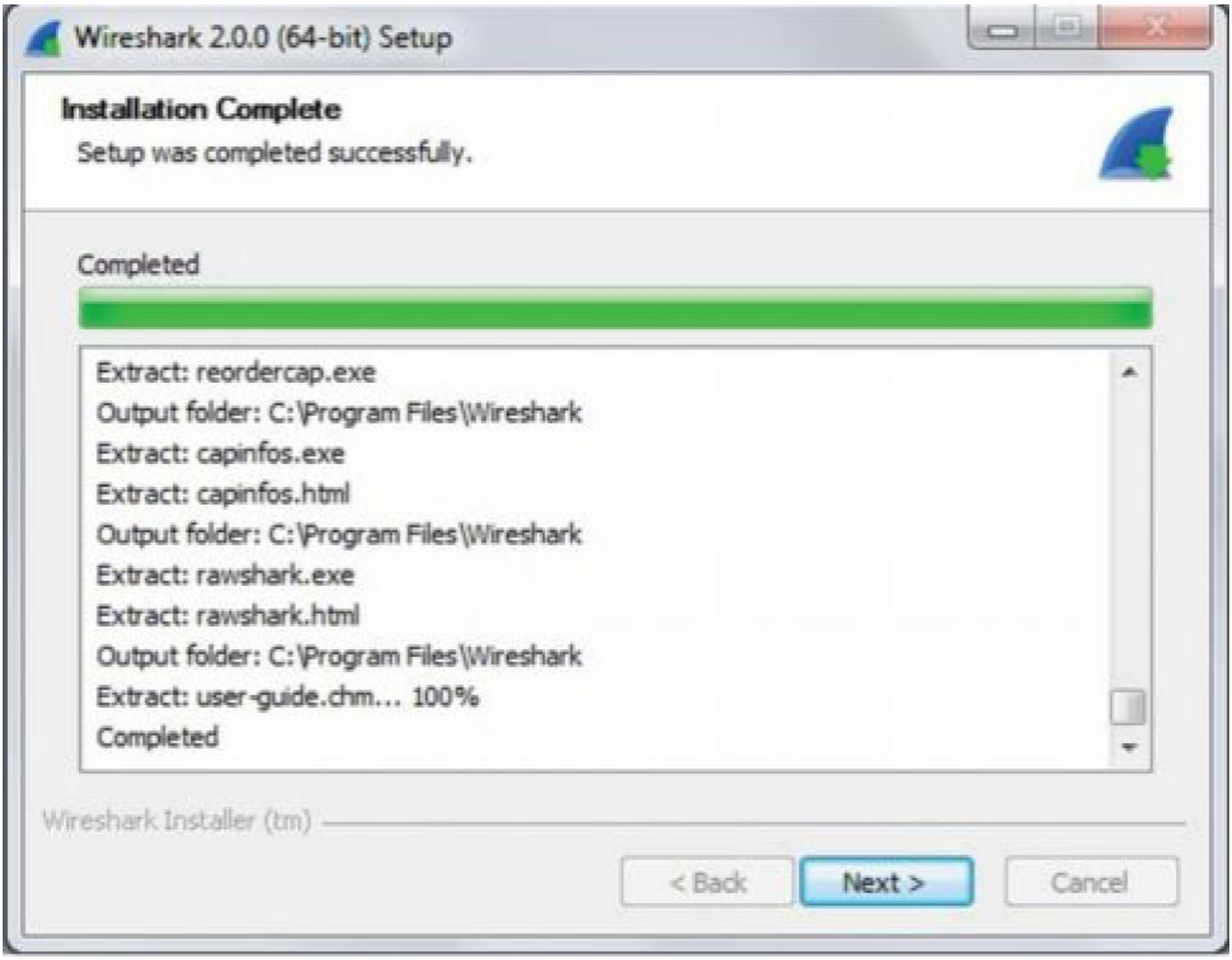


Figure A-17: Completing the WinPcap 4.1.3 Setup Wizard Screen

15. Click the Next button to display the Completing the Wireshark 2.0.0 (64-bit) Setup Wizard screen, as shown in the following figure.

Figure A-18: Completing the Wireshark 2.0.0 Setup Wizard Screen

16. Click the **Finish** button to complete the installation process.
17. Click the **Start** button to display the list of available programs and applications, and you can see the newly installed Wireshark application, as shown in the following figure.

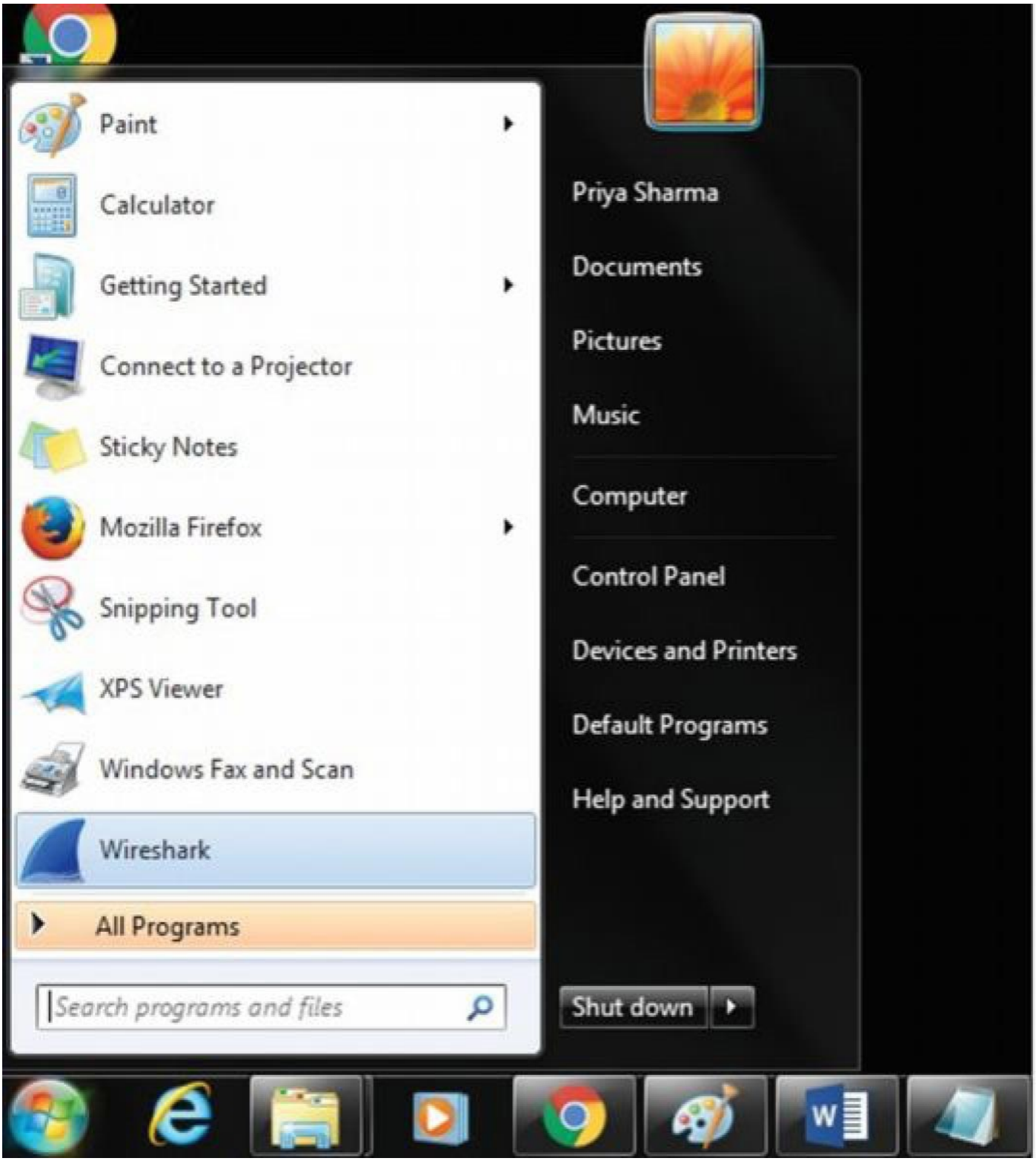


Figure A-19: The Start Menu with the Newly Installed Wireshark Application

Installing CommView for WiFi

This appendix is provided as an example of a commercial product installation procedure and is not an endorsement for this product over another. CommView is a network monitoring and analyzing application and is available in following two flavors:

- Commview for Ethernet network (Standard edition)
- Commview for Wireless 802.11 networks (CommView for WiFi)

For the purpose of this document, we will discuss the CommView for WiFi application. CommView for WiFi is a network monitor and analyzer application for all types of wireless networks, namely 802.11 a/b/g/n/ac. CommView application captures every packet being transmitted wirelessly and provides important network information, such as access points, stations, signal strength, network connections, list of packets, protocol used, protocol distribution charts, and so on. This network information enables you to identify and troubleshoot network problems.

CommView for WiFi supports more than 100 network protocols, which enables you view all the details of the captured packet, using a tree structure that includes protocol layers and packet headers.

CommView for WiFi is an effective tool to analyze network traffic and can be used by:

- WLAN administrators
- Wireless LAN security professionals
- Users who are interested in monitoring their WLAN traffic
- Programmers developing software for wireless networks

You can perform the following tasks using CommView for WiFi:

- Scan the air for Wi-Fi stations and access points.
- Capture 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac WLAN traffic.
- Specify WEP or WPA keys to decrypt encrypted packets.
- View detailed per-node and per-channel statistics.
- View detailed IP connections statistics: IP addresses, ports, sessions, etc.
- Reconstruct TCP sessions.
- Configure alarms that can notify you about important events, such as suspicious packets, high bandwidth utilization, unknown addresses, rogue access points, etc.
- View protocol charts and monitor bandwidth utilization.
- Browse captured and decoded packets in real time.
- Search for strings or hex data in captured packet contents.
- Log individual or all packets to files.
- Load and view capture files offline.
- Import and export packets in Sniffer®, EtherPeek™, AiroPeek™, Observer®, NetMon, Tcpdump, hex, and text formats.
- Export any IP address to SmartWhois for quick, easy IP lookup.
- Capture data from multiple channels simultaneously using several USB adapters.
- Capture A-MPDU and A-MSDU packets.
- Simulate access points.

To use this product, you need to purchase it by specifying the package desired at:

www.tamos.com/order/

The following figure shows the above web page with CommView for WiFi application highlighted.

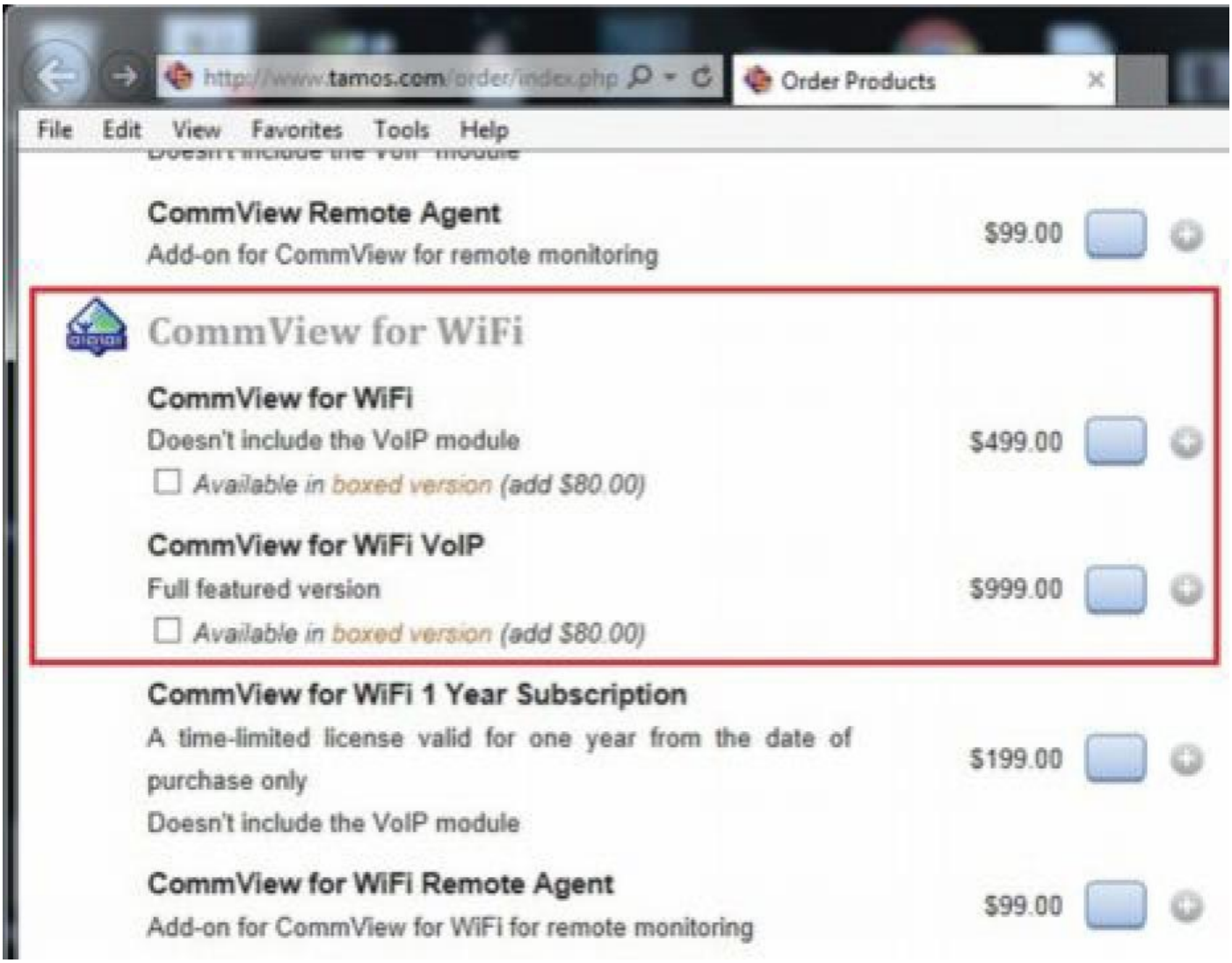


Figure A-20: Link to Purchase CommView for WiFi

If you do not want to purchase this application before trying it, you can download an evaluation version from the following web page:

www.tamos.com/download/main/index.php

Select CommView for WiFi for download by clicking on the download sign adjacent to it, as shown in the following figure.

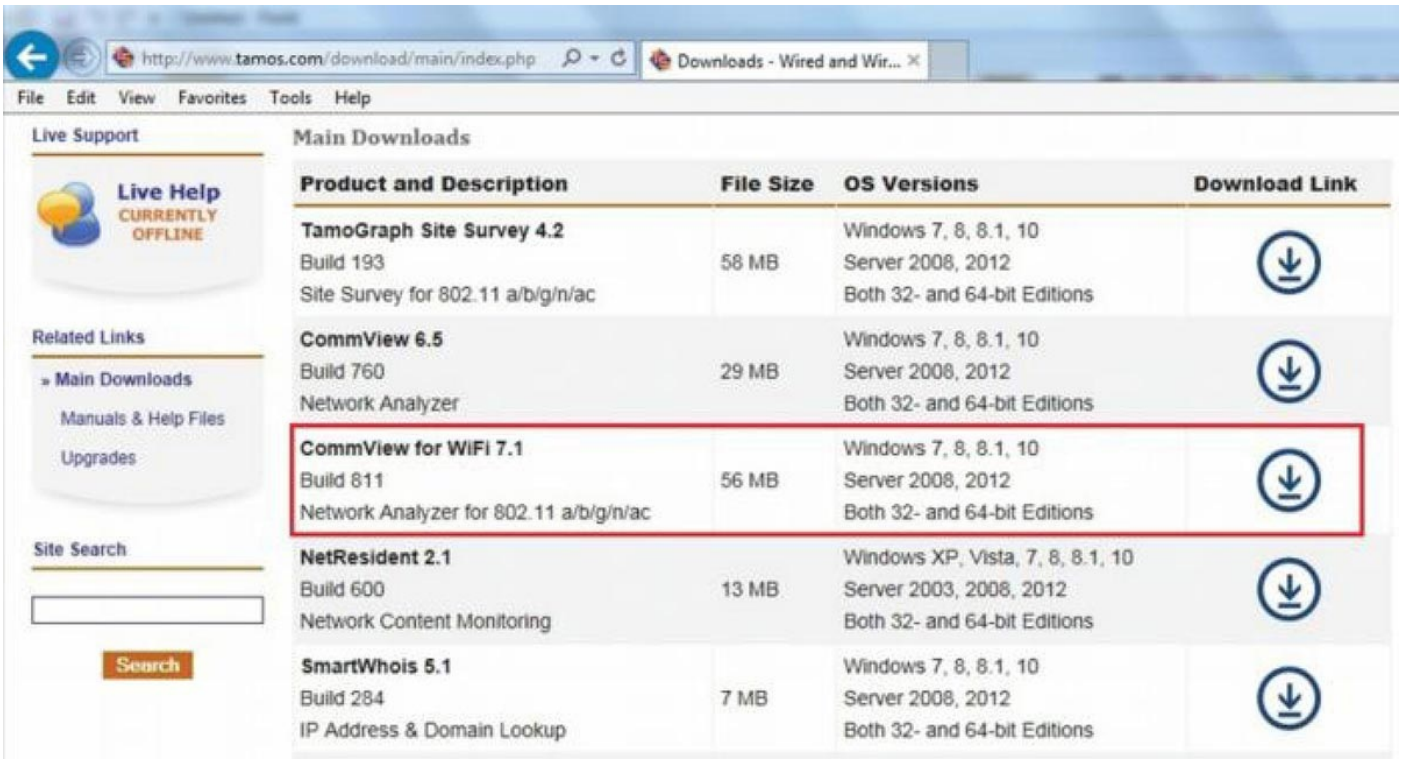


Figure A-21: Link to Download CommView for WiFi

After you have downloaded the CommView for WiFi application, the steps to install this application are as follows:

1. Double-click the **Setup** application file, as shown in the following figure.

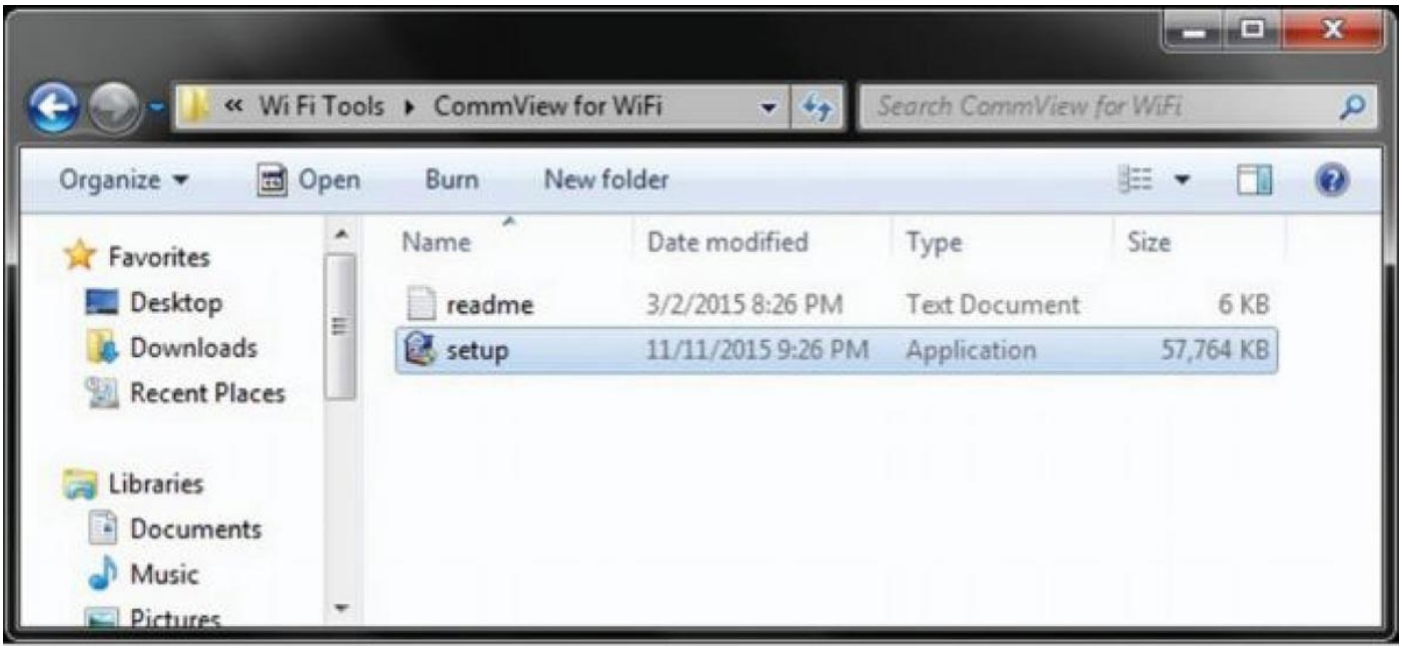


Figure A-22: CommView for WiFi Setup Application File

2. Clicking the **Setup** application file, displays the checking the system configuration message box, as shown in the following figure.

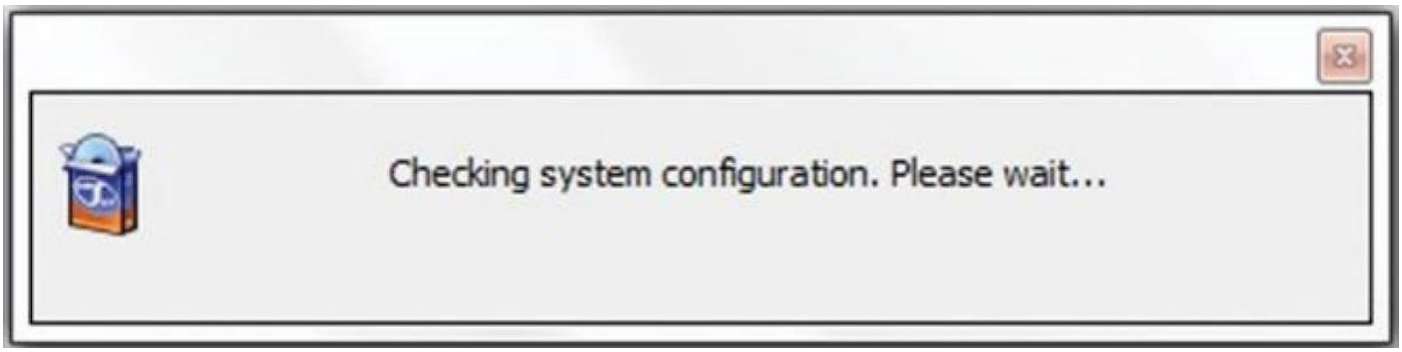


Figure A-23: CommView for WiFi Installation Message Box

The system checks for the configuration required to install CommView for WiFi and closes the message box, to display the **Welcome to the CommView for WiFi Setup Wizard** screen, as shown in the following figure.

Figure A-24: Welcome to the CommView for WiFi Setup Wizard Screen

3. Click the **Next** button to start the installation process, and display the **License Agreement** screen, as shown in the following figure.

Figure A-25: License Agreement Screen

4. Select the I accept the terms in the license agreement option, as shown in the following figure.

Figure A-26: License Agreement Screen with the "I accept…" Option Selected

Selecting the I accept the terms in the license agreement option enables the Next button.

5. Click the **Next** button to display the **License Type** screen, as shown in the following figure.

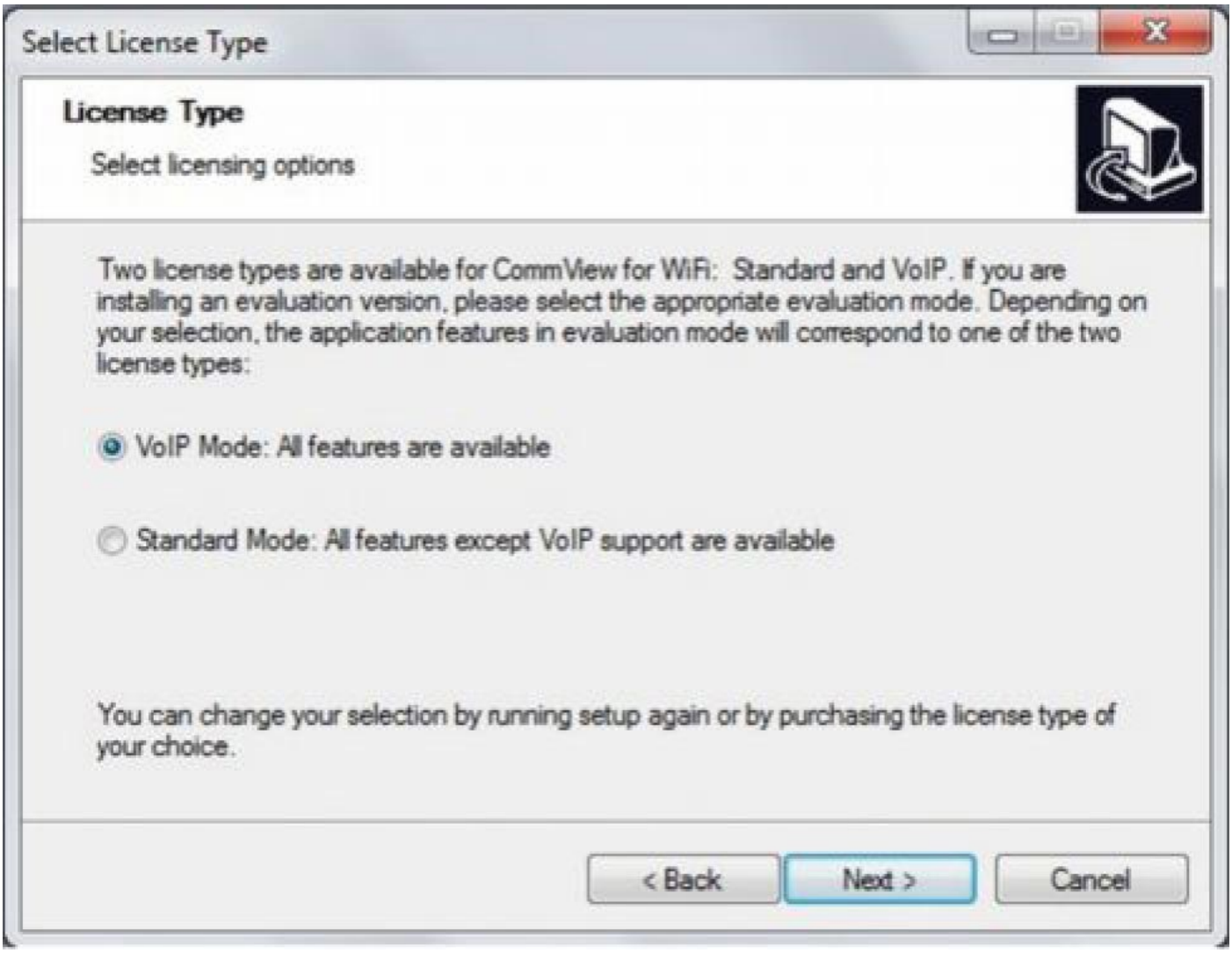


Figure A-27: License Type Screen

The **VoIP Mode: All features are available** option is selected by default. You can select the **Standard Mode** option, if required.

Click the **Next** button to display the **Destination Folder** screen, as shown in the following figure.

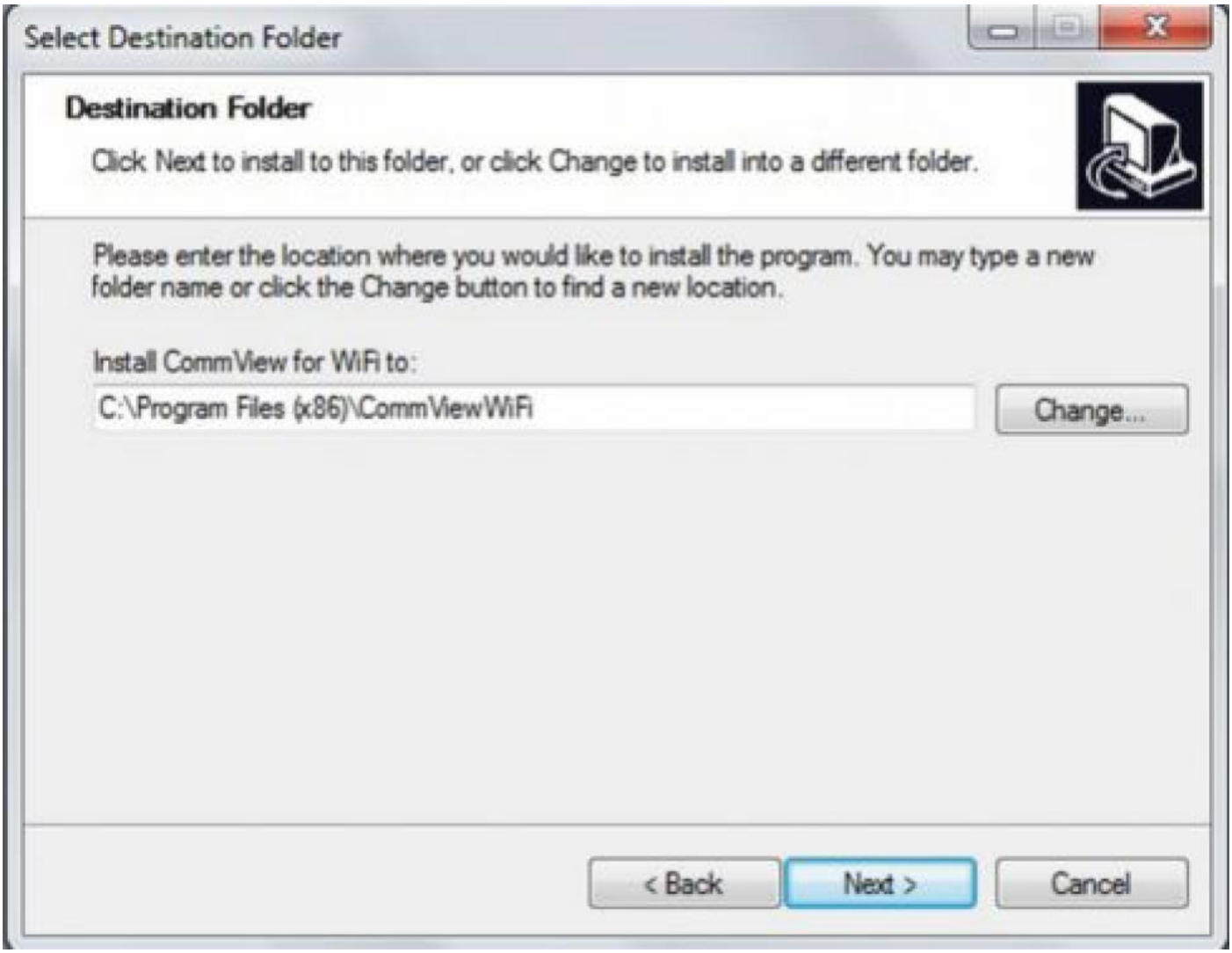


Figure A-28: Destination Folder Screen

6. Specify the folder in which you would like to store the CommView for WiFi application files. By default the folder location is specified as shown in the following figure. If you want to change the folder location, click the **Change** button to display the **Select Folder** dialog box. Select the folder location and click the **Open** button to close the **Select Folder** dialog box. The system displays the selected folder location in the **Install CommView for WiFi to:** text box.
7. Click the **Next** button to display the **Additional Settings** screen, as shown in the following figure.

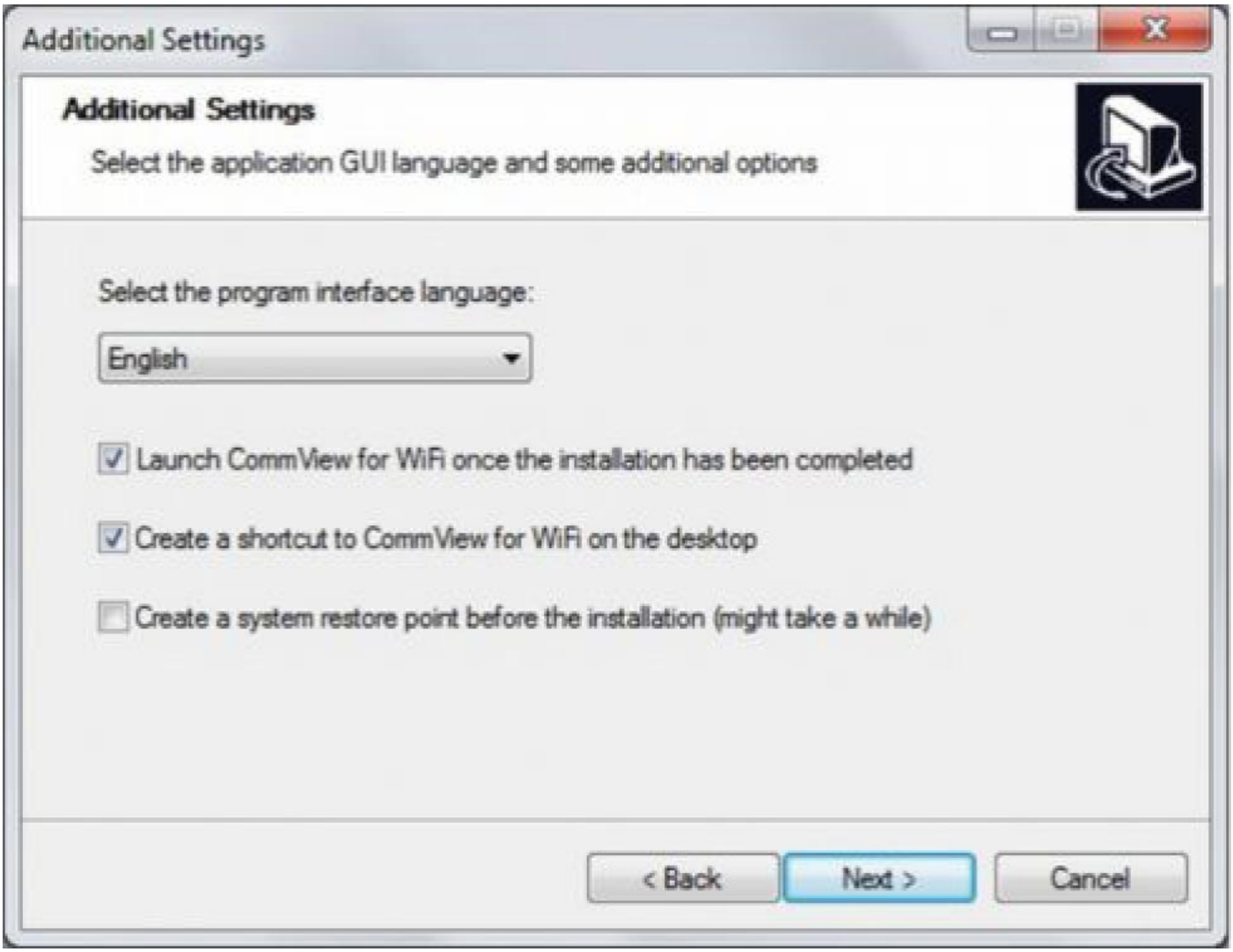


Figure A-29: Additional Settings Screen

8. Select the program interface language as per your requirements, and allow the system to create a shortcut on completion of the installation process. Two of the additional settings are selected by default.

9. Make the changes as per your requirements, and click the **Next** button to display the **Ready to Install the Program** screen, as shown in the following figure.

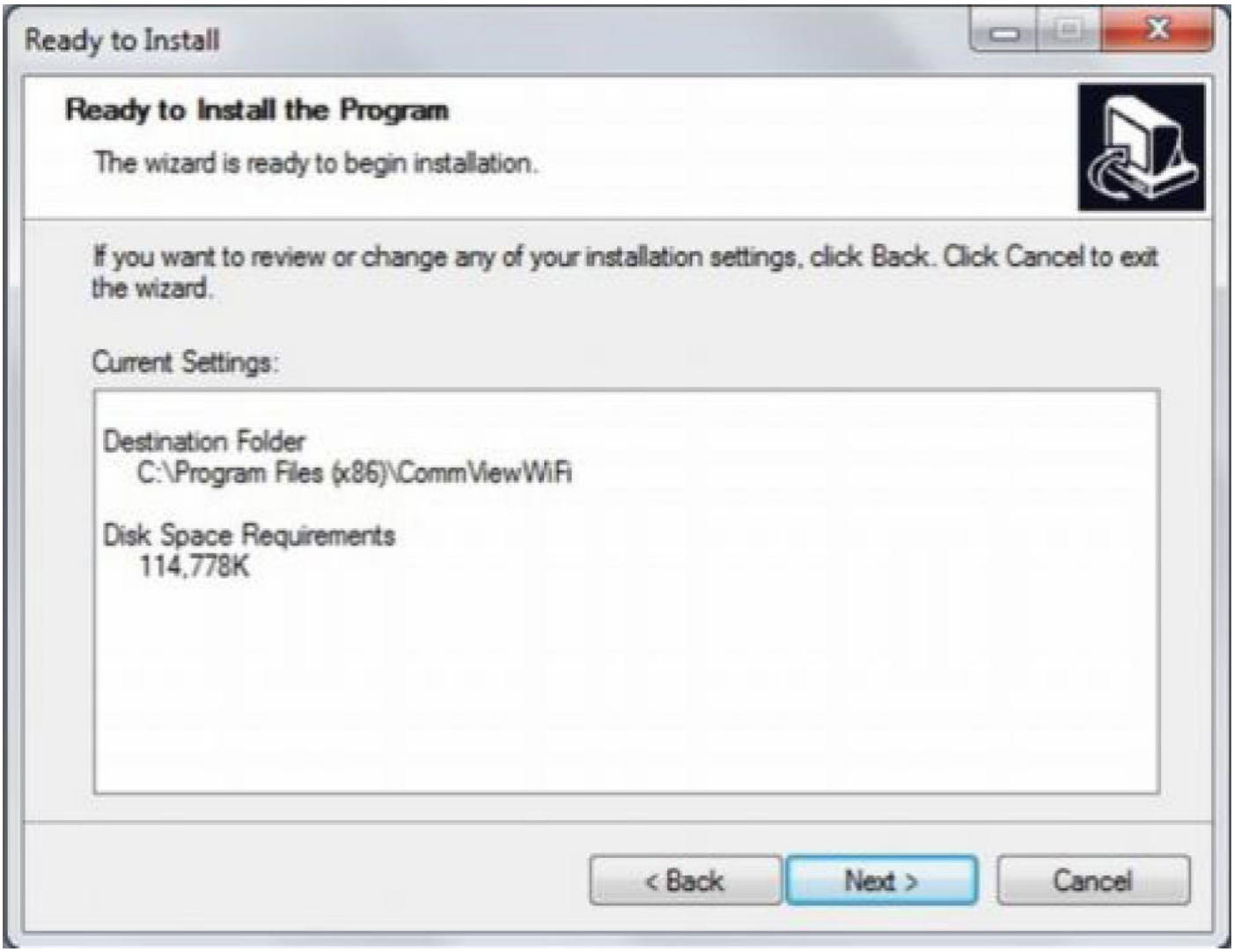


Figure A-30: Additional Settings Screen

The **Ready to Install the Program** displays the current settings, which include the destination folder and the disk space requirements.

10. Click the **Next** button to start the installation process, as shown in the following figure.

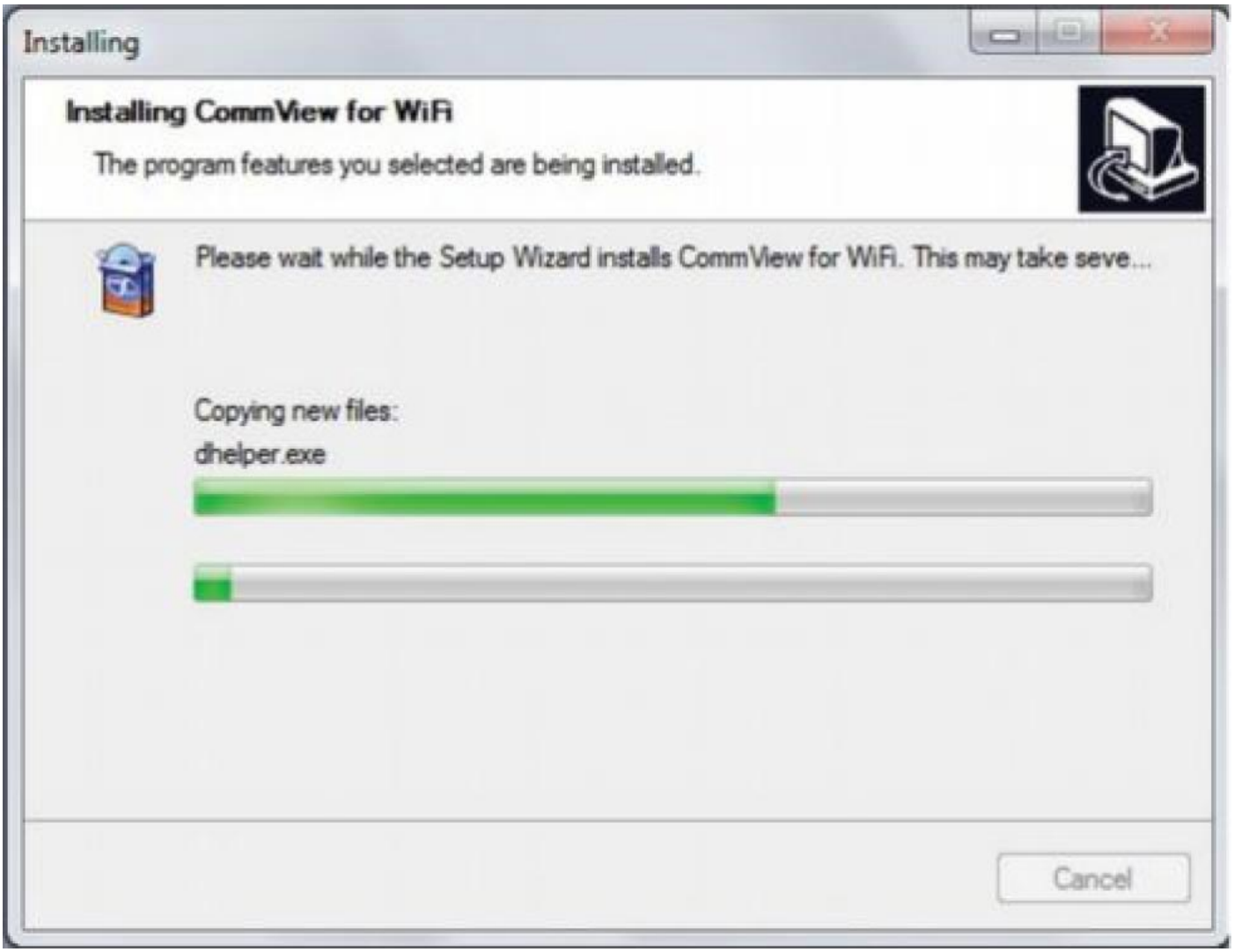


Figure A-31: Installing CommView for WiFi Screen

The system installs the CommView for WiFi application and displays the **Setup Complete Wizard** screen on completion of the installation process, as shown in the following process.

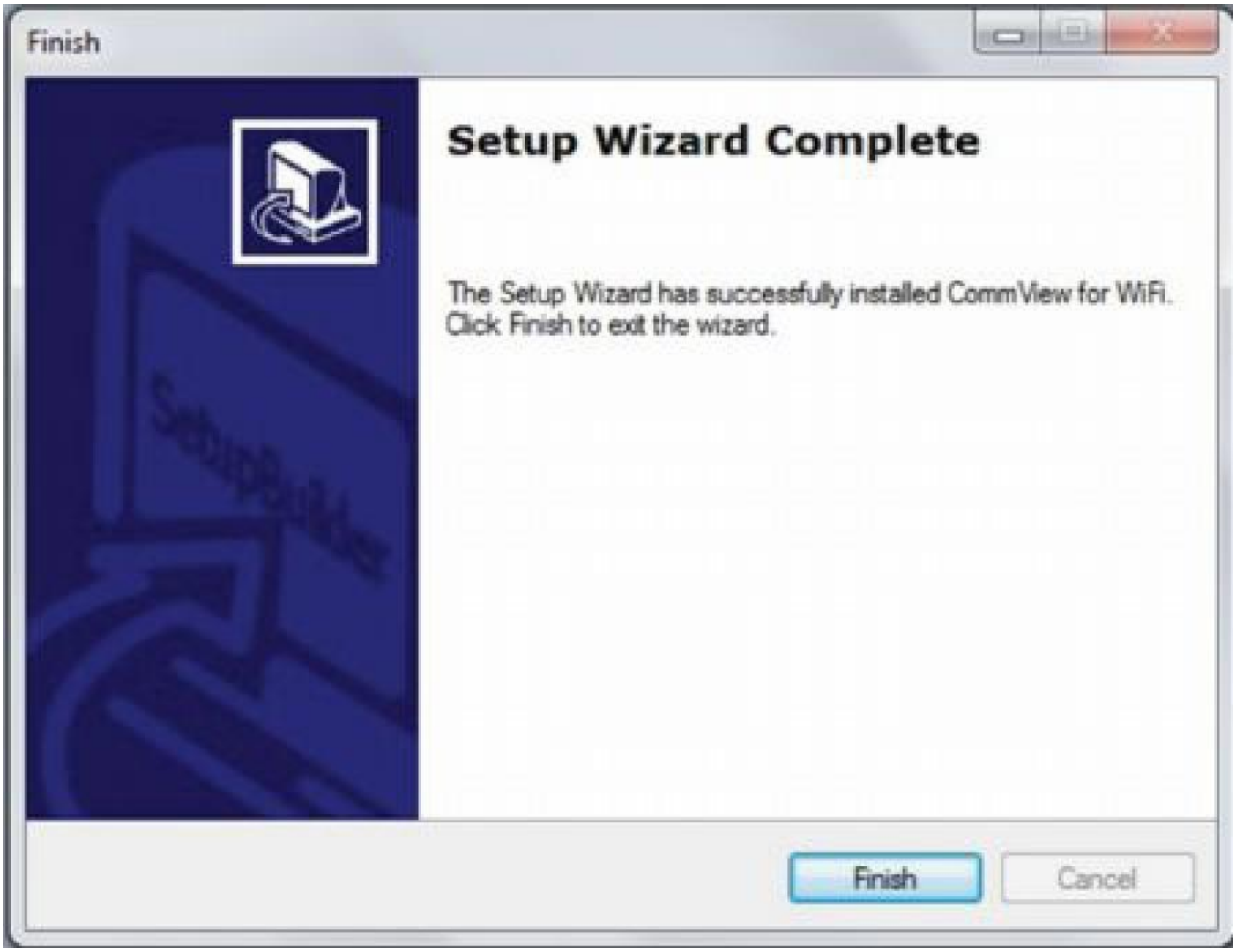


Figure A-32: Setup Wizard Complete Screen

11. Click the **Finish** button to complete the installation process. After the installation process is complete, the system automatically displays the Driver Installation screen, as shown in the following figure.

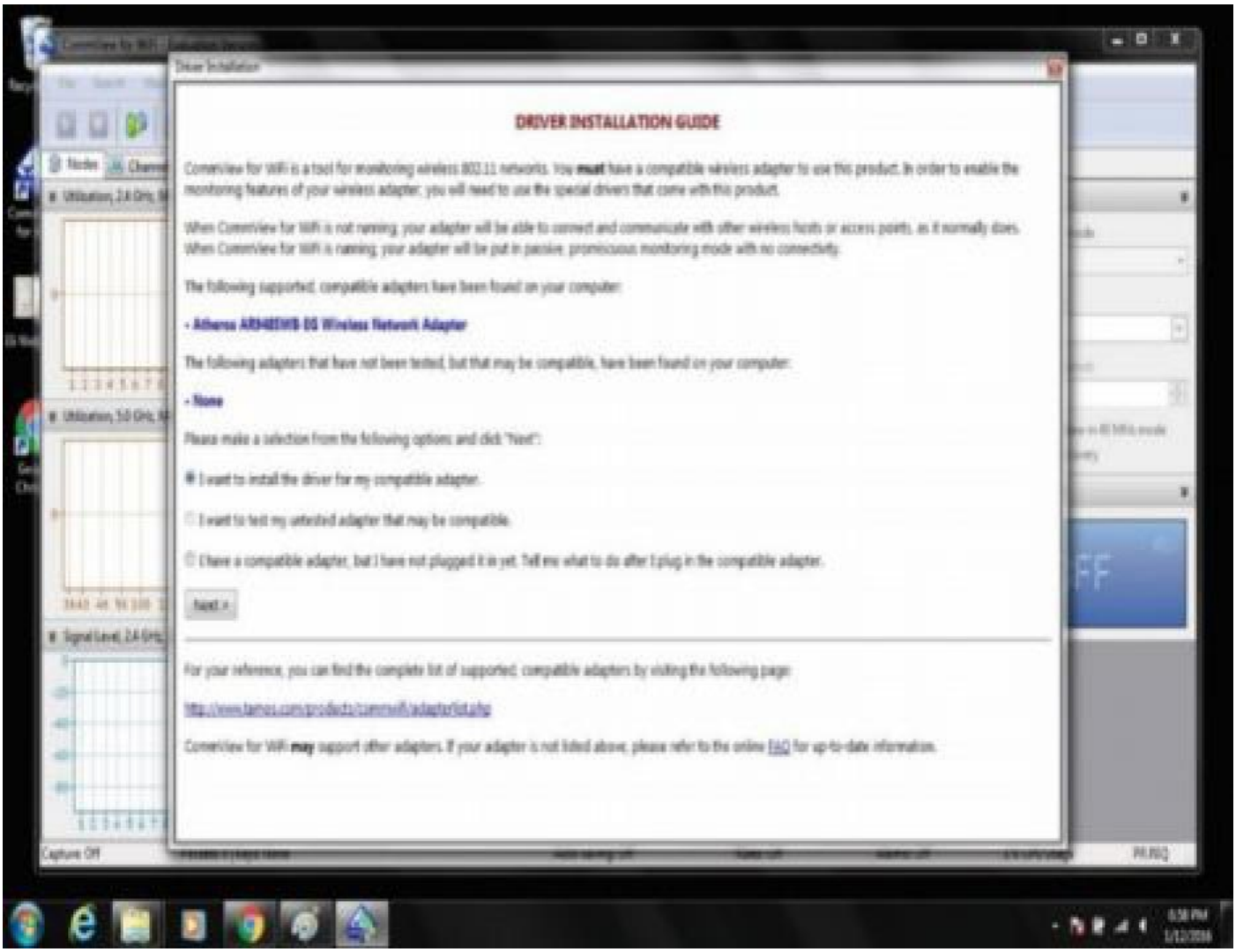


Figure A-33: Driver Installation Screen

The system displays the name of the adapters found in its configuration, which is compatible to CommView for WiFi application along with the list of adapters found in its configuration, but are not compatible with this application. Also, the system displays the action you can perform on these drivers. By default, the **I want to install the driver for my compatible adapter** option is selected.

12. Click the **Next** button to install the driver for the compatible adapter and display the **Driver Installation** screen, as shown in the following figure.

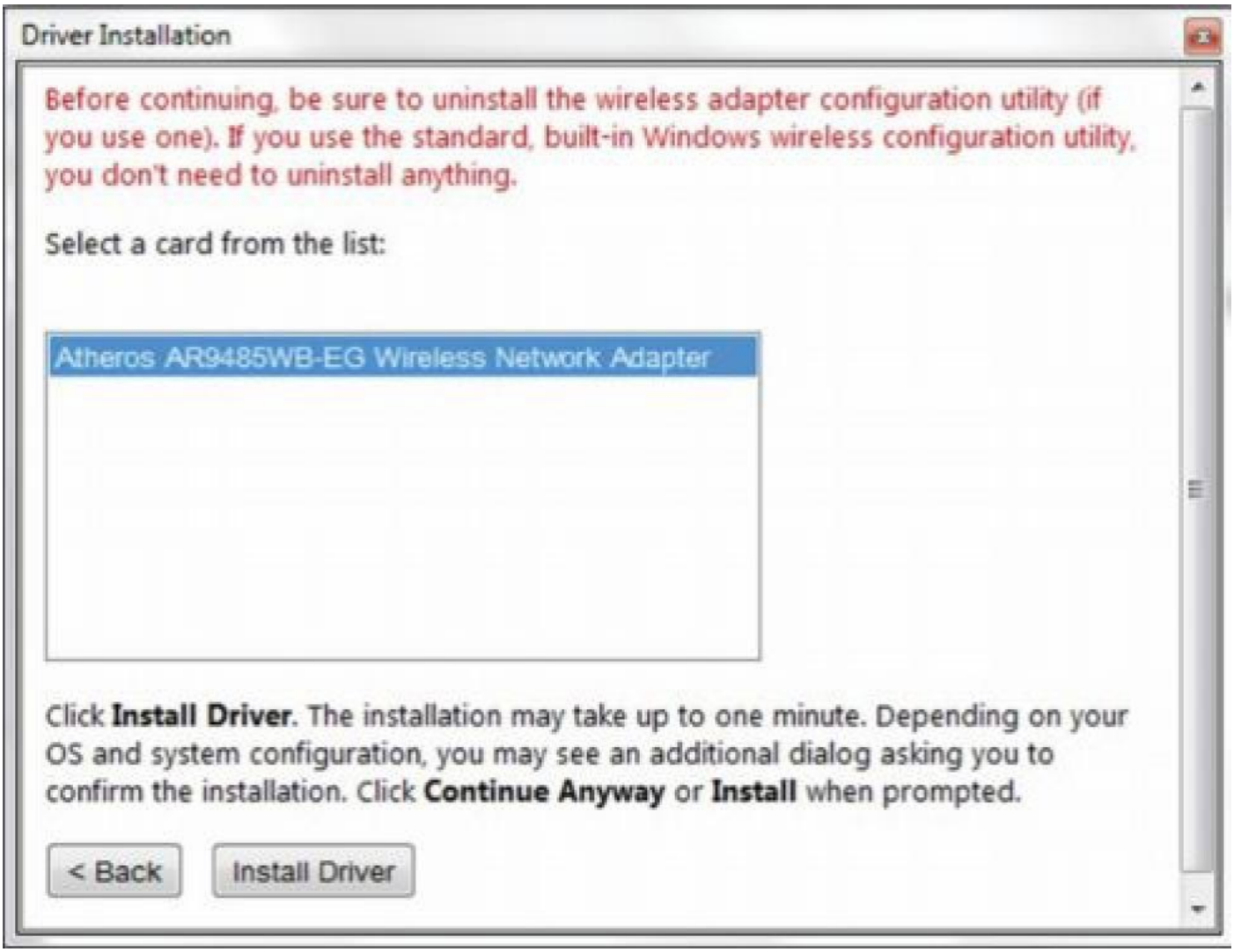


Figure A-34: Driver Installation Screen

The system displays the available network adapter in the **Select a card from the list:** list box with the available network adapter.

13. Click the **Install Driver** button.

    Clicking the **Install Driver** button starts the installation of the required driver. The system displays the **Driver Installation – Installation Complete** screen after the driver installation is complete, as shown in the following figure.

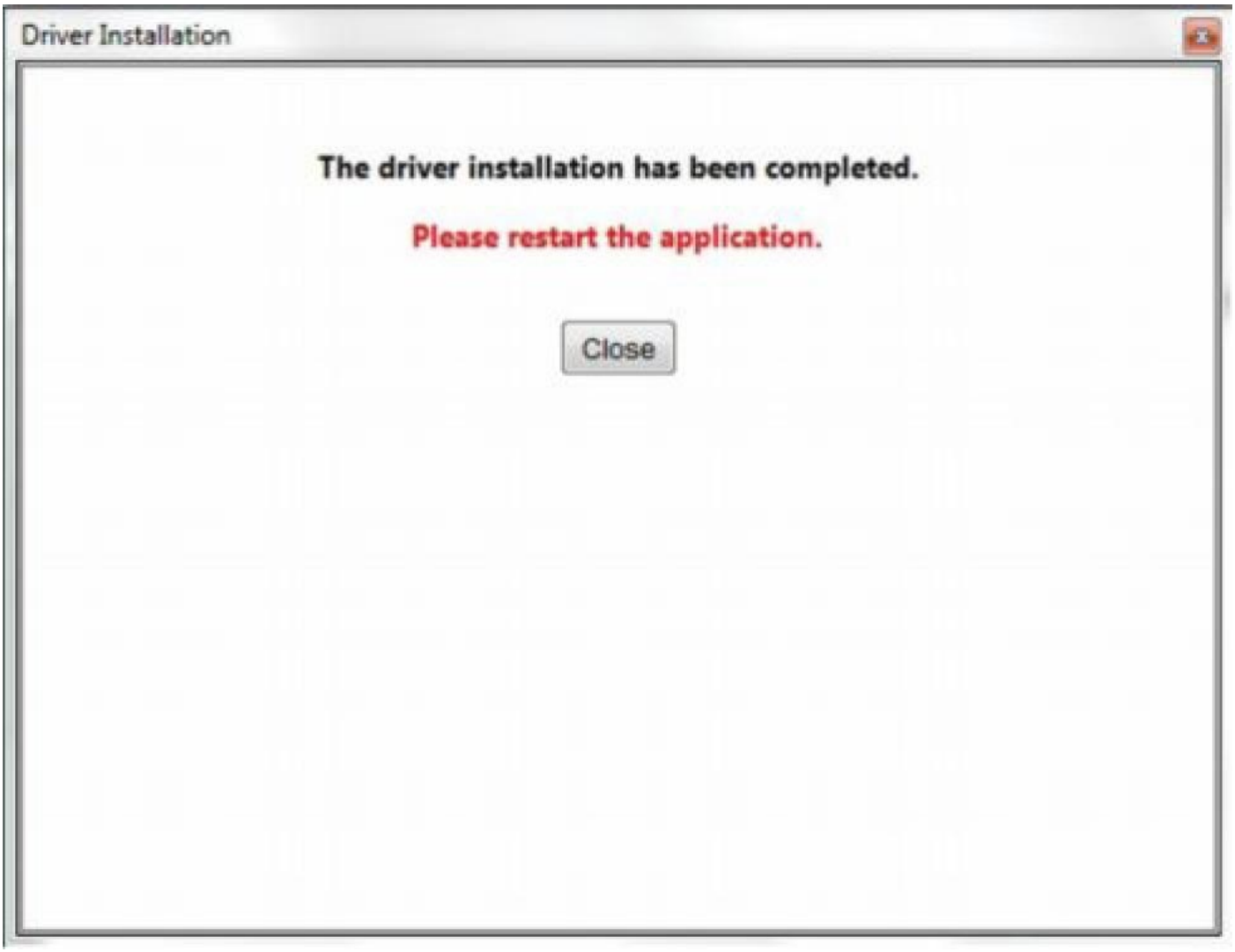


Figure A-35: Driver Installation—Installation Complete Screen

14. Click the **Close** button to close the **Driver Installation—Installation Complete** screen. The driver installation process requires a restart of the system.

    The system restarts and displays the shortcut of the **CommView for WiFi** application on the Desktop after the restart is complete, as shown in the following figure.

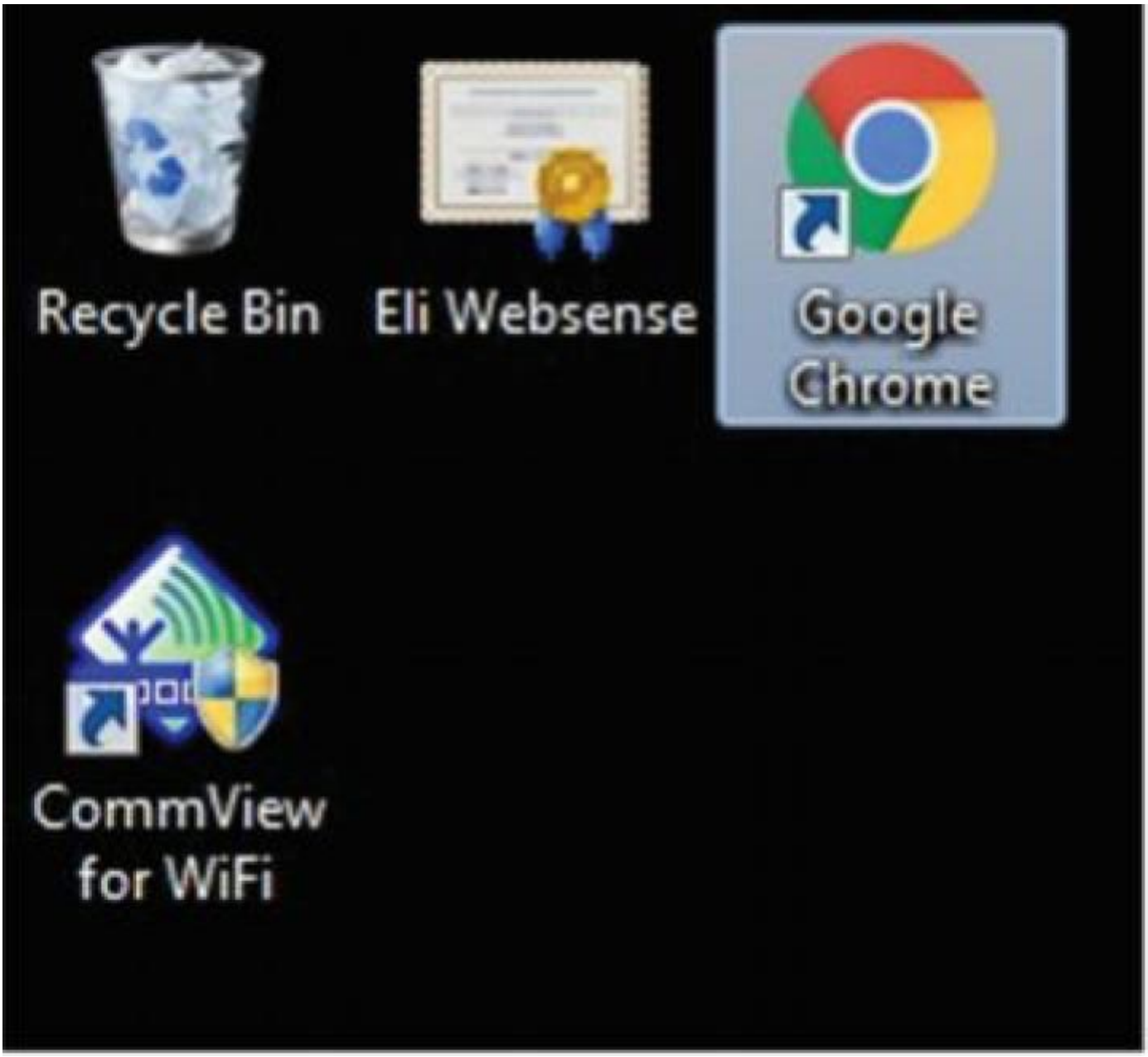


Figure A-36: Desktop with the CommView for WiFi Shortcut

Glossary

40 MHz Intolerant: A bit potentially set in the 802.11 frame allowing STAs to indicate that 40 MHz channels should not be used in their BSS or in surrounding networks. The bit is processed only in the 2.4 GHz band.

4-Way Handshake: The process used to generate encryption keys for unicast frames (Pairwise Transient Key (PTK)) and transmit encryption keys for group (broadcast, multicast) (Group Temporal Key (GTK)) frames using material from the 802.1X/EAP authentication or the pre-shared key (PSK). The PTK and GTK are derived from the Pairwise Master Key (PMK) and Group Master Key (GMK) respectively.

802.11: A standard maintained by the IEEE for implementing and communicating with wireless local area networks (WLANs). Regularly amended, the standard continues to evolve to meet new demands. Several Physical Layer (PHY) methods are specified and the Medium Access Control (MAC) sublayer is also specified.

802.11a: An 802.11 amendment that operates in the 5GHz band. It uses OFDM modulation and is called the OFDM PHY. It can support data rates of up to 54 Mbps.

802.11aa: An 802.11 amendment that added support for robust audio and video streaming through MAC enhancements. It specifies a new category of station called a Stream Classification Service (SCS) station. The SCS implementation is optional for a WMM QoS station.

802.11ac: An 802.11 amendment that operates in the 5GHz band. It uses MU-MIMO, beamforming, and 256 QAM technology, up to 8 spatial streams and OFDM modulation. Support is included for data rates up to 6933.3 Mbps.

802.11ae: An 802.11 amendment that provides prioritization of management frames. It defines a new Quality of Service Management Frame (QMF). When the QMF service is used, some management frames may be transmitted using an access category other than the one used for voice (AC_VO). When communicating with stations that do not support the QMF service, the station uses access category AC_VO to transmit management frames. When QMF is supported, the beacon frame includes a QMF Policy element.

802.11ah: An 802.11 draft that specifies operations in the sub-1 GHz range. Frequencies used vary by regulatory domain. The draft supports 1, 2, 4, 8 and 16 MHz channels with OFDM modulation.

802.11ax: An 802.11 draft that will support bi-directional MU-MIMO, higher modulation rates and sub-channelization. It is too early to know the final details of this amendment at the time of writing; however, it is planned to operate in the 2.4 GHz and 5 GHz band.

802.11b: An IEEE 802.11 amendment that operates in the 2.4GHz ISM band. It uses HR/DSSS and earlier technology. It can support data rates of up to 11Mbps.

802.11e: An 802.11 amendment, now incorporated into the most recent rollup, that provided quality of service extensions to the wireless link through probabilistic prioritization based on the contention window. The Wi-Fi Multimedia (WMM) certification is based on this amendment.

802.11g: An IEEE 802.11 amendment that operates in the 2.4GHz ISM band. It uses ERP-OFDM and earlier technology. It can support data rates of up to 54Mbps.

802.11i: An 802.11 amendment, now incorporated into the most recent rollup, which provided security enhancements to the standard and resolved weaknesses in the original WEP encryption solution. It provided for TKIP/RC4 (now deprecated) and CCMP/AES cipher suites and encryption algorithms.

802.11n: An IEEE 802.11 amendment that operates in the 2.4 ISM and 5GHz UNII/ISM bands. It uses MIMO, HT-OFDM and earlier technology. It can support data rates of up to 600Mbps.

802.11k: An IEEE 802.11 amendment that specifies and defines WLAN characteristics and mechanisms.

802.11r: An IEEE 802.11 amendment that enables roaming between access points.

802.11u: An IEEE 802.11 amendment that adds features for mobile communication devices such as phones and tablets.

802.11w: An IEEE 802.11 amendment to increase security for the management frames.

802.11y: An IEEE 802.11 amendment that allows registered stations to operate at a higher power output in the 3650-3700 MHz band.

802.1X: 802.1X is an IEEE standard that uses the Extensible Authentication Protocol (EAP) framework to authenticate devices attempting to connect to the LAN or WLAN. The process involves the use of a supplicant to be authenticated, authenticator, and authentication server.

802.11 State Machine: The 802.11 state machine defines the condition of the connection of a client STA to another STA and can be in one of three states: Unauthenticated/Unassociated, Authenticated/Unassociated, or Authenticated/Associated.

802.3: A set of standards maintained by the IEEE for implementing and communicating with wired Ethernet networks and including Power over Ethernet (PoE) specifications.

AAA Framework: Authentication, Authorization, and Accounting is a framework for monitoring usage, enforcing policies, controlling access to computer resources, and providing the correct billing amount for services.

AAA Server Credential: The AAA server credential is the validation materials used for the server. When mutual authentication is required, a server certificate is typically used as the AAA server credential.

Absorption: Occurs when an obstacle absorbs some or all of a radio wave's energy.

Access Category (AC): An access category is a priority class. 802.11 specifies four different priority classes – voice (AC_VO), video (AC_VI), best effort (AC_BE), and background (AC_BK).

Access Layer Forwarding: Data forwarding that occurs at the access layer, also called *distributed data forwarding*. The data is distributed from the access layer directly to the destination without passing through a centralized controller.

Access Point: An access point (AP) is a device containing a radio that is used to create an access network, bridge network or mesh network. The AP contains the Distribution System Service.

Access Port: An AP used for mesh networks and that connects to the wired or wireless network at the edge of the mesh.

Acknowledgement Frame: A frame sent by the receiving 802.11 station confirming the received data.

Access Control List (ACL): ACLs are lists that inform a STA or user what permissions are available to access files and other resources. ACLs are also used in routers and switches to control packets allowed through to other networks.

Active Mode: A power-save mode in which the station never turns the radio off.

Active Scanning: A scanning (network location) method in which the client broadcasts probe requests and records the probe responses in order to determine the network with which it will establish an association.

Active Survey: A wireless survey conducted on location that involves measuring throughput rates, round trip time, and packet loss by connecting devices to an AP and transmitting data during the survey.

Ad-Hoc Mode: The colloquial name for an Independent Basic Service Set (IBSS). STAs connect directly with each other and an AP is not used.

Adjacent Overlapping Channels: Adjacent overlapping channels are channels whose bands interfere with their neighboring channels on the primary carrier frequencies. Non-overlapping channels are channels whose bands do not interfere with neighboring channels on the primary carrier frequencies.

Adjacent Channel Interference (ACI): ACI occurs when channels near each other (in the frequency domain) interfere with one another due to either partial frequency overlap on primary carrier frequencies or excessive output power.

AES (Advanced Encryption Standard): The encryption cipher used with CCMP and WPA2 providing improved security over WEP/RC4 or TKIP/RC4.

AID: Association ID (AID) is an identification assigned by a wireless STA (AP) to another STA (client) in order to transmit the correct data to that device in an Infrastructure Basic Service Set.

AirTime Fairness: Transmits more frames to client STAs with higher data rates than those with lower data rates so that the STAs get fair access to the air (medium) instead of having to wait for slower data rate STAs.

Aggregated MAC Protocol Data Units (A-MPDU): A-MPDU transmissions are created by transmitting multiple MPDUs as one PHY frame as opposed to A-MSDU transmissions, which are created by passing multiple MSDUs down to the PHY layer as a single MPDU.

Aggregated MAC Service Data Unit (A-MSDU): See *Aggregated MAC Protocol Data Unit*.

Amplification: The process of increase a signal's power level.

Amplifier: A device intended to increase the power level of a signal.

Amplitude: The power level of a signal.

Antenna: A device that converts electric power into radio waves and radio waves into electric power.

Association: The condition wherein a client STA is linked with an AP for frame transmission through the AP to the network.

Announcement Traffic Indication Message (ATIM): A traffic indication map (sent in a management frame) in an Ad-Hoc (IBSS) network to notify other clients of pending data transfers for power saving purposes.

Attenuation: The loss of signal strength as an RF wave passes through a medium.

Attenuator: A device that intentionally reduces the strength of an RF signal.

Authentication: The process of user or device identity validation.

Authentication and Key Management (AKM): The protocols used to authenticate a client STA on a WLAN and generate encryption key for use in frame encryption.

Authentication Server: The authentication server validates the client before allowing access to the network. In an 802.1X/EAP implementation for WLANs, the authentication server is often a RADIUS server.

Authenticator: The device that provides access to authentication services in order to allow connected devices to access network resources. In an 802.1X/EAP implementation for WLANs, the authenticator is typically the AP or controller.

Automatic Power Save Delivery (APSD): APSD is a power saving method which uses both scheduled (S-APSD) and unscheduled (U-APSD) frame delivery methods. S-APSD sends frames to a power save STA from the AP at a planned time. U-APSD sends frames to a power save STA from the AP when the STA sends a frame to the AP. The frame from the STA is considered a trigger frame.

Autonomous AP: An AP that can perform security functions, RF management, and configuration without the need for a centralized WLAN controller or any other control platform.

Azimuth Chart: A chart showing the radiation pattern of an antenna as viewed from the top of the antenna. Also called an H-Plane Chart or H-Chart.

Backoff timer: The timer used during CSMA/CA to wait for access to the medium, which is selected from the contention window.

Band Steering: A method used by vendors to encourage STAs to connect to the 5 GHz band instead of the 2.4 GHz band, which is more congested. Typically implemented by ignoring probe requests for some period of time before allowing connection to the 2.4 GHz radio by clients known to have a 5 GHz radio based on previous connections to the AP or controller.

Bandwidth: The frequencies used for transmission of data. For example, a 20 MHz wide

channel has 20 MHz of bandwidth.

Basic Service Area (BSA): The coverage area provided by an AP wherein client STAs may connect to the AP to transmit data on the WLAN or through the AP to the network.

Basic Service Set (BSS): An AP and its associated STAs. Identified by the BSSID.

Basic Service Set Identification (BSSID): The ID for the BSS. Often the MAC address of the AP STA. When multiple SSIDs are used, another MAC address-like BSSID is generated.

Beacon Frame: A frame transmitted periodically from an AP that indicates the presence of a BSS network and contains capabilities and requirements of the BSS. Also colloquially called a beacon instead of the full phrase, beacon frame.

Beamforming: Directing radio waves to a specific area or device by manipulating the RF waveforms within the different radio chains.

Beamwidth: The width of the radiated signal lobe from the antenna in the intended direction of propagation. It is usually measured at the point where 3 dB of loss is experienced.

Bill of materials (BOM): A list of the materials and licenses required to assemble a system, in the case of WLANs, including APs, controllers, PoE injectors, licenses, etc.

Bit: A basic unit of information for computer systems. A bit can have a value of 1 or 0. Used in binary math.

Block Acknowledgement: An acknowledgement frame that groups together multiple ACKs instead of transmitting each individual ACK when a block transmission has been received.

Bridge: A device used to connect two networks. Wireless bridges create the connection across the wireless medium.

BSS Transition: Roaming that occurs between two BSSs that are part of the same ESS.

Byte: A basic unit of information that typically consists of 8 bits. Also called an octet.

Capacity: The number of clients and applications a network or AP can handle.

Captive Portal: Authentication technique that re-routes a user to a special webpage to verify their credentials before allowing access to the network. Commonly used in hotel and guest networks.

Guest Networks: A segregated network that is designed for use by temporary visitors.

CardBus: A PCMCIA PC Card standard interface that supports 32-bits and operates at speeds of up to 33 MHz. It is primarily used in laptops.

Carrier Frequencies: The frequency of a carrier signal or the frequencies used to modulate information.

Carrier Sense Multiple Access (CSMA): CSMA is a protocol that allows a node to detect the presence of traffic before sending data on a shared network. Used in CSMA/CA.

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA): CSMA/CA is

the method in 802.11 networks in which a node only sends data if the shared network is idle in order to avoid collisions.

CCMP: Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP) is an key management solution that provides for improved security over WEP.

CCMP/AES: CCMP used with AES, as it is in 802.11 networks, is a key management and encryption protocol that provides more security than WEP. It is based on the AES standard and uses a 128 bit key and 128 bit block size.

Centralized Forwarding: Every forwarding decision is made by a centralized forwarding engine, such as the WLAN controller.

Certificate Authority (CA): A server that validates the authenticity of a certificate used in authentication and encryption systems. The CA may issues certificates or it may authorize other servers to do the same.

CompactFlash (CF): Originally produced in 1994 by SanDisk, CF is a flash memory mass storage device format that can support up to 256 GB. CF devices can also function as 802.11 WLAN adapters.

Channel: A specified range of frequencies used in the 802.11 standard used by devices to communicate on the network. Channels are commonly 20, 40, 80 and 160 MHz in width in WLANs. Newer standards will support 1, 2, 4, 8 and 16 MHz channels in sub-1 GHz networks.

Channel Width: The range of frequencies a single channel encompasses.

Clear Channel Assessment (CCA): CCA is a feature defined in the IEEE 802.11 standard that allows a client to determine idle or busy state of the medium based on energy levels of a frame or raw energy levels as specified in each PHY.

Client Utilities: Software installed on devices that allows the device to connect to, authenticate with and participate in a WLAN.

Co-Channel Interference (CCI): Congestion cause by the normal operations of CSMA/CA when multiple BSSs exist on the same channel. Commonly called co-channel congestion (CCC) today as well.

Collision Avoidance (CA): A method in which devices attempt to avoid simultaneous data transmissions in order to prevent frame collisions. Used in CSMA/CA.

Coding: A process used to encode bits to be transmitted on the wireless medium such that error recovery can be achieved. Part of forward error correction (FEC) and defined in the modulation and coding schemes (MCSs) from 802.11n forward.

Containment: A process used against a detected rogue AP to prevent any connected clients from accessing the network.

Contention Window: A number range defined in the 802.11 standard and varying by QoS category from which a number is selected at random for the backoff timer in the CSMA/CA process.

Control Frame: An 802.11 frame that is used to control the communications process on

the wireless medium. Control frames include, RTS frames, CTS frames, PS-Poll frames and ACK frames.

Controlled Port: In an 802.1X authentication system, the virtual port that allows all frames through to the network, but only after authentication is completed.

Controller-Based AP: An AP managed by a centralized controller device. Also called a lightweight AP or thin AP.

Coverage: 1) The colloquial term used for the BSA of an AP. 2) The requirement of available WLAN connectivity throughout a facility, campus or area. Often specified in minimum signal strength as dBm; for example, -67 dBm.

Clear-to-Send (CTS) Frame: A CTS frame sent from one STA to another to indicate that the other STA can transmit on the medium. The duration value in the CTS frame is used to silence all other STAs by setting their NAV timers.

Data Frame: An 802.11 frame specified for use in carrying data based on the general frame format. Also used for some signaling purposes as null data frames.

Data Rate: The rate at which data is sent across the wireless medium. Typically represented as megabits per second (Mbps) or gigabits per second (Gbps). The data rate should not be confused with throughput rate, which is a measurement of Layer 4 throughput or useful user data.

dBd (decibel to dipole): A relative measurement of antenna gain compared to a dipole antenna. Calculated as 2.14 dB greater than dBi as a dipole antenna already has 2.14 dBi gain.

dBi (decibel to isotropic): A relative measurement of antenna gain compared to a theoretical isotropic radiator. When necessary, calculated as 2.14 dB less than dBd.

dBm (decibel to milliwatt): An absolute measurement of the power of an RF signal based on the definition of 0 dBm = 1 milliwatt (mW).

Distributed Coordination Function (DCF): A protocol defined in 802.11 that uses carrier sensing, backoff timers, interframe spaces and frame duration values to diminish collisions on the wireless medium.

Elevation Chart: A chart showing the radiation pattern of an antenna as viewed from the side antenna. Also called an E-Plane Chart or E-Chart.

Deauthentication Frame: A notification frame sent from an 802.11 STA to another STA in order to terminate a connection between them.

Decibel (dB): A logarithmic, relative unit used when measuring antenna gain, signal attenuation, and signal-to-noise ratios. Strictly defined as 1/10 of a bel.

Delay: The time it takes for a bit of data to travel from one node to another. Also called latency.

Delivery Traffic Indication Message (DTIM): A message sent from an AP to clients in the Beacon frame indicating that it has data to transmit to the clients specified by the AIDs.

Differentiated Services Code Point (DSCP): A Layer 3 QoS marking system. IP packets can include DSCP markings in the headers. Eight precedence levels, 0-7, are defined.

Diffraction: The bending of waves around a very large object in relation to the wave.

Direct-Sequence Spread Spectrum (DSSS): A modulation technique where data is coupled with coding that spreads the data across a wide frequency range. Provides 1 or 2 Mbps data rates in 802.11 networks.

Disassociation Frame: A frame sent from one STA to another in order to terminate the association.

Distributed Forwarding: See Access Layer Forwarding. Also called, distributed data forwarding.

Distribution System (DS): The system that connects a set of BSSs and LANs such that an ESS is possible.

Distribution System Medium (DSM): The medium used to interconnect APs through the DS such that they can communicate with each other for ESS operations using either wired or wireless for the DS connection.

Domain Name System (DNS): A protocol and service that provides host name resolution (looking up the IP address of a given host name) and recursive IP address lookups (finding the host name of a known IP address). Also, colloquially used to reference the server that provides DNS lookups.

Driver: Software that allows a computer to interact with a hardware device such as a WLAN adapter.

Duty Cycle: A measure of the time a radio is transmitting or a channel is consumed by a transmitting device.

Dynamic Frequency Selection (DFS): A setting on radios that dynamically changes the channel selection based on detected interference from radar systems. Many 5 GHz channels require DFS operations.

Dynamic Rate Switching (DRS): The process of reducing a client’s data rate as frame transmission failures occur or signal strength decreases. DRS results in lower data rates but fewer transmissions required to successfully transmit a frame.

Encryption: The process of converting data into a form that unauthorized users cannot understand by encoding the data with an algorithm and a key or keys.

Enhanced Distributed Channel Access (EDCA): An enhancement to DCF introduced in 802.11e that implements priority based queuing for transmissions in 802.11 networks based on access categories.

Equivalent Isotropically Radiated Power (EIRP): The output power required of an isotropic radiator to equal the measured power output from an antenna in the intended direction of propagation.

Extended Rate Physical (ERP): A physical layer technology introduced in 802.11g that uses OFDM (from 802.11a) in the 2.4 GHz band and offers data rates up to 54 Mbps.

Extended Service Set (ESS): A group of one or more BSSs that are interconnected by a DS.

Extensible Authentication Protocol (EAP): An authentication framework that defines message formats for authentication exchanges used by 802.1X WLAN authentication solutions.

Fade Margin: An amount of signal strength, in dB, added to a link budget to ensure proper operations.

Fast Fourier Transform (FFT): A mathematical algorithm that takes in a waveform as represented in the time or space domain and shows it in the frequency domain. Used in spectrum analyzers to show real-time views in the frequency domain (Real-time FFT).

Fragmentation: The process of fragmenting 802.11 frames based on the fragmentation threshold configured. Fragmented frames have a greater likelihood of successful delivery in the presence of sporadic interference.

Frame Aggregation: A feature in the IEEE 802.11n PHY and later PHYs that increases throughput by sending more than one frame in a single transmission. Aggregated MSDUs or aggregated MPDUs may be supported.

Frame: A well-defined, meaningful set of bits used to communicate management and control information on a network or transfer payloads from higher layers. Frames are defined at the MAC and PHY layer.

Free Space Path Loss: The natural loss of amplitude that occurs in an RF signal as it propagates through space and the wave front spreads.

Fresnel Zones: Ellipsoid shaped zones around the visual LoS in a wireless link. The first Freznel zone should be 60% clear and would preferably be 80% clear to allow for environmental changes.

Frequency: The speed at which a waveform cycles in a second.

Full Duplex: A communication system that allows an endpoint to send data to the network at the same time as it receives data from the network.

Gain: The increase in signal strength in a particular direction. Can be accomplished passively by directing energy into a smaller area or actively by increasing the strength of the broadcasted signal before it is sent to the antenna.

Group Key Handshake: Used to transfer the GTK among STAs in an 802.11 network if the GTK requires updating. Initiated by the AP/controller in a BSS.

Group Master Key (GMK): Used to generate the GTK for encryption of broadcast and multicast frames and is unique to each BSS.

Group Temporal Key (GTK): Used to encryption broadcast and multicast frames and is unique to each BSS.

Guard Interval (GI): A period of time between symbols within a frame used to avoid intersymbol interference.

Half Duplex: A communication system that allows only sending or receiving data by an

endpoint at any given time.

Hidden Node: The problem that arises when nodes cannot receive each other's frames, which can lead to packet collisions and retransmissions.

High Density: A phrase referencing a WLAN network type that is characterized by large numbers of devices requiring access.

Highly-Directional Antenna: An antenna, such as a parabolic dish or grid antenna, that has a high gain in a specified direction and a low beamwidth measurement as compared to semi-directional and omnidirectional antennas.

High Rate Direct Sequence Spread Spectrum (HR/DSSS): An amendment-based PHY (802.11b) that increase the data rate in 2.4 GHz from the original 1 or 2 Mbps to 5.5 and 11 Mbps while maintaining backward compatibility with 1 and 2 Mbps.

High Throughput (HT): An amendment-based PHY (802.11n) that increased the data rate up to 600 Mbps and added support for transmit beamforming and MIMO.

Hotspot: A term referencing a wireless network connection point that is typically open to the public or to paid subscribers.

Independent Basic Service Set (IBSS): A set of 802.11 devices operating in ad-hoc (peer-to-peer) mode without the use of an AP.

Institute of Electrical and Electronics Engineers (IEEE): A standardization organization that develops standard for multiple industries including the networking industry with standard such as 802.3, 802.11 and 802.16.

Intentional Radiator: Any device that is purposefully sending radio waves. Signal strength of the intentional radiator is measured at the point where energy enters the radiating antennas.

Interference: In WLANs, an RF signal or incidental RF energy that is radiated in the same frequencies as the WLAN and that has sufficient amplitude and duty cycle to prevent 802.11 frames from successful delivery.

Interframe Space (IFS): A time interval that must exist between frames. Varying lengths are used in 802.11 and a references as DIFS, SIFS, EIFS and AIFS in common use.

Internet Engineering Task Force (IETF): An open group of volunteers develops Internetworking standards through request for comments (RFC) documents. Examples include RADIUS, EAP and DNS.

Isotropic Radiator: A theoretical antenna that spreads the radiaton equally in every directon as a sphere. None exist in reality, but the concept is used to measure relative antenna gain in dBi.

Jitter: The variance in delay between packets sent on a network. Excessive jitter can result in poor quality for real-time applications such as voice and video.

Jumbo Frame: An Ethernet frame that contains more than 1500 bytes of payload and up to 9000 to 9216 bytes.

Latency: The time taken data to move between places. Typically synonymous with delay

in computer networking.

Layer 1: The physical layer (PHY) that is responsible for framing and transmitting bits on the medium. In 802.3 and 802.11 the entirety of Layer 1 is defined.

Layer 2: The data-link layer that deals with data frames moving within a local area network (LAN). In 802.3 and 802.11, the MAC sublayer of Layer 2 is defined.

Layer 3: The network layer where packets of data are routed between sender and receiver. Most modern networks use Internet Protocol (IP) at Layer 3.

Layer 4: The transport layer where segmentation occurs for upper layer data and TCP (connection oriented) and UDP (connectionless) are the most commonly used protocols.

Lightning Arrestor: A device that can redirect ambient energy from a lightning strike away from attached equipment.

Line of sight (LoS): When existing, the visual path between to ends. RF LoS is different from visual LoS. RF LoS does not require the same clear path for the remote receiver to hear the signal. When creating bridge links, visual LoS is often the starting point.

Link Budget: The measurement of gains and losses through an intentional radiator, antenna and over a transmission medium.

Loss: The reduction in the amplitude of a signal.

MAC filtering: A common setting that only allows specific MAC addresses onto a network. Ineffective against knowledgeable attackers because the MAC address can be spoofed to impersonate authorized devices.

Management Frame: A frame type defined in the 802.11 standard that encompasses frames used to manage access to the network including beacon, probe request, prober response, authentication, association, reassociation, deauthentication and disassociation frames.

Master Session Key (MSK): A key derived between an EAP client and EAP server and exported by the EAP method. Used to derive the PMK, which is used to derive the PTK. The MSK is used in 802.1X/EAP authentication implementations. In personal authentication implementations, the PMK is derived from the pre-shared key.

Maximal Ratio Combining (MRC): A method of increasing the signal-to-noise ratio (SNR) by combining signals received on multiple radio chains (multiple antennas and radios).

Mesh: A network that uses interconnecting devices to form a redundant set of connections offering multiple paths through the network. 802.11s defined mesh for 802.11 networks.

Mesh BSS: A basic service set that forms a self-contained network of mesh stations.

milliwatt (mW): A unit of electrical energy used in measuring output power of RF signals in WLANs. A mW is equal to 1/1000 of a watt (W).

Mobile User: A user that physically moves while connected to the network. The opposite of a stationary user.

Modulation: The process of changing a wave by changing its amplitude, frequency,

and/or phase such that the changes represent data bits.

Modulation and Coding Scheme (MCS): Term used to describe the combination of the radio modulation scheme and the coding scheme used when transmitting data, first introduced in 802.11n.

MPDU: A MAC protocol data unit (MPDU) is a portion of data to be delivered to a MAC layer peer on a network and it is data prepared for the PHY layer by the MAC sublayer. The MAC sublayer receives the MSDU from upper layers on transmission and creates the MPDU. It receives the MPDU from the lower layer on receiving instantiation and removes the MAC header and footer to create the MSDU for the upper layers.

MSDU: A MAC service data unit is a portion of transmitted data to be handled by the MAC sublayer that has yet to be encapsulated into a MAC Layer frame.

Maximum Transmission Unit (MTU): The largest amount of data that can be sent at a particular layer of the OSI model. Typically set at layer 4 for TCP.

Multi-User MIMO (MU-MIMO): An enhancement to MIMO that allows the AP STA to transmit to multiple client STAs simultaneously.

Multipath: The phenomenon that occurs when multiple copies of the same signal reach a receiver based on RF behaviors in the environment.

Multiple Channel Architecture (MCA): A wireless network design using multiple channels strategically designed so that the implemented BSSs have minimal interference with one another.

Multiple Input/Multiple Output (MIMO): A technology used to spread a stream of data bits across multiple radio chains using spatial multiplexing at the transmitter and to recombine these streams at the receiver.

Narrowband Interference: Interference that covers a very narrow band of frequencies and typically not the full with of an 802.11 channel when used in reference to WLAN interferers.

Near-Far: A problem that occurs when a high powered device is closer to the AP in a BSS and a low powered device is farther from the AP. Most near-far problems are addressed with standard CSMA/CA operations in 802.11 networks.

Network Allocation Vector (NAV): The NAV is a virtual carrier sense mechanism used in CSMA/CA to avoid collisions and is a timer set based on the duration values in frames transmitted on the medium.

Network Segmentation: The process used to separate a larger network into smaller networks often utilizing Layer 3 routers or multi-layer switches.

Noise: RF energy in the environment that is not part of the intentional signal of your WLAN.

Noise Floor: The amount of noise that is consistently present in the environment, which is typically measured in dBm.

Network Time Protocol (NTP): A protocol used to synchronize clocks in devices using centralized time servers.

Octet: A group of eight ones and zeros. An 8-but byte. Sometimes simply called a byte.

Orthogonal Frequency Division Multiplexing (OFDM): A modulation technique and a named physical layer in 802.11 that provides data rates up to 54 Mbps and operates in the 5 GHz band. The modulation is used in all bands, but the named PHY operates only in the 5 GHz band.

Omni-Directional Antenna: An antenna that propagates in all directions horizontally. Creates a coverage area similar to a donut shape (toroidal). Also known as a dipole antenna.

Dipole Antenna: An antenna that propagates in all directions horizontally. Creates a coverage area similar to a donut (toroidal) shape. Also known as a omni-directional antenna.

Open System Authentication: A simple frame exchange, providing no real authentication, used to move through the state machine in relation to the connection between two 802.11 STAs.

Opportunistic Key Caching (OKC): A roaming solution for WLANs wherein the keys derived from the 802.1X/EAP authentication are cached on the AP or controller such that only the 4-way handshake is required at the time of roaming.

OSI (Open Systems Interconnection) Model: A theoretical model for communication systems that works by separating the communications process into seven, well-defined layers. The seven layers are Application, Presentation, Session, Transport, Network, Data Link and Physical.

Packet: Data as represented at the network layer (Layer 4) for TCP communications.

Passive Gain: An increase in strength of a signal by focusing the signal's energy rather than increasing the actual energy available, such as with an amplifier.

Passive scanning: A scanning (network location) method wherein a STA waits to receive beacon frames from an AP which contain information about the WLAN.

Passive survey: A survey conducted on location that gathers information about RF interference, signal strength and coverage areas by monitoring RF activity without active communications.

Passphrase Authentication: A type of access control that uses a phrase as the pass key. Also called personal in WPA and WPA2.

Phase: A measurement of the variance in arrival state between to copies of a wave form. Waves are said to be in phase or out of phase by some degree. The phase can be manipulated for modulation.

PHY: A shorthand notation for physical layer which is the physical means of communication on a network to transmit bits.

Physical (PHY) Layer: The physical (PHY) layer refers to the physical means by which a message is communicated. Layer one of the OSI model.

PLCP: Physical Layer Convergence Protocol (PLCP) is the name of the service within the PHY that receives data from the upper layers and sends data to the upper layers. It is the

interaction point with the MAC sublayer.

PMD: Physical Medium Dependent (PMD) is the service within the PHY responsible for sending and receiving bits on the RF medium.

PMK Caching: Stores the PMK so a device only has to perform the 4 way handshake when connecting to an AP to which it has already connected.

Pairwise master Key (PMK): The key derived from the MSK, which is generated during 802.1X/EAP authentication. Used to derive the PTK. Used in unidirectional communications with a single peer.

PoE Injector: Any device that adds Power over Ethernet (PoE) to ethernet cables. Come in two variants, endpoint (such as switches) and midspan (such as inline injectors).

Point-to-Multipoint (PtMP): A connection between a single point and multiple other points for wireless bridging or WLAN access.

Point-to-Point (PtP): A connection between two points often used to connect two networks via bridging.

Polarization: The technical term used to reference the orientation of antennas related to the electric field in the electromagnetic wave.

Power over Ethernet (PoE): A method of providing power to certain hardware devices that can be powered across the Ethernet cables. Specified in 802.3 as a standard. Various classes are defined based on power requirements.

PPDU: PLCP Protocol Data Unit (PPDU) is the prepared bits for transmission on the wired or wireless medium. Sometimes also called a PHY Layer frame.

Preauthentication: Authenticating with an AP to which the STA is not intending to immediately connect so that roaming delays are reduced.

Pre-shared Key (PSK): Refers to any security protocol that uses a password or passphrase or string as the key from which encryption materials are derived.

Primary Channel: When implementing channels wider than 20 MHz in 802.11n and 802.11ac, the 20 MHz channel on which management and control frames are sent and the channel used by STAs not supporting the wider channel.

Probe Request: A type of frame sent when a client device wants information about APs in the area or is seeking a specific SSID to which it desires to connect.

Probe Response: A type frame sent in response to a probe request that contains information about the AP and the requirements of BSSs it provides.

Protected Management Frame (PMF): Frames used for managing a wireless network that are protected from spoofing using encryption. Protocol defined in the 802.11w amendment.

Protocol Analyzer: Hardware or software used to capture and analyze networking communications. WLAN protocol analyzers have the ability to capture 802.11 frames from the RF medium and decode them for display and analysis.

Protocol Decodes: The way information in captured packets or frames is interpreted for

display and analysis.

PSDU: PLCP Service Data Unit (PSDU) is the name for the contents that are contained within the PPDU, the PLCP Protocol Data Unit. It is the same as the MPDU as perceived and received by the PHY.

PTK (Pairwise Transient Key): A key derived during the 4-way handshake and used for encryption only between two specific endpoints, such as an AP and a single client.

Quality of Service (QoS): Traffic prioritization and other techniques used to improve the end-user experience. IEEE 802.11e includes QoS protocols for wireless networks based on access categories.

QoS BSS: A BSS supporting 802.11e QoS features.

Radio Chains: A reference to the radio and antenna used together to transmit in a given frequency range. Multi-stream devices have multiple radio chains as one radio chain is required for each stream.

Radio Frequency (RF): The electromagnetic wave frequency range used in WLANs and many other wireless communication systems.

Radio Resource Management (RRM): Automatic management of various RF characteristics like channel selection and output power. Known by different terms among the many WLAN vendors, but referencing the same basic capabilities.

RADIUS: Remote Authentication Dial-In User Service (RADIUS) refers to a network protocol that handles AAA management which allows for authentication, authorization and accounting (auditing). Used in 802.11 WLANs as the authentication server in an 802.1X/EAP implementation.

RC4 (Rivest Cipher 4): An encryption cipher used in WEP and with TKIP. A stream cipher.

Real-Time Location Service (RTLS): A function provided by many WLAN infrastructure and overlay solutions allowing for device location based on triangulation and other algorithms.

Reassociation: The process used to associate with another AP in the same ESS. May also be used when a STA desires to reconnect to an AP to which it was formerly connected.

Received Channel Power Indicator (RCPI): Introduced in 802.11k, a power measurement calculated as INT((dBm + 110) * 2). Expected accuracy is +/- 5 dB. Ranges from 0-220 are available with 0 equaling or less than -110 dBm and 220 equaling or greater than 0 dBm. The value is calculated as an average of all received chains during the reception of the data portion of the transmission. All PHYs support RCPI and, though 802.11ac does not explicitly list its formulation, it references the 802.11n specification for calculation procedures.

Received Signal Strength Indicator (RSSI): A relative measure of signal strength for a wireless network. The method to measure RSSI is not standardized though it is constrained to a limited number of values in the 802.11 standard. Many use the term RSSI to reference dBm, and the 802.11 standard uses terms like DataFrameRSSI and

BeaconRSSI and defines them as the signal strength in dBm of the specified frames, so the common vernacular is understandable. However, according to the standard, “absolute accuracy of the RSSI reading is not specified” (802.11-2012, Clause 14.3.3.3).

Reflection: An RF behavior that occurs when a wave meets a reflective obstacle large than the wavelength similar to light waves in a mirror.

Refraction: An RF behavior that occurs as an RF wave passes through material causing a bending of the wave and possible redirection of the wave front.

Regulatory Domain: A reference to geographic regions management by organizations like the FCC and ETSI that determine the allowed frequencies, output power levels and systems to be used in RF communications.

Remote AP: An AP designed to be implemented at a remote location and managed across a WAN link using special protocols.

Resolution Bandwidth (RBW): The smallest frequency that can be extracted from a received signal by a spectrum analyzer or the configuration of that frequency. Many spectrum analyzers allow for the adjustment of the RBW within the supported range of the analyzer.

Retry: That which occurs when a frame fails to be delivered successfully. A bit set in the frame to specify that it is a repeated attempt at delivery.

Return Loss: A measure of how much power is lost in delivery from a transmission line to an antenna.

RF Cables: A cable, typically coaxial, that allows for the transmission of electromagnetic waves between a transceiver and an antenna.

RF Calculator: A software application used to perform calculations related to RF signal strength values.

RF Connector: A component used to connect RF cables, antennas and transmitters. RF connectors come in many standardized forms and should match in type and resistance.

RF Coverage: Synonymous with coverage in WLAN vernacular. Reference to the BSA provided by an AP.

RF Link: An established connection between two radios.

RF Line of Sight (LoS): The existence of a path, possibly including reflections, refractions and pass-through of materials, between two RF transceivers.

RF Propagation: The process by which RF waves move throughout an area including reflection, refraction, scattering, diffraction, absorption and free space path loss.

RF Signal Splitter: An RF component that splits the RF signal with a single input and multiple outputs. Historically used with some antenna arrays, but less common today in WLAN implementations.

RF Site Survey: The process of physically measuring the RF signals within an area to determine resulting RF behavior and signal strength. Often performed as a validation procedure after implementation based on a predictive model.

Roaming: That which occurs when a wireless STA moves from one AP to another either because of end user mobility or changes in the RF coverage.

Robust Security Network (RSN): A network that supports CCMP/AES or WPA2 and optionally TKIP/RC4 or WPA. To be an RSN, the network must support only RSN Associations (RSNAs), which are only those associations that use the 4-way handshake. WEP is not supported in an RSN.

Robust Security Network Association (RSNA): An association between a client STA and an AP that was established through authentication resulting in a 4-way handshake to derive unicast keys and transfer group keys. WEP is not supported in an RSNA.

Rogue Access Point: An access point that is connected to a network without permission from a network administrator or other official.

Rogue Containment: Procedures used to prevent clients from associating with a rogue AP or to prevent the rogue AP from communicating with the wired network.

Rogue Detection: Procedures used to identify rogue devices. May include simple identification of unclassified APs or algorithmic processes that identify likely rogues.

Role-Based Access Control (RBAC): An authorization system that assigns permissions and rights based on user roles. Similar to group management of authorization policies.

RSN Information Element: A portion of the beacon frame that specifies the security used on the WLAN.

Request to Send/Clear to Send (RTS/CTS): A frame exchange used to clear the channel before transmitting a frame in order to assist in the reduction of collisions on the medium. Also used as a backward compatible protection mechanism.

RTS Threshold: The minimum size of a frame required to use RTS/CTS exchanges before transmission of the frame.

S-APSD: See Automatic Power Save Delivery.

Scattering: An RF behavior that occurs when an RF wave encounters reflective obstacles that are smaller than the wavelength. The result is multiple reflections or scattering of the wave front.

Secondary Channel: When implementing channels wider than 20 MHz in 802.11n and 802.11ac, the second channel used to form a 40 MHz channel for data frame transmissions to and from supporting client STAs.

Semi-Directional Antenna: An antenna such as a yagi or a patch that has a propagation pattern which maximizes gain in a given direction rather than an omni-directional pattern, having a larger beamwidth than highly directional antennas.

Service Set Identifier (SSID): The BSS and ESS name used to identify WLAN. Conventionally made to be readable by humans. Maximum of 32 bytes long.

Signal Strength: A measure of the amount of RF energy being received by a radio. Often specified as the RSSI, but referenced in dBm, which is not the proper definition of RSSI from the 802.11 standard.

Single Channel Architecture (SCA): A WLAN architecture that places all APs on the same channel and uses a centralized controller to determine when each AP can transmit a frame. No control of client transmissions to the network is provided.

Single Input Single Output (SISO): A radio transmitter that supports one radio chain and can send and receive only a single stream of bits.

Signal to Noise Ratio (SNR): A comparison between the received signal strength and the noise floor. Typically presented in dB. For example, given a noise floor of -95 dBm and a signal strength of -70 dBm, the SNR is 25 dB.

Space-Time Block Coding (STBC): The use of multiple streams of the same data across multiple radio chains to improve reliability of data transfer through redundancy.

Spatial Multiplexing (SM): Used with MIMO technology to send multiple spatial streams of data across the channel using multiple radio chains (radios coupled with antennas).

Spatial Multiplexing Power Save (SMPS): A power saving feature from 802.11n that allows a station to use only one radio (or spatial stream).

Spatial Streams: The partitioning of a stream of data bits into multiple streams transmitted simultaneously by multiple radio chains in an AP or client STA.

Spectrum Analysis: The inspection of raw RF energy to determine activity in an area on monitored frequencies. Useful in troubleshooting and design planning.

Spectrum Analyzer: A hardware and software solution that allows the inspection of raw RF energy.

Station (STA): Any device that can use IEEE 802.11 protocol. Includes both APs and clients.

Supplicant: In 802.1X, the device attempting to be authenticated. Also the term used for the client software on a device that is capable of connecting to a WLAN.

Sweep Cycle: The time it takes a spectrum analyzer to sweep across the frequencies monitored. Often a factor of the number of frequencies scanned and the RBW.

System Operating Margin (SOM): The actual positive difference in the required link budget for a bridge link to operate properly and the received signal strength in the link.

Temporal Key Integrity Protocol (TKIP): The authentication and key management protocol supported by WPA systems and implemented as an interim solution between WEP and CCMP.

Transition Security Network (TSN): A network that allows WEP connections during the transition period over to more secure protocols and an eventual RSN. An RSN does not allow WEP connections.

Transmit Beamforming (TxBF): The use of multiple antennas to transmit a signal strategically with varying phases so that the communication arrives at the receiver such that the signal strength is increased.

Transmit Power Control (TPC): A process implemented in WLAN devices allowing for

the output power to be adjusted according to local regulations or by an automated management system.

U-APSD: See Automatic Power Save Delivery.

Uncontrolled Port: In an 802.1X authentication system, the virtual port that allows only authentication frames/packets through to the network and, when authentication is successfully completed, provides the 802.1X service with the needed information to open the controlled port.

User Priority (UP): A value (from 0–7) assigned to prioritize traffic that correspond to different access categories for WMM QoS.

Virtual Carrier Sense: The 802.11 standard currently defines the Network Allocation Vector (NAV) for use in virtual carrier sensing. The NAV is set based on the duration value in perceived frames within the channel.

Voltage Standing Wave Ratio (VSWR): The Voltage Standing Wave Ratio is the ratio between the voltage at the maximum and minimum points of a sanding wave.

Milliwatt: One thousandth of a watt. A common measurement for output power in WLAN devices.

Watt: A unit of power. Strictly defined as the energy consumption rate of one joule per second such that 1 W is equal to 1 joule per 1 second.

Wavelength: The distance between two repeating points on a wave. Wavelength is a factor of the frequency and the constant of the speed of light.

Wired Equivalent Privacy (WEP): A legacy method of security defined in the original IEEE 802.11 standard in 1997. Used the RC4 cipher like TKIP (WPA), but implemented it poorly. WEP is deprecated and should no longer be used.

Wi-Fi Alliance: An association that certifies WLAN equipment to interoperate based on selected portions of the 802.11 standard and other standards. Certifications include those based on each PHY as well as QoS and security.

Wi-Fi Multimedia (WMM): A QoS certification created and tested by the Wi-Fi Alliance using traffic prioritizing methods defined in the IEEE 802.11e.

Wi-Fi Multimedia Power Save (WMM-PS): A power saving certification designed by the Wi-Fi Alliance and optimized for mobile devices and implementing methods designated in the IEEE 802.11e amendment.

Wireless Intrusion Prevention System (WIPS): A system used to detect and prevent unwanted intrusions in a WLAN by detecting and preventing rogue APs and other WLAN threats.

Wireless Local Area Network (WLAN): A local area network that connects devices using wireless signals based on the 802.11 protocol rather than wires and the common 802.3 protocol.

WPA-Enterprise: A security protocol designed by the Wi-Fi Alliance. Requires an 802.1X authentication server. Uses the TKIP encryption protocol with the RC4 cipher. Implements a portion of 802.11i and the older, no deprecated TKIP/RC4 solution.

WPA-Personal: A security protocol designed by the Wi-Fi Alliance. Does not require an authentication server. Uses the TKIP encryption protocol with the RC4 cipher. Also known as WPA-PSK (Pre-Shared Key).

WPA2-Enterprise: A security protocol designed by the Wi-Fi Alliance. Requires an 802.1X authentication server. Uses the CCMP key management protocol with the AES cipher. Also known as WPA2-802.1X. Implements the non-deprecated portion of 802.11i.

WPA2-Personal: A security protocol designed by the Wi-Fi Alliance. Does not require an authentication server. Uses the CCMP key management protocol with the AES cipher. Also known as WPA2-PSK (Pre-Shared Key).

Wi-Fi Protected Setup (WPS): A standard designed by the Wi-Fi Alliance to secure a network without requiring much user knowledge. Users connect either by entering a PIN associated with the device or by Push-Button which allows users to connect when a real or virtual button is pushed.

Index

20 MHz OFDM Signal Pattern 413

40 MHz OFDM Signal Pattern 413

802.11 adapter drivers 531

802.11 Architecture Terms 86

802.11 Communications 73, *87*

802.11 Frame Types 170

802.11 Frames 147

802.11 General Frame Format 156

802.11 PHY 206

802.11 PHY (PLCP) Header 212

802.11 PHY Preamble 209

802.11 State Machine 93

802.11-2012 121

802.11ac APs 272

802.11e 111

802.11g 211

802.11i (Robust Security Networks (RSNs)) 251

802.11s 121

802.2 Logical Link Control (LLC) sublayer 80

A+ objectives 9

access points (APs) 242

access ports 243

ACI 348

ACK *171*

ACK frames 193

Acknowledgement (ACK) Frames 193

Acrylic Wi-Fi 405

Acrylic Wi-Fi Home 135

Acrylic Wi-Fi Professional 502

Action 170

Active Scanning with Probe Request and Probe Response Frames 90

Adapter Limitations 531

Address 1, 2, 3, and 4 165

Address 1-4 333

AirMagnet Spectrum XT 366

AirMagnet Wi-Fi Analyzer Pro 314

Aliases 334

Amplitude 381

Analyzing Wired Traffic 351

Analyzing WLAN Traffic 332

antenna beamwidths 392

Antenna Factors 392

antennas 252

AP Antenna Gain 273

AP Antennas 272

AP Configuration Processes 269

AP Data Rates 276

AP Management 275

AP Management Capabilities 263

AP Mounting Options 266

AP Ports 272

AP Power Options 277

AP QoS 274

AP Receive Sensitivity 277

AP Security 273

AP Security Capabilities 263

AP Spec Sheet 270

AP Standards 271

AP Transmit Power 276

AP WLAN Capabilities 276

Application Layer *18*

Applied Analysis 344

Arbitration IFS (AIFS) 108

Arrival Time 333

Association *87*, 99, 170

Association and Disassociation Frames 187

association identifier (AID) 151

Authenticated/Associated 93

Authenticated/Unassociated 93

Authentication *87*, 95, 170, 516

Authentication frames 185

Authentication Server 199

Authenticator 199

automatic rate shifting 115

Autonomous Access Points 243

Availability 471

Azimuth 394

Basic Service Area (BSA) *86*, 250

Basic Service Set (BSS) *86*

Basic Service Set Identifier (BSSID) *86*

Beacon 170

Beacon Frame Timing 197

Beacon Frames 88, 173

Beacon Interval 88

bit 76

Bits, Bytes, and Octets 76

BlockAck *171*

BlockAckReq *171*

Bluetooth Signal Pattern 414

Border Gateway Protocol (BGP) 295

bridge mode 248

Broadcast 451

broadcast address 155

bytes 76

cable classifications/categories 465

cable failure 470

Cable Faults 464

cable tester 470

Cached or Pre-configured Information 452

Capability Information 88

Capacity analysis 345

Capturing Wired Traffic 350

Capturing WLAN Traffic 329

Carrier Sense 104

Carrier Sense/Clear Channel Assessment 209

CCI 162, 348, 496, 498, 539, 541

CCI and ACI 346

Centralized WLAN Architecture or Split MAC 126

Certificate servers (public key infrastructure (PKI)) 296

CF cards 237

CF Parameter Set 89

Channel performance 346

channel scanning 319

Channel utilization 346

Cisco CleanAir 367

Cisco Troubleshooting Process 3

class of service (CoS) 460

clear channel assessment (CCA) 104

Client Device Types and Functions 230

Client Issues 530

Client Security 528

Cloud-based Architecture 127

Co-Channel and Adjacent-Channel Interference 497

collision avoidance (CA) 102, 110

collision detection (CD) 102

common ports 456

Common Wireless Architectures 124

Common WLAN Issues 493

CommView for WiFi 315

CommView for WiFi channel usage 503

CommView for WiFi configuration interface 325

CommView for WiFi dashboard 323

CommView for WiFi installation 569

CommView for WiFi Options dialog 327

CommView for WiFi supported adapters 316

Compact Flash cards 237

CompTIA Methodologies 9

Configuration Errors 532

contention window (CW) 109, 167

Control Frames 171

Control Wrapper *171*

Cooperative Control 133

Cordless Phone Signal Pattern 417

crimping tool 468

crossover cable 467

CSMA/CA 102

CSMA/CA coordination functions 511

CTS *171*

CWNP Methodology 11

DA and SA Fields 154

Data Field 155

Data Frames 171

Data Link Layer *29*, 80

Data Protection *87*

Database servers 296

Data-Rate Factors 115

dBd 380

dBi 380

dBm 377

DBPSK—Differential Binary Phase Shift Keying (BPSK) 216

Deauthentication 99, 170

Deauthentication frames 186

Decibel (dB) 372

Default and Misconfigured Settings 520

Default and Weak Passwords 520

Default Configuration Settings 520

Delta Time 333

Destination Address (DA) 154, 462

Detecting Multipath 507

Device Form Factors 236

DHCP 451

DHCP Issues 450

DHCP location 450

DHCP negative acknowledgement 450

DHCP option 43 126

DHCP pool depletion 450

DHCP servers *296*

DHCP traffic analysis 352

Differentiated Services Code Point (DSCP) 457

DIFS interval 108

Disassociation 102, 170

Discovery Protocols 527

Distributed (Coordination Function) Interframe Space (DIFS) 108

Distributed Coordination Function (DCF) 102

Distribution System (DS) *86*

Distribution System Medium (DSM) *86*

DNS 451

DNS Issues 446

DNS servers *296*

DNS traffic analysis 352

Domain Name System (DNS) 438

Drivers 531

Dropped calls 513

DSSS Parameter Set 89

DSSS—Direct Sequence Spread Spectrum 216

dual-band 231, 272

Duration field 192

Duration/ID field 164

Duty Cycle 397

Dynamic Host Configuration Protocol (DHCP) 440

Dynamic rate selection 115

dynamic rate shifting 115

dynamic rate switching 115

EAP Frames 201

EAPoL protocol 200

EDCAF (Enhanced Distributed Coordination Access Function) 111

Elevation 394

Encapsulation 36

Encryption 516

End-to-End QoS 462

Equipment Installation 530

Equivalent Isotropically Radiated Power (EIRP) 391

ERP Information 89

ERP—Extended Rate PHY 216

Ethernet and Other Wired Connectivity 258

Ethernet Frames 152

Ethernet Switches 286

Ethertype 155

experiential expertise 14

Expert analysis 322

ExpressCard 239

Extended Interframe Space (EIFS) 108

Extended Service Set (ESS) *86*

Extended Supported Rates 89

Extension field 156

Fade Margin 390

fat APs 243

FCC ID 231, 233

FCS 169

FCS field 156

FFT Duty Cycle 397

FH Parameter Set 88

Filtering 253, 321

Firmware Upgrades 521

Font configuration 327

Fragmentation *88*

frame 75

Frame Body field 169

Frame capture 318

Frame Check Sequence (FCS) 154

Frame Check Sequence field 169

Frame Control 160

Frame Control field 160

Frame decoding 320

Frame Transmission *87*

frames 148

free space path loss (FSPL or FPL) 386

Frequency 381

Group addresses 154

Hardware Troubleshooting 445

HCF (Hybrid Coordination Function) 111

Hidden Nodes 508

highlighting or colorization 321

Home office troubleshooting 476

Hotspot Support 261

HR/DSSS—High Rate DSSS 216

HT Capabilities 89

HT Control field 160, 167

HT Control Middle subfield 168

HT Operation 90

HT PHY 212

HT-Greenfield *212*

HT—High Throughput 216

HT-Mixed PPDU *212*

Hubbing Out 350

Hybrid WLAN Architecture 126

IBSS Parameter Set 89

ICMP ECHO 47

Identity servers 296

IEEE Standards Support 251

IGRP (Interior Gateway Routing Protocol) 295

Independent Basic Service Set (IBSS 114

Independent Basic Service Set (IBSS) *86*, 90

Infrastructure Basic Service Set (BSS) 114

inSSIDer 405

Installing WLAN Analysis Software 555

Insufficient Capacity 495

integrated services routers (ISRs) 290

Intelligent Edge or Distributed 124

Intentional Radiator 391

interframe space (IFS) 105

Interframe Spacing 105

Internet Connectivity problems 474

Internet of Things (IoT) 534

Inter-Switch Link (ISL) frames 461

inter-VAP filtering 255

IP Routers 290

IPCONFIG 444

iPerf 41

IS-IS (Intermediate System to Intermediate System) 295

Laptop spectrum analysis adapters 284

Layer 1 32

Layer 2 29

Layer 2 QoS 460

Layer 3 27

Layer 3 QoS 458

Layer 4 25

Layer 5 23

Layer 6 21

Layer 7 19

LDAP Packets 205

Least significant bit (LSB) 151

Length/Type Field 155

lightweight APs 243

Lightweight Directory Access Protocol (LDAP) 205

Link Adaptation Control field 168

Link Adaptation Control subfield 168

Link Budget 386

LinkSprinter 445, 457

Load Planning 346

locally-administered address 155

Locating Devices 421

Logical Link Control (LLC) sublaye 84

long-guard interval 118

LSB first (LSBF) 151

MAC 79

MAC address filtering 253

MAC Layer Management Entity (MLME) 207

MAC protocol data unit 82

Management Frames 170

Media Access Control (MAC) sublayer 80

mesh function 260

Mesh Networking 260

mesh wireless access layers 123

Metageek Chanalyzer 285, 368

Metageek Chanalyzer band/channel selection 409

Metageek Chanalyzer channel tab 403

Metageek Chanalyzer device location feature 421

Metageek Chanalyzer FFT (density graph) view 401

Metageek Chanalyzer interferer identifiers 412

Metageek Chanalyzer report builder 404

Metageek Chanalyzer RF-activity waterfall view 401

Metageek Chanalyzer Wi-Fi integration 405

Metageek Wi-Spy DBx 366

Microsoft Troubleshooting Process 8

Microwave Oven Signal Pattern 420

milliwatts (mW) 371

MIMO 253

MIMO PHY 122

Mini-PCI cards 239

Mobile Device Management (MDM) 517

Modern Issues 534

modulation 215

monitor mode 318

Monitoring servers 296

More Data field 163

More Fragments subfield 162

Most significant bit (MSB) 150

Most significant bit first (MSBF) 151

MPDU 82

MSDU 81, 82

Multicast addresses 154

Multipath 506

Multiple Channel Architecture (MCA) 127

multipoint-to-multipoint (MPtMP) 120

Multirate support 115

Multi-User-MIMO (MU-MIMO) 535

Narrowband interference 505

NAV timer 104

Near-Far Problem 510

NETSH 50, 444

NETSH WLAN SHOW DRIVERS 52

NETSH WLAN SHOW INTERFACES 53

NETSH WLAN SHOW NETWORKS 54

NETSH WLAN SHOW PROFILES 53

Netstat 49

network allocation vector (NAV) 104

Network Allocation Vector (NAV) 85

network interface card (NIC) 230

Network Layer *27*

Network+ objectives 10

Network-Based Application Recognition (NBAR) 461

Networking Tools 40

New Operational Bands 536

Non-HT PPDU *212*

non-promiscuous mode 318

NSLookup 49, 444

NTP servers 296

NTP service 471

Null Data frames 194

octet 35, 76, 152

OFDM PHY 107

OFDM—Orthogonal Frequency Division Multiplexing 216

OmniPeek 308, 315

OmniPeek channel usage 502

OmniPeek dashboard 323

OmniPeek font configuration 327

OmniPeek network utilization graph 345

OmniPeek options window 325

OmniPeek packet size distribution graph 347

OmniPeek QoS tagging 352

Open System Authentication 96

Open Systems Interconnection (OSI) Model 15

Operating System Bugs and Vulnerabilities 533

Operating System Commands 444

Operating System Tools 45

Operational Modes 247

Order field 163

OSI Model 16

OSPF (Open Shortest Path First) 295

Packet size distribution 347

packet slicing 321

packet truncating 321

Passive Scanning with Beacon Frames 93

pathping 49

PC Cards 239

PCI 239

PCI Express (PCIe) 239

PCMCIA adapter card 237

Performance Monitor 473

Performing Spectrum Analysis 410

Phase 381

PHY 79

PHY Limitations 495

Physical Layer *31*

Physical Layer Convergence Protocol (PLCP) 80

Physical Layer Convergence Protocol (PLCP) sublayer 206

Physical Layer Management Entity (PLME) 207

Physical Medium Dependent (PMD) 80

Physical Medium Dependent (PMD) sublayer 206

physical signaling sublayer (PLC) 153

PING 46, 444

PLCP protocol data unit (PPDU) 206

PLCP Service Data Unit (PSDU) 206

PoE Issues 456

Point (Coordination Function) Interframe Space (PIFS) 107

Point Coordination Function (PCF) frames 172

Policy non-compliance 516

Port Mirroring (Port Spanning) 350

Portal *86*

Power Management *88*

Power Management (PM) bit 195

Power Management field 163

Power over Ethernet (PoE) 259, 443

Power Save Poll (PS-Poll) frames 195

PPDU 82

Preamble 153

Presentation Layer *21*

Pre-Shared Key (PSK) 198

probabilistic prioritization 514

Probe 170

Probe Request and Probe Response Frames 183

Promiscuous mode 318

Protected Frame field 163

protection mechanisms 348

Protocol Analysis 307, 317

Protocol Analysis Hardware 285, 309

Protocol Analysis Software 313

protocol analyzer 44, 182, 308, 536

protocol analyzer software 308

Protocol Analyzers 443

protocol data units 82

Protocol filtering 254

Protocol Overhead 346

Protocol Version bits 160

PSDU 82

QAM—Quadrature Amplitude Modulation 216

QBPSK—Quadrature Binary Phase Shift Keying (QPSK) 216

QoS access points (QoS AP) 112

QoS common problems 463

QoS Configuration Problems 514

QoS Control field 160, 166

QoS Issues 457

QoS settings 455

QoS stations (QoS STA) 112

QoS traffic analysis 352

Quality of Service (QoS) 251, 438

Radio Cards 255

RADIUS Packets 202

RADIUS protocol 200

Reachability 471

Reassociation *87*, 101, 170

Reassociation Request and Response Frames 188

Receive (Rx) 209

Received Signal Strength Indicator (RSSI) 383

Recognizing Patterns 411

Reduced IFS (RIFS) 107

Redundancy 472

Relative Time 333

Remote Authentication Dial-In User Service (RADIUS) 202

Remote Configuration 527

remote packet capture (RPCAP) 285

repeater mode 249

Reporting servers 296

Request to Send (RTS) and Clear to Send (CTS) Frames 192

Request to Send/Clear to Send (RTS/CTS) 113

Resolution bandwidth (RBW) 398

Resource Monitor 473

Results of Multipath 506

Retries and CRCs 346

Retry count 346

Retry field 163

RF Cell Sizing 525

RF Interference 505

RF metrics 330

RF noise 505

RF Noise and Noise Floor 504

RIP, the Routing Information Protocol 296

RJ-45 connector 467

Roaming delays 516

rogue wireless equipment 522

root mode 247

routing protocols 294

RSN 89

RTS *171*

RTS/CTS *88*, 113, 509

Scanning *87*

SD cards 238

Secure Digital IO cards 238

Security 198

Security baselines in 802.11 wireless networks 517

Security Issues 516

Segmentation 35

sequence control field 166

Service availability problems 471

service set identifier (SSID) 86, 517

Service traffic analysis 352

Session Layer *23*

SFD 153

Shannon-Hartley theorem 116

Shared Key Authentication 97

shielded twisted pair (STP) 465

Short Interframe Space (SIFS) 106

short-guard interval (SGI) 117

SHOW DRIVERS 51

SHOW INTERFACES 51

SHOW NETWORKS 51

SHOW PROFILES 51

SIFS interval 107

SIFS time interval 107

signal-to-noise ratio (SNR) 116, 382

Single MAC Model (Edge, Autonomous, or Standalone) 118

Single-channel architecture (SCA) 131

Site survey software (or planning software) 536

slot time 107

sniffer 329

SNMP Community Strings 526

Solutions for Multipath 507

Source Address (SA) 154

Source, Destination, BSSID 333

Spectrum Analysis Hardware 284, 366

spectrum analysis software 368

spectrum analysis terminology 369

spectrum analyzer 38

Spectrum Analyzer Features 399

Spectrum analyzer installing and configuring 407

Spectrum analyzer views 399

Spectrum analyzer Wi-Fi 405

Spectrum Analyzers 44, 536

Spectrum analyzers reports 403

Spectrum XT automatic device identification 412

Spectrum XT channel summary 402

Spectrum XT FFT view 400

Spectrum XT report 406

Spectrum XT report builder 403

Spectrum XT spectrogram view 402

Spectrum XT Wi-Fi integration 406

Split MAC Model (Centralized) 119

SSID 88

SSID Calc 499

Staging and Testing 529

Start Frame Delimiter (SFD) field 210

start-of-frame delimiter (SFD) 153

Station (STA) *86*

station management entity (SME) 207

Supplicant 199

Supplicant Issues 533

Supported Rates 89

supporting remote office workers 477

Sweep Cycles 397

Switch Configuration 442

Switching and Routing Issues 455

Synchronization *87*

Synchronization (Sync) field 210

System Operating Margin (SOM) 386

TamoSoft's Throughput Tester 42

target beacon transmission time (TBTT) 197

Telecommuters 476

thick APs 243

thin APs 243

throughput testers 41

TIM 89

Timestamp 88

TRACEROUTE 47, 444

tracert 48

Transmit (Tx) 209

Transmit Power Control (TPC) 511

Transport Layer *25*

Trigger frames 196

Troubleshooting Issues 443

Troubleshooting Layers 38

Troubleshooting Methodologies 2

Troubleshooting Tools 443

Troubleshooting Voice-Over-WLAN (VoWLAN) Issues 512

Troubleshooting Wired-Side QoS 463

truncating 321

TShark 560

Unauthenticated/Unassociated 93

Unified WLAN Architecture 127

unmanaged switch 286

unshielded twisted pair (UTP) 465

Usage breakdown by data rate 346

Usage breakdown by frame types 346

USB adapters 236

User Priority (UP) value 112

Utilization 399

UTP EIA/TIA Cable Classifications 465

Variable output power 256

vendor class identifier (VCI) 478

Vendor Methodologies 2

VHT Capabilities 90

VHT Operation 90

VHT PHY 212

VHT subfield 168

VHT—Very High Throughput 216

Video Transmitter Signal Pattern 418

View Available Networks (VAN) 474

Virtual APs (VAPs) 255

Virtual or Physical Addresses 333

VoWLAN roaming 514

VPN 477

watt (W) 370

Wavelength 381

Weather-related Issues 512

wideband interference 505

Wideband Jammer Signal Pattern 418

Wi-Fi adapter’s off/on status 531

Wi-Fi Analyzer Pro dashboard 322

Wi-Fi Certified Passpoint 261

Wi-Fi metrics 330

Wi-Fi scanner 182, 405

Wired Hardware 286

Wired Issues 437

wired networking analysis 349

Wired Traffic 350

Wired-side Limitations 496

Wireless Analysis Hardware 284

wireless client stations (STAs) 243

Wireless Mesh 120

Wireless Multimedia (WMM) 113

wireless STA to wireless STA filtering 255

Wireshark 156, 314

Wireshark ACK filter 194

Wireshark association request and response filter 188

Wireshark authentication filter 186

Wireshark beacon filter 182

Wireshark colorization 185, 334, 336

Wireshark DHCP option 43 capture 453

Wireshark DNS response capture 449

Wireshark download 557

Wireshark filters 341

Wireshark installation 556

Wireshark Network Analysis 349

Wireshark packet lengths 343

Wireshark probe request and response filter 183

Wireshark protocol analyzer 350

Wireshark protocol hierarchy statistics 343

Wireshark PS Poll filter 194, 197

Wireshark reassociation request and response filter 191

Wireshark RTS/CTS filter 193

Wireshark TKIP PSK capture 198

Wireshark WLAN Statistics 341

WLAN Analysis Hardware and Software 308

WLAN Architectures 118

WLAN Controller Access 442

WLAN Controller Configuration Process 282

WLAN Controller Issues 451

WLAN Controllers and Managers 278

WLAN Hardware 229

WLAN Network Management System or Centralized Management with Distributed Processing 125

WLAN protocol analyzer dashboards 322

WLAN protocol analyzer installing and configuring 324

WLAN PtMP model 118

WLAN QoS (wireless multimedia (WMM)) 514

WMM (802.11e) 514

WMM-PS 196

WPA and WPA2 Personal 198

WPA2 Enterprise 199

US·MLE
United States
Medical
Licensing
Examination
®

-
-
-
-
-

(A)
(B)
(C)
(D)
(E)

*

*

*

*

*

*

*

*

*

*
*

(A)
(B)
(C)
(D)
(E)

2.

(A)
(B)
(C)
(D)
(E)

3.

(A)
(B)
(C)
(D)
(E)

4.

(A)
(B)
(C)
(D)
(E)

-year-

5.

(A)
(B)
(C)
(D)
(E)

6.

(A)
(B)
(C)
(D)
(E)

7.

(A)
(B)
(C)
(D)
(E)
(F)

8.

(A)
(B)

-year-

9.

(A)
(B)
(C)
(D)
(E)

10.

(A)
(B)
(C)
(D)
(E)
(F)

11.

(A)
(B)
(C)
(D)
(E)
(F)

12.

(A)
(B)
(C)
(D)
(E)

13.

(A)
(B)
(C)
(D)
(E)

14.

(A)
(B)
(C)
(D)
(E)

-year-

15.

(A)
(B)
(C)
(D)
(E)

16.

(A)
(B)
(C)
(D)
(E)

17.

(A)
(B)
(C)
(D)

18.

(A)
(B)
(C)
(D)
(E)
(F)

19.

(A)
(B)
(C)
(D)
(E)

20.

(A)
(B)
(C)
(D)
(E)

21.

(A)
(B)
(C)
(D)
(E)

22.

(A)
(B)
(C)

-year-

(D)

(E)

23.

(A)

(B)

(C)

(D)

(E)

24.

(A)

(B)

(C)

(D)

(E)

25.

(A)

(B)

(C)

(D)

(E)

26.

(A)
(B)
(C)
(D)
(E)

27.

(A)
(B)
(C)
(D)
(E)

28.

(A)
(B)
(C)
(D)
(E)

29.

(A)
(B)
(C)
(D)
(E)

30.

(A)
(B)
(C)
(D)
(E)

31.

(A)
(B)
(C)
(D)
(E)
(F)

32.

(A)

(A)
(B)
(C)
(D)
(E)

33.

(A)
(B)
(C)
(D)
(E)

34.

(A)
(B)
(C)
(D)
(E)

35.

(A)
(B)
(C)
(D)

36.

(A)
(B)
(C)

37.

(A)
(B)
(C)
(D)
(E)

38.

(A)
(B)
(C)
(D)
(E)

39.

(A)
(B)
(C)
(D)
(E)

40.

(A)
(B)
(C)
(D)
(E)

41.

(C)
(D)
(E)

42.

(A)
(B)
(C)
(D)

43.

(A)
(B)
(C)
(D)
(E)

-year-

44.

(A)
(B)
(C)
(D)
(E)
(F)

45.

(A)
(B)
(C)
(D)
(E)

46.

(A)
(B)
(C)
(D)
(E)

47.

(A)
(B)
(C)
(D)
(E)

-year-

48.

(A)
(B)
(C)
(D)
(E)
(F)

49.

(A)
(B)
(C)
(D)
(E)
(F)

50.

(A)
(B)
(C)
(D)
(E)

51.

(A)
(B)
(C)
(D)
(E)

-year-

52.

(A)
(B)
(C)
(D)
(E)
(F)
(G)

53.

(A)
(B)
(C)
(D)
(E)

54.

(A)
(B)
(C)
(D)

55.

(A)
(B)
(C)
(D)
(E)

-year-

56.

(A)
(B)
(C)
(D)
(E)

57.

(A)
(B)
(C)
(D)
(E)

58.

(A)
(B)
(C)
(D)
(E)

59.

(A)
(B)
(C)
(D)
(E)

-year-

60.

(A)
(B)
(C)
(D)
(E)

61.

(A)
(B)
(C)
(D)
(E)

62.

(A)
(B)
(C)
(D)

63.

(A)
(B)
(C)
(D)
(E)

64.

-year-

(A)

(B)

(C)

(D)

(E)

(F)

65.

(A)
(B)
(C)
(D)
(E)

66.

(A)
(B)
(C)
(D)
(E)

67.

(A)
(B)
(C)
(D)
(E)

68.

(A)
(B)
(C)
(D)
(E)

69.

(A)
(B)
(C)
(D)
(E)

70.

(A)
(B)
(C)
(D)

71.

(A)
(B)
(C)
(D)

72.

(A)

(A)
(B)
(C)
(D)
(E)

73.

(A)
(B)
(C)
(D)
(E)

74.

(A)
(B)
(C)
(D)
(E)

75.

(A)
(B)
(C)
(D)
(E)

76.

(A)
(B)
(C)
(D)
(E)

77.

(A)
(B)
(C)
(D)
(E)

78.

(A)
(B)
(C)
(D)
(E)
(F)

79.

(A)
(B)
(C)
(D)
(E)

80.

(A)
(B)
(C)
(D)
(E)
(F)
(G)
(H)

81.

(A)
(B)
(C)
(D)
(E)
(F)

82.

(A)
(B)
(C)
(D)
(E)

83.

(A)
(B)
(C)
(D)
(E)

84.

(A)
(B)
(C)
(D)
(E)

(F)

85.

(A)
(B)
(C)
(D)
(E)
(F)

86.

(A)
(B)
(C)
(D)
(E)

87.

(A)
(B)
(C)
(D)
(E)

88.

(A)
(B)
(C)
(D)
(E)

89.

90.

(A)
(B)
(C)
(D)
(E)
(F)

91.

(A)
(B)
(C)
(D)
(E)

92.

(A)
(B)
(C)
(D)
(E)

93.

(A)
(B)
(C)
(D)

94.

(A)
(B)
(C)
(D)
(E)

95.

(A)
(B)
(C)
(D)

96.

(A)
(B)
(C)
(D)

(E)

97.

(A)
(B)
(C)
(D)

98.

(A)
(B)
(C)
(D)
(E)

99.

(A)
(B)
(C)
(D)

(E)

100.

(A)

(B)

101.

(A)
(B)
(C)
(D)

102.

(A)
(B)
(C)
(D)
(E)

103.

(A)
(B)
(C)

104.

(A)
(B)
(C)
(D)
(E)
(F)

105.

(A)
(B)
(C)
(D)
(E)

106.

(A)
(B)
(C)
(D)
(E)

107.

(A)
(B)
(C)
(D)

(E)

108.

(A)
(B)
(C)
(D)

109.

(A)
(B)
(C)
(D)
(E)

110.

(A)
(B)
(C)
(D)
(E)

111.

(A)
(B)
(C)
(D)
(E)

112.

(A)
(B)
(C)
(D)
(E)

113.

(A)
(B)
(C)
(D)

114.

(A)
(B)
(C)
(D)
(E)

115.

(A)

(B)
(C)
(D)
(E)

116.

(A)
(B)
(C)
(D)
(E)

117.

(A)
(B)
(C)
(D)
(E)

49.
50.

87.
88.
89.
90.

1.
2.
4.
5.
6.
7.
8.
9.
10.

41.
42.
43.
46.
47.
48.
49.
50.

81.
82.
83.
84.
85.
86.
87.
88.
89.
90.

US·MLE
United States
Medical
Licensing
Examination
®

-
-
-
-
-

(A)
(B)
(C)
(D)
(E)

*

*

*

*

*

*

*

*

*

*
*

(A)
(B)
(C)
(D)
(E)

2.

(A)
(B)
(C)
(D)
(E)

3.

(A)
(B)
(C)
(D)
(E)

4.

(A)
(B)
(C)
(D)
(E)

-year-

5.

(A)
(B)
(C)
(D)
(E)

6.

(A)
(B)
(C)
(D)
(E)

7.

(A)
(B)
(C)
(D)
(E)
(F)

8.

(A)
(B)

-year-

9.

(A)
(B)
(C)
(D)
(E)

10.

(A)
(B)
(C)
(D)
(E)
(F)

11.

(A)
(B)
(C)
(D)
(E)
(F)

12.

(A)
(B)
(C)
(D)
(E)

13.

(A)
(B)
(C)
(D)
(E)

14.

(A)
(B)
(C)
(D)
(E)

-year-

15.

(A)
(B)
(C)
(D)
(E)

16.

(A)
(B)
(C)
(D)
(E)

17.

(A)
(B)
(C)
(D)

18.

(A)
(B)
(C)
(D)
(E)
(F)

19.

(A)
(B)
(C)
(D)
(E)

20.

(A)
(B)
(C)
(D)
(E)

21.

(A)
(B)
(C)
(D)
(E)

22.

(A)
(B)
(C)

-year-

(D)

(E)

23.

(A)

(B)

(C)

(D)

(E)

24.

(A)

(B)

(C)

(D)

(E)

25.

(A)

(B)

(C)

(D)

(E)

26.

(A)
(B)
(C)
(D)
(E)

27.

(A)
(B)
(C)
(D)
(E)

28.

(A)
(B)
(C)
(D)
(E)

29.

(A)
(B)
(C)
(D)
(E)

30.

(A)
(B)
(C)
(D)
(E)

31.

(A)
(B)
(C)
(D)
(E)
(F)

32.

(A)

(A)
(B)
(C)
(D)
(E)

33.

(A)
(B)
(C)
(D)
(E)

34.

(A)
(B)
(C)
(D)
(E)

35.

(A)
(B)
(C)
(D)

36.

(A)
(B)
(C)

37.

(A)
(B)
(C)
(D)
(E)

38.

(A)
(B)
(C)
(D)
(E)

39.

(A)
(B)
(C)
(D)
(E)

40.

(A)
(B)
(C)
(D)
(E)

41.

(C)
(D)
(E)

42.

(A)
(B)
(C)
(D)

43.

(A)
(B)
(C)
(D)
(E)

-year-

44.

(A)
(B)
(C)
(D)
(E)
(F)

45.

(A)
(B)
(C)
(D)
(E)

46.

(A)
(B)
(C)
(D)
(E)

47.

(A)
(B)
(C)
(D)
(E)

-year-

48.

(A)
(B)
(C)
(D)
(E)
(F)

49.

(A)
(B)
(C)
(D)
(E)
(F)

50.

(A)
(B)
(C)
(D)
(E)

51.

(A)
(B)
(C)
(D)
(E)

-year-

52.

(A)
(B)
(C)
(D)
(E)
(F)
(G)

53.

(A)
(B)
(C)
(D)
(E)

54.

(A)
(B)
(C)
(D)

55.

(A)
(B)
(C)
(D)
(E)

-year-

56.

(A)
(B)
(C)
(D)
(E)

57.

(A)
(B)
(C)
(D)
(E)

58.

(A)
(B)
(C)
(D)
(E)

59.

(A)
(B)
(C)
(D)
(E)

-year-

60.

(A)
(B)
(C)
(D)
(E)

61.

(A)
(B)
(C)
(D)
(E)

62.

(A)
(B)
(C)
(D)

63.

(A)
(B)
(C)
(D)
(E)

64.

-year-

(A)

(B)

(C)

(D)

(E)

(F)

65.

(A)
(B)
(C)
(D)
(E)

66.

(A)
(B)
(C)
(D)
(E)

67.

(A)
(B)
(C)
(D)
(E)

68.

(A)
(B)
(C)
(D)
(E)

69.

(A)
(B)
(C)
(D)
(E)

70.

(A)
(B)
(C)
(D)

71.

(A)
(B)
(C)
(D)

72.

(A)

(A)
(B)
(C)
(D)
(E)

73.

(A)
(B)
(C)
(D)
(E)

74.

(A)
(B)
(C)
(D)
(E)

75.

(A)
(B)
(C)
(D)
(E)

76.

(A)
(B)
(C)
(D)
(E)

77.

(A)
(B)
(C)
(D)
(E)

78.

(A)
(B)
(C)
(D)
(E)
(F)

79.

(A)
(B)
(C)
(D)
(E)

80.

(A)
(B)
(C)
(D)
(E)
(F)
(G)
(H)

81.

(A)
(B)
(C)
(D)
(E)
(F)

82.

(A)
(B)
(C)
(D)
(E)

83.

(A)
(B)
(C)
(D)
(E)

84.

(A)
(B)
(C)
(D)
(E)

(F)

85.

(A)
(B)
(C)
(D)
(E)
(F)

86.

(A)
(B)
(C)
(D)
(E)

87.

(A)
(B)
(C)
(D)
(E)

88.

(A)
(B)
(C)
(D)
(E)

89.

90.

(A)
(B)
(C)
(D)
(E)
(F)

91.

(A)
(B)
(C)
(D)
(E)

92.

(A)
(B)
(C)
(D)
(E)

93.

(A)
(B)
(C)
(D)

94.

(A)
(B)
(C)
(D)
(E)

95.

(A)
(B)
(C)
(D)

96.

(A)
(B)
(C)
(D)

(E)

97.

(A)
(B)
(C)
(D)

98.

(A)
(B)
(C)
(D)
(E)

99.

(A)
(B)
(C)
(D)

(E)

100.

(A)

(B)

101.

(A)
(B)
(C)
(D)

102.

(A)
(B)
(C)
(D)
(E)

103.

(A)
(B)
(C)

104.

(A)
(B)
(C)
(D)
(E)
(F)

105.

(A)
(B)
(C)
(D)
(E)

106.

(A)
(B)
(C)
(D)
(E)

107.

(A)
(B)
(C)
(D)

(E)

108.

(A)
(B)
(C)
(D)

109.

(A)
(B)
(C)
(D)
(E)

110.

(A)
(B)
(C)
(D)
(E)

111.

(A)
(B)
(C)
(D)
(E)

112.

(A)
(B)
(C)
(D)
(E)

113.

(A)
(B)
(C)
(D)

114.

(A)
(B)
(C)
(D)
(E)

115.

(A)

(B)
(C)
(D)
(E)

116.

(A)
(B)
(C)
(D)
(E)

117.

(A)
(B)
(C)
(D)
(E)

49.
50.

87.
88.
89.
90.

1.
2.
4.
5.
6.
7.
8.
9.
10.

41.
42.
43.
46.
47.
48.
49.
50.

81.
82.
83.
84.
85.
86.
87.
88.
89.
90.

US·MLE
United States
Medical
Licensing
Examination
®

-
-
-
-
-

(A)
(B)
(C)
(D)
(E)

*

*

*

*

*

*

*

*

*

*
*

(A)
(B)
(C)
(D)
(E)

2.

(A)
(B)
(C)
(D)
(E)

3.

(A)
(B)
(C)
(D)
(E)

4.

(A)
(B)
(C)
(D)
(E)

-year-

5.

(A)
(B)
(C)
(D)
(E)

6.

(A)
(B)
(C)
(D)
(E)

7.

(A)
(B)
(C)
(D)
(E)
(F)

8.

(A)
(B)

-year-

9.

(A)
(B)
(C)
(D)
(E)

10.

(A)
(B)
(C)
(D)
(E)
(F)

11.

(A)
(B)
(C)
(D)
(E)
(F)

12.

(A)
(B)
(C)
(D)
(E)

13.

(A)
(B)
(C)
(D)
(E)

14.

(A)
(B)
(C)
(D)
(E)

-year-

15.

(A)
(B)
(C)
(D)
(E)

16.

(A)
(B)
(C)
(D)
(E)

17.

(A)
(B)
(C)
(D)

18.

(A)
(B)
(C)
(D)
(E)
(F)

19.

(A)
(B)
(C)
(D)
(E)

20.

(A)
(B)
(C)
(D)
(E)

21.

(A)
(B)
(C)
(D)
(E)

22.

(A)
(B)
(C)

-year-

(D)

(E)

23.

(A)

(B)

(C)

(D)

(E)

24.

(A)

(B)

(C)

(D)

(E)

25.

(A)

(B)

(C)

(D)

(E)

26.

(A)
(B)
(C)
(D)
(E)

27.

(A)
(B)
(C)
(D)
(E)

28.

(A)
(B)
(C)
(D)
(E)

29.

(A)
(B)
(C)
(D)
(E)

30.

(A)
(B)
(C)
(D)
(E)

31.

(A)
(B)
(C)
(D)
(E)
(F)

32.

(A)

(A)
(B)
(C)
(D)
(E)

33.

(A)
(B)
(C)
(D)
(E)

34.

(A)
(B)
(C)
(D)
(E)

35.

(A)
(B)
(C)
(D)

36.

(A)
(B)
(C)

37.

(A)
(B)
(C)
(D)
(E)

38.

(A)
(B)
(C)
(D)
(E)

39.

(A)
(B)
(C)
(D)
(E)

40.

(A)
(B)
(C)
(D)
(E)

41.

(C)
(D)
(E)

42.

(A)
(B)
(C)
(D)

43.

(A)
(B)
(C)
(D)
(E)

-year-

44.

(A)
(B)
(C)
(D)
(E)
(F)

45.

(A)
(B)
(C)
(D)
(E)

46.

(A)
(B)
(C)
(D)
(E)

47.

(A)
(B)
(C)
(D)
(E)

-year-

48.

(A)
(B)
(C)
(D)
(E)
(F)

49.

(A)
(B)
(C)
(D)
(E)
(F)

50.

(A)
(B)
(C)
(D)
(E)

51.

(A)
(B)
(C)
(D)
(E)

-year-

52.

(A)
(B)
(C)
(D)
(E)
(F)
(G)

53.

(A)
(B)
(C)
(D)
(E)

54.

(A)
(B)
(C)
(D)

55.

(A)
(B)
(C)
(D)
(E)

-year-

56.

(A)
(B)
(C)
(D)
(E)

57.

(A)
(B)
(C)
(D)
(E)

58.

(A)
(B)
(C)
(D)
(E)

59.

(A)
(B)
(C)
(D)
(E)

-year-

60.

(A)
(B)
(C)
(D)
(E)

61.

(A)
(B)
(C)
(D)
(E)

62.

(A)
(B)
(C)
(D)

63.

(A)
(B)
(C)
(D)
(E)

64.

-year-

(A)

(B)

(C)

(D)

(E)

(F)

65.

(A)
(B)
(C)
(D)
(E)

66.

(A)
(B)
(C)
(D)
(E)

67.

(A)
(B)
(C)
(D)
(E)

68.

(A)
(B)
(C)
(D)
(E)

69.

(A)
(B)
(C)
(D)
(E)

70.

(A)
(B)
(C)
(D)

71.

(A)
(B)
(C)
(D)

72.

(A)

(A)
(B)
(C)
(D)
(E)

73.

(A)
(B)
(C)
(D)
(E)

74.

(A)
(B)
(C)
(D)
(E)

75.

(A)
(B)
(C)
(D)
(E)

76.

(A)
(B)
(C)
(D)
(E)

77.

(A)
(B)
(C)
(D)
(E)

78.

(A)
(B)
(C)
(D)
(E)
(F)

79.

(A)
(B)
(C)
(D)
(E)

80.

(A)
(B)
(C)
(D)
(E)
(F)
(G)
(H)

81.

(A)
(B)
(C)
(D)
(E)
(F)

82.

(A)
(B)
(C)
(D)
(E)

83.

(A)
(B)
(C)
(D)
(E)

84.

(A)
(B)
(C)
(D)
(E)

(F)

85.

(A)
(B)
(C)
(D)
(E)
(F)

86.

(A)
(B)
(C)
(D)
(E)

87.

(A)
(B)
(C)
(D)
(E)

88.

(A)
(B)
(C)
(D)
(E)

89.

90.

(A)
(B)
(C)
(D)
(E)
(F)

91.

(A)
(B)
(C)
(D)
(E)

92.

(A)
(B)
(C)
(D)
(E)

93.

(A)
(B)
(C)
(D)

94.

(A)
(B)
(C)
(D)
(E)

95.

(A)
(B)
(C)
(D)

96.

(A)
(B)
(C)
(D)

(E)

97.

(A)
(B)
(C)
(D)

98.

(A)
(B)
(C)
(D)
(E)

99.

(A)
(B)
(C)
(D)

(E)

100.

(A)

(B)

101.

(A)
(B)
(C)
(D)

102.

(A)
(B)
(C)
(D)
(E)

103.

(A)
(B)
(C)

104.

(A)
(B)
(C)
(D)
(E)
(F)

105.

(A)
(B)
(C)
(D)
(E)

106.

(A)
(B)
(C)
(D)
(E)

107.

(A)
(B)
(C)
(D)

(E)

108.

(A)
(B)
(C)
(D)

109.

(A)
(B)
(C)
(D)
(E)

110.

(A)
(B)
(C)
(D)
(E)

111.

(A)
(B)
(C)
(D)
(E)

112.

(A)
(B)
(C)
(D)
(E)

113.

(A)
(B)
(C)
(D)

114.

(A)
(B)
(C)
(D)
(E)

115.

(A)

(B)
(C)
(D)
(E)

116.

(A)
(B)
(C)
(D)
(E)

117.

(A)
(B)
(C)
(D)
(E)

49.
50.

87.
88.
89.
90.

1.
2.
4.
5.
6.
7.
8.
9.
10.

41.
42.
43.
46.
47.
48.
49.
50.

81.
82.
83.
84.
85.
86.
87.
88.
89.
90.

US·MLE
United States
Medical
Licensing
Examination
®

-
-
-
-
-

(A)
(B)
(C)
(D)
(E)

*

*

*

*

*

*

*

*

*

*
*

(A)
(B)
(C)
(D)
(E)

2.

(A)
(B)
(C)
(D)
(E)

3.

(A)
(B)
(C)
(D)
(E)

4.

(A)
(B)
(C)
(D)
(E)

-year-

5.

(A)
(B)
(C)
(D)
(E)

6.

(A)
(B)
(C)
(D)
(E)

7.

(A)
(B)
(C)
(D)
(E)
(F)

8.

(A)
(B)

-year-

9.

(A)
(B)
(C)
(D)
(E)

10.

(A)
(B)
(C)
(D)
(E)
(F)

11.

(A)
(B)
(C)
(D)
(E)
(F)

12.

(A)
(B)
(C)
(D)
(E)

13.

(A)
(B)
(C)
(D)
(E)

14.

(A)
(B)
(C)
(D)
(E)

-year-

15.

(A)
(B)
(C)
(D)
(E)

16.

(A)
(B)
(C)
(D)
(E)

17.

(A)
(B)
(C)
(D)

18.

(A)
(B)
(C)
(D)
(E)
(F)

19.

(A)
(B)
(C)
(D)
(E)

20.

(A)
(B)
(C)
(D)
(E)

21.

(A)
(B)
(C)
(D)
(E)

22.

(A)
(B)
(C)

-year-

(D)

(E)

23.

(A)

(B)

(C)

(D)

(E)

24.

(A)

(B)

(C)

(D)

(E)

25.

(A)

(B)

(C)

(D)

(E)

26.

(A)
(B)
(C)
(D)
(E)

27.

(A)
(B)
(C)
(D)
(E)

28.

(A)
(B)
(C)
(D)
(E)

29.

(A)
(B)
(C)
(D)
(E)

30.

(A)
(B)
(C)
(D)
(E)

31.

(A)
(B)
(C)
(D)
(E)
(F)

32.

(A)

(A)
(B)
(C)
(D)
(E)

33.

(A)
(B)
(C)
(D)
(E)

34.

(A)
(B)
(C)
(D)
(E)

35.

(A)
(B)
(C)
(D)

36.

(A)
(B)
(C)

37.

(A)
(B)
(C)
(D)
(E)

38.

(A)
(B)
(C)
(D)
(E)

39.

(A)
(B)
(C)
(D)
(E)

40.

(A)
(B)
(C)
(D)
(E)

41.

(C)
(D)
(E)

42.

(A)
(B)
(C)
(D)

43.

(A)
(B)
(C)
(D)
(E)

-year-

44.

(A)
(B)
(C)
(D)
(E)
(F)

45.

(A)
(B)
(C)
(D)
(E)

46.

(A)
(B)
(C)
(D)
(E)

47.

(A)
(B)
(C)
(D)
(E)

-year-

48.

(A)
(B)
(C)
(D)
(E)
(F)

49.

(A)
(B)
(C)
(D)
(E)
(F)

50.

(A)
(B)
(C)
(D)
(E)

51.

(A)
(B)
(C)
(D)
(E)

-year-

52.

(A)
(B)
(C)
(D)
(E)
(F)
(G)

53.

(A)
(B)
(C)
(D)
(E)

54.

(A)
(B)
(C)
(D)

55.

(A)
(B)
(C)
(D)
(E)

-year-

56.

(A)
(B)
(C)
(D)
(E)

57.

(A)
(B)
(C)
(D)
(E)

58.

(A)
(B)
(C)
(D)
(E)

59.

(A)
(B)
(C)
(D)
(E)

-year-

60.

(A)
(B)
(C)
(D)
(E)

61.

(A)
(B)
(C)
(D)
(E)

62.

(A)
(B)
(C)
(D)

63.

(A)
(B)
(C)
(D)
(E)

64.

-year-

(A)

(B)

(C)

(D)

(E)

(F)

65.

(A)
(B)
(C)
(D)
(E)

66.

(A)
(B)
(C)
(D)
(E)

67.

(A)
(B)
(C)
(D)
(E)

68.

(A)
(B)
(C)
(D)
(E)

69.

(A)
(B)
(C)
(D)
(E)

70.

(A)
(B)
(C)
(D)

71.

(A)
(B)
(C)
(D)

72.

(A)

(A)
(B)
(C)
(D)
(E)

73.

(A)
(B)
(C)
(D)
(E)

74.

(A)
(B)
(C)
(D)
(E)

75.

(A)
(B)
(C)
(D)
(E)

76.

(A)
(B)
(C)
(D)
(E)

77.

(A)
(B)
(C)
(D)
(E)

78.

(A)
(B)
(C)
(D)
(E)
(F)

79.

(A)
(B)
(C)
(D)
(E)

80.

(A)
(B)
(C)
(D)
(E)
(F)
(G)
(H)

81.

(A)
(B)
(C)
(D)
(E)
(F)

82.

(A)
(B)
(C)
(D)
(E)

83.

(A)
(B)
(C)
(D)
(E)

84.

(A)
(B)
(C)
(D)
(E)

(F)

85.

(A)
(B)
(C)
(D)
(E)
(F)

86.

(A)
(B)
(C)
(D)
(E)

87.

(A)
(B)
(C)
(D)
(E)

88.

(A)
(B)
(C)
(D)
(E)

89.

90.

(A)
(B)
(C)
(D)
(E)
(F)

91.

(A)
(B)
(C)
(D)
(E)

92.

(A)
(B)
(C)
(D)
(E)

93.

(A)
(B)
(C)
(D)

94.

(A)
(B)
(C)
(D)
(E)

95.

(A)
(B)
(C)
(D)

96.

(A)
(B)
(C)
(D)

(E)

97.

(A)
(B)
(C)
(D)

98.

(A)
(B)
(C)
(D)
(E)

99.

(A)
(B)
(C)
(D)

(E)

100.

(A)

(B)

101.

(A)
(B)
(C)
(D)

102.

(A)
(B)
(C)
(D)
(E)

103.

(A)
(B)
(C)

104.

(A)
(B)
(C)
(D)
(E)
(F)

105.

(A)
(B)
(C)
(D)
(E)

106.

(A)
(B)
(C)
(D)
(E)

107.

(A)
(B)
(C)
(D)

(E)

108.

(A)
(B)
(C)
(D)

109.

(A)
(B)
(C)
(D)
(E)

110.

(A)
(B)
(C)
(D)
(E)

111.

(A)
(B)
(C)
(D)
(E)

112.

(A)
(B)
(C)
(D)
(E)

113.

(A)
(B)
(C)
(D)

114.

(A)
(B)
(C)
(D)
(E)

115.

(A)

(B)
(C)
(D)
(E)

116.

(A)
(B)
(C)
(D)
(E)

117.

(A)
(B)
(C)
(D)
(E)

49.
50.

87.
88.
89.
90.

1.
2.
4.
5.
6.
7.
8.
9.
10.

41.
42.
43.
46.
47.
48.
49.
50.

81.
82.
83.
84.
85.
86.
87.
88.
89.
90.