cwnp®
Certified Wireless Network Professional

Official Study Guide

Exam PW0-204

CWSP®

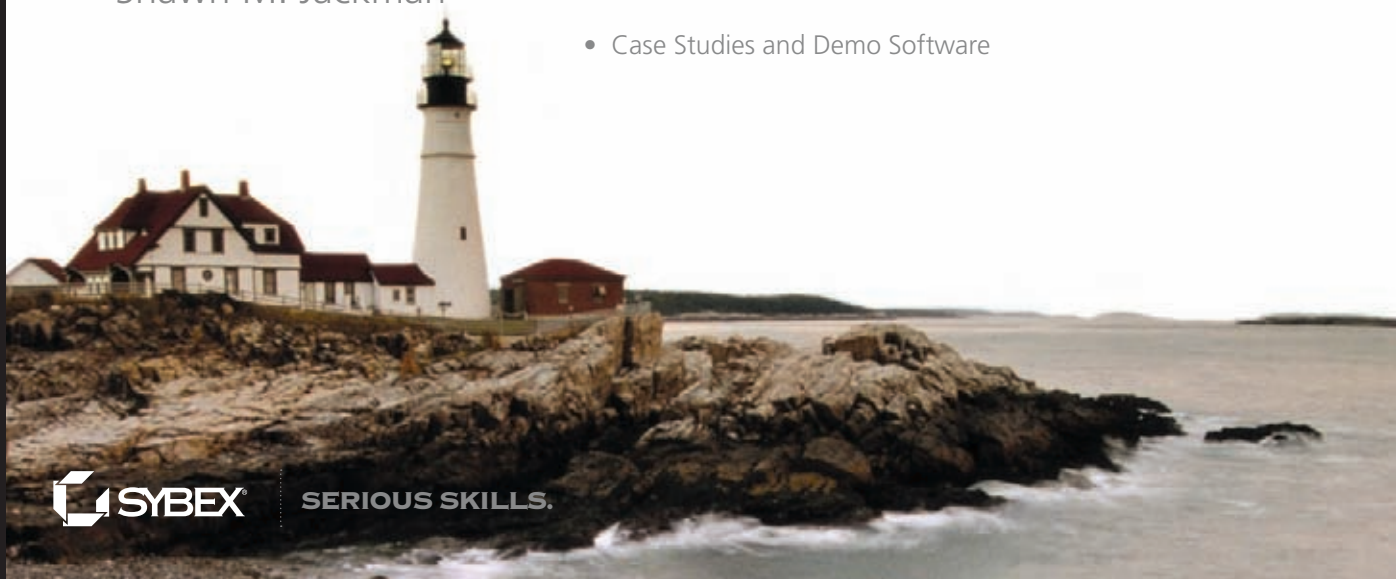
Certified Wireless Security Professional

Official Study Guide

David D. Coleman
David A. Westcott
Bryan E. Harkins
Shawn M. Jackman

Includes Real-World Scenarios, Hands-On Exercises, and Leading-Edge Exam Prep Software Featuring:

- Hundreds of Sample Questions
- Electronic Flashcards
- Case Studies and Demo Software



SYBEX SERIOUS SKILLS.

CWSP®

Certified Wireless Security Professional Official

Study Guide

CWSP®

Certified Wireless Security Professional Official

Study Guide

David Coleman, David Westcott,
Bryan Harkins, and Shawn Jackman

WILEY
Wiley Publishing, Inc.

Acquisitions Editor: Jeff Kellum
Development Editor: Gary Schwartz
Technical Editors: Sam Coyl and Marcus Burton
Production Editor: Rachel McConlogue
Copy Editor: Liz Welch
Editorial Manager: Pete Gaughan
Production Manager: Tim Tate
Vice President and Executive Group Publisher: Richard Swadley
Vice President and Publisher: Neil Edde
Media Project Manager 1: Laura Moss-Hollister
Media Associate Producer: Marilyn Hummel
Media Quality Assurance: Josh Frank
Book Designers: Judy Fung and Bill Gibson
Proofreader: Publication Services, Inc.
Indexer: Ted Laux
Project Coordinator, Cover: Lynsey Stanford
Cover Designer: Ryan Sneed

Published simultaneously in Canada

ISBN: 978-0-470-43891-6

Library of Congress Cataloging-in-Publication Data

CWSP : certified wireless security professional official study guide (exam PW0-204) / David D. Coleman . . . [et al.]. — 1st ed.

p. cm.

ISBN 978-0-470-43891-6

1. Wireless communication systems — Security measures — Examinations — Study guides.
2. Telecommunications engineers — Certification. I. Coleman, David D.

TK5103.2.C87 2010

005.8076—dc22

2009042658

10 9 8 7 6 5 4 3 2 1

Dear Reader,

Thank you for choosing *CWSP: Certified Wireless Security Professional Official Study Guide*. This book is part of a family of premium-quality Sybex books, all of which are written by outstanding authors who combine practical experience with a gift for teaching.

Sybex was founded in 1976. More than 30 years later, we're still committed to producing consistently exceptional books. With each of our titles, we're working hard to set a new standard for the industry. From the paper we print on, to the authors we work with, our goal is to bring you the best books available.

I hope you see all that reflected in these pages. I'd be very interested to hear your comments and get your feedback on how we're doing. Feel free to let me know what you think about this or any other Sybex book by sending me an email at `nedde@wiley.com`. If you think you've found a technical error in this book, please visit `http://sybex.custhelp.com`. Customer feedback is critical to our efforts at Sybex.

Best regards,

Neil Edde
Vice President and Publisher
Sybex, an Imprint of Wiley

We dedicate this book to all the men and women of the United States Armed Forces for putting their private lives aside to preserve and protect freedom. Thank you for your service and your sacrifice.

Acknowledgments

David Coleman would once again like to thank his children, Brantley and Carolina, for their patience and understanding of their father throughout the writing of yet another book. I love you kids very much. David would also like to thank his mother, Marjorie Barnes, and his stepfather, William Barnes, for many years of support and encouragement. David would also like to thank his brother, Rob Coleman, for all his help during a tough year.

David Westcott would like to thank his parents, Kathy and George, who have provided so much support and love and from whom he has learned so much. He would also like to thank Janie, Jennifer, and Samantha for their patience and understanding of life on the road and for their support throughout the writing of this book.

Bryan Harkins would like to thank his wife, Ronda, and his two daughters, Chrystan and Catelynn, for enduring the constant travel and time away from them it has taken to create this book. I love the three of you very much. I would also like to thank my parents for always being there and my brother Chris for getting me into IT in the first place. Additionally, I would like to thank David Thomas and Ralf Deltrap of Motorola AirDefense Solutions for making me part of the AirDefense team years ago.

Shawn Jackman would like to thank his parents, Alice and Steve, for the many years of encouragement and unquestioning support, but most of all for leading by example as a parent, provider, and character example. Shawn would also like to thank his wife, Joy, the world's most supportive and wonderful woman a Wi-Fi geek could ever ask for. And, of course, to his children, Summer, Pierce, and Julia, who are loved by their daddy more than they will ever know.

Writing *CWSP: Certified Wireless Security Professional Official Study Guide* has been an adventure from the start. We would like to thank the following individuals for their support and contributions during the entire process.

We must first thank Sybex acquisitions editor Jeff Kellum for initially finding us and bringing us on to this project. Jeff is an extremely patient and understanding editor who occasionally sends a nasty email message. We would also like to thank our development editor, Gary Schwartz. We also need to send special thanks to our editorial manager, Pete Gaughan; our production editor, Rachel McConlogue; and Liz Welch, our copyeditor.

We also need to give a big shout-out to our technical editor, Sam Coyl. Sam is a member of the IEEE with many years of practical experience in wireless communications. His contributions to the book were nothing short of invaluable. When Sam is not providing awesome technical editing, he is vice president of business development for Netrepid (`www.netrepid.com`), a wireless solutions provider.

We would also like to thank Marcus Burton, Cary Chandler, Abbey Cole, and Kevin Sandlin of the CWNP program (`www.cwnp.com`). All CWNP employees, past and present, should be proud of the internationally renowned wireless certification program that sets the education standard within the enterprise Wi-Fi industry. It has been a pleasure working with all of you the past 10 years. Special thanks go to Marcus Burton for his feedback and content review.

Thanks goes to the students who attended an October 2009 CWSP evaluation class held in Atlanta. Those students include Ray Baum and Max Lopez from the University of Colorado, Joe Altmann from Polycom, and Randall Bobula from the CME Group. Also contributing that week was our favorite Meruvian, Diana Cortes from the University of Miami.

We would also like to thank Devin Akin, Chief Architect of Aerohive Networks. Devin has been a Wi-Fi guru for all four authors for many years.

Shawn would also like to thank the following co-workers and professional colleagues: Nico Arcino, Ken Fisch, Tom Head, Jon Krabbenschmidt, and George Stefanick.

We would also like to thank the following individuals and companies for their support and contributions to the book:

Aerohive Networks (`www.aerohive.com`) — Devin Akin, Adam Conway, and Paul Levasseur

AeroScout (`www.aeroscout.com`) — Steffan Haithcox and Scott Phillips.

AirDefense (`www.airdefense.net`) — Ralf Deltrap and David Thomas

AirMagnet (`www.airmagnet.com`) — Dilip Advani

AirWave (`www.airwave.com`) — Patrick Smith

Aruba Networks (`www.arubanetworks.com`) — Carolyn Cutler, Chris Leach, Andy Logan, Susan Wells, and Micah Wilson

By-Light (`www.by-light.com`) — Steve Hurdle

CACE Technologies (`www.cacetech.com`) — Janice Spampinato

Cisco Systems (`www.cisco.com`) — Chris Allen, John Helm, Matt Swartz, and Hao Zhao

Fluke Networks (`www.flukenetworks.com`) — Carolyn Carter, Dan Klimke, and Lori Whitmer

Immunity (`www.immunityinc.com`) — Steven Laskowski

NetStumbler (`www.netstumbler.com`) — Marius Milner

Polycom (`www.polycom.com`) — Justin Borthwick, Geri Mitchell-Brown, and Steve Rolapp

Vocera (`www.vocera.com`) — Arun Mirchandani, Steve Newsome, and Brian Sturges

Wi-Fi Alliance (`www.wifi.org`) — Kelly Davis-Felner and Krista Ford

WildPackets (`www.wildpackets.com`) — Stephanie Temples

About the Authors

David D. Coleman is a WLAN security consultant and trainer. He teaches the CWNP classes that are recognized throughout the world as the industry standard for wireless networking certification, and he also conducts vendor-specific Wi-Fi training. He has also taught numerous "train-the-trainer" classes and "beta" classes for the CWNP program. David has instructed IT professionals from around the globe in wireless networking administration, wireless security, and wireless frame analysis. The company he founded, AirSpy Networks (`www.airspy.com`), specializes in corporate training and has worked in the past with Avaya, Nortel, Polycom, and Siemens. AirSpy Networks also specializes in government classes, and it has trained numerous computer security employees from various law enforcement agencies, the U.S. Marines, the U.S. Army, the U.S. Navy, the U.S. Air Force, and other federal and state government agencies. David has written many books and white papers about wireless networking, and he is considered an authority on 802.11 technology.

David is also a member of the Certified Wireless Network Expert (CWNE) Roundtable, a selected group of individuals who work with the CWNP program to provide direction for the CWNP exams and certifications. David resides in Atlanta, Georgia, where he shares a home with his two children, Carolina and Brantley. David Coleman is CWNE #4, and he can be reached via email at `david@airspy.com`.

David Westcott is an independent consultant and technical trainer with over 25 years of experience in information technology, specializing in computer networking and security. In addition to providing advice and direction to corporate clients, David has been a certified trainer for over 17 years, providing training to government agencies, corporations, and universities around the world. David was an adjunct faculty member for Boston University's Corporate Education Center for over 10 years, and he has developed courseware on wireless networking, wireless mesh networking, wired networking, and security for Boston University and many other clients.

Since installing his first wireless network in 1999, David has become a Certified Wireless Network Trainer, Administrator, Security Professional, and Analysis Professional. David is also a member of the CWNE Roundtable. David has earned certifications from Cisco, Aruba, Microsoft, EC-Council, CompTIA, and Novell. David lives in Concord, Massachusetts with his wife Janie and his stepdaughters, Jennifer and Samantha. A licensed pilot, he enjoys flying his Piper Cherokee 180 around New England when he is not flying around the world commercially. David is CWNE #7, and he can be reached via email at `david@westcott-consulting.com`.

Shawn Jackman currently oversees wireless enterprise engineering for a large healthcare provider and adopter of 802.11 technology. Prior to that, Shawn has been on both sides of the table, working for a WLAN manufacturer and with wireless integrators. Shawn has been intensely focused on large-scale VoWiFi, QoS, and RTLS applications for over three years, and he spends a considerable amount of his time doing end-user design, deployment, and troubleshooting for various vendors' equipment. Shawn has traveled the United States and internationally designing wired and wireless networks, from concept to completion, for healthcare, warehouse, hospitality, education, metro/municipal, government, franchise, and retail environments. He has served as an on-air technical personality for a weekly syndicated call-in talk radio show with over 5 million listeners worldwide and is considered an authority on Wi-Fi technology.

Shawn is a member of the CWNE Roundtable. He lives in the San Francisco Bay area with his wife Joy and their three children, Summer, Pierce, and Julia. Shawn is CWNE #54, and he can be reached via email at `shawn.jackman@cwne.com`.

Bryan Harkins is currently the training and development manager for Motorola AirDefense Solutions and has over 20 years experience in the IT field. He has been involved in areas ranging from customer support and sales to network security and design. He has developed custom curriculum for government agencies and Fortune 500 companies alike. Over the years, he has helped numerous students reach their certification and knowledge goals through his exceptional skills as an instructor. He delivers both public and private wireless security classes around the world and holds several prestigious industry certifications, including MCSE, CWNE, and CWNT.

Bryan has spoken during Secure World Expo, Armed Forces Communications and Electronics Association (AFCEA) events, and Microsoft Broad Reach as well as many other industry events. He holds a degree in aviation from Georgia State University. Bryan is a native of Atlanta, Georgia, and still lives in the area with his wife Ronda and two daughters, Chrystan and Catelynn. Bryan is also a member of the CWNE Roundtable. Bryan is CWNE #44, and he can be reached via email at `bryan.harkins@motorola.com`.

Contents at a Glance

Contents

Table of Exercises

Foreword

Wi-Fi is nearly ubiquitous. The term *Wi-Fi* is certainly well known and well understood. With such widespread acceptance comes widespread usage, requiring robust security. The IEEE has, as of this writing, succeeded in ratifying two major amendments to the 802.11 standard: 802.11i and 802.11n. Both require major adjustments to any enterprise's WLAN security strategy.

The ratification of the 802.11n amendment will likely have an even greater effect on Wi-Fi security than did the 802.11i amendment for one simple reason: 802.11n has caused many more enterprises to adopt Wi-Fi for regular, daily, and mission-critical networking applications because they now believe that wireless is about as close to wired as it can get. In other words, most people think 802.11n makes wireless fast enough to use in the enterprise.

That's a great step. It means that there will be even more WLAN installations in every industry—which means more people will need to know how to install, manage, and troubleshoot these boundary-less networks. More importantly, *you* will have to know how to secure these networks!

With your acquisition of *CWSP: Certified Wireless Security Professional Official Study Guide,* you have taken a huge step toward making yourself indispensible to your organization's wireless team. Well done! Now you can start preparing to prove your knowledge of enterprise Wi-Fi security. You can learn how hackers are trying to attack your wireless LAN, how to prevent them from doing so, and how to guide your organization's policy toward large-scale deployment of enterprise Wi-Fi infrastructure and applications.

The CWSP certification is now the third step in the CWNP line of certifications and remains focused on securing an enterprise 802.11 WLAN. CWSP includes topics such as 802.1X/EAP types, fast secure roaming, robust security networks, Layer 2 and 3 VPNs, wireless intrusion prevention system (WIPS) implementation, intrusion and attack techniques, and much more. Additional CWNP certifications focus more intensely on protocol analysis, quality of service, design, advanced surveying, VoWiFi, location tracking, and RF spectrum management.

David Coleman (CWNE #4) and David Westcott (CWNE #4) have worked as Certified Wireless Network Trainers (CWNTs) for as long as the CWNT certification has been available, and each was quick to pursue all CWNP certifications as they were released. Each has years of experience with a breadth of WLAN technologies and leading-edge products, which is obvious to their students and anyone working alongside them in the field. Having worked with each of these gentlemen for years, I can confidently say there could be no finer pair of seasoned trainers collaborating on a CWSP book.

The addition of Shawn Jackman (CWNE #54) and Bryan Harkins (CWNE #44) brings to the book a wealth of field experience from the WLAN security and healthcare markets. Jackman leads the WLAN team at a major healthcare organization and Harkins is the lead

technical instructor for Motorola's AirDefense unit. These WLAN veterans have devoted hundreds of hours to pouring their experience into this book, and the reader is certain to acquire a plethora of 802.11 knowledge. Coleman, Harkins, Jackman, and Westcott have played a big role in the shaping of CWNP and have each added tremendous value to the CWNA and CWSP certifications specifically.

We thank each of these fine authors for their constant support of CWNP, and congratulate them on the completion of their second Study Guide.

Kevin Sandlin
Co-founder and CEO
CWNP Inc.

Introduction

If you have purchased this book or if you are even thinking about purchasing this book, you probably have some interest in taking the CWSP® (Certified Wireless Security Professional) certification exam or in learning what the CWSP certification exam is about. The authors would like to congratulate you on this first step, and we hope that our book can help you on your journey. Wireless local area networking (WLAN) is currently one of the hottest technologies on the market. Security is an important and mandatory aspect of 802.11 wireless technology. As with many fast-growing technologies, the demand for knowledgeable people is often greater than the supply. The CWSP certification is one way to prove that you have the knowledge and skills to secure 802.11 wireless networks successfully. This study guide is written with that goal in mind.

This book is designed to teach you about WLAN security so that you have the knowledge needed not only to pass the CWSP certification test, but also to be able to design, install, and support wireless networks. We have included review questions at the end of each chapter to help you test your knowledge and prepare for the exam. We have also included labs, white papers, and presentations on the CD to facilitate your learning further.

Before we tell you about the certification process and its requirements, we must mention that this information may have changed by the time you are taking your test. We recommend that you visit `www.cwnp.com` as you prepare to study for your test to check out the current objectives and requirements.

Do not just study the questions and answers! The practice questions in this book are designed to test your knowledge of a concept or objective that is likely to be on the CWSP exam. The practice questions will be different from the actual exam questions. If you learn and understand the topics and objectives in this book, you will be better prepared for the test.

About CWSP® and CWNP®

If you have ever prepared to take a certification test for a technology with which you are unfamiliar, you know that you are not only studying to learn a different technology, but you are also probably learning about an industry with which you are unfamiliar. Read on and we will tell you about the CWNP Program. *CWNP* is an abbreviation for *Certified Wireless Network Professional*. There is no CWNP test. The CWNP Program develops courseware and certification exams for wireless LAN technologies in the computer networking industry. The CWNP certification program is a vendor-neutral program.

The objective of the CWNP Program is to certify people on wireless networking, not on a specific vendor's product. Yes, at times the authors of this book and the creators of the certification will talk about, or even demonstrate how to use a specific product; however,

the goal is the overall understanding of wireless technology, not the product itself. If you learned to drive a car, you physically had to sit and practice in one. When you think back and reminisce, you probably do not tell anyone that you learned to drive a Ford; you probably say you learned to drive using a Ford.

There are five wireless certifications offered by the CWNP Program:

CWTS™: Certified Wireless Technology Specialist The CWTS certification is the latest certification from the CWNP Program. CWTS is an entry-level enterprise WLAN certification, and it is a recommended prerequisite for the CWNA certification. This certification is geared specifically toward both WLAN sales and support staff for the enterprise WLAN industry. The CWTS certification exam (PW0-070) verifies that sales and support staffs are specialists in WLAN technology and have all the fundamental knowledge, tools, and terminology to sell and support WLAN technologies more effectively.

CWNA®: Certified Wireless Network Administrator The CWNA certification is a foundation-level Wi-Fi certification; however, it is not considered an "entry-level" technology certification. Individuals taking the CWNA exam (PW0-104) typically have a solid grasp of network basics such as the OSI model, IP addressing, PC hardware, and network operating systems. Many candidates already hold other industry-recognized certifications, such as CompTIA Network+ or Cisco CCNA, and are looking to the CWNA certification to enhance or complement existing skills.

CWSP®: Certified Wireless Security Professional The CWSP certification exam (PW0-204) is focused on standards-based wireless security protocols, security policy, and secure wireless network design. This certification introduces candidates to many of the technologies and techniques that intruders use to compromise wireless networks and administrators use to protect wireless networks. With recent advances in wireless security, WLANs can be secured beyond their wired counterparts.

CWNE®: Certified Wireless Network Expert The CWNE certification (PW0-300) is the highest-level certification in the CWNP Program. By successfully completing the CWNE requirements, you will have demonstrated that you have the most advanced skills available in today's wireless LAN market. The CWNE exam (PW0-300) focuses on advanced WLAN analysis, design, troubleshooting, quality of service (QoS) mechanisms, spectrum management, and extensive knowledge of the IEEE 802.11 standard as amended.

CWNT®: Certified Wireless Network Trainer Certified Wireless Network Trainers are qualified instructors certified by the CWNP Program to deliver CWNP training courses to IT professionals. CWNTs are technical and instructional experts in wireless technologies, products, and solutions. To ensure a superior learning experience for our customers, CWNP Education Partners are required to use CWNTs when delivering training using Official CWNP Courseware.

How to Become a CWSP

To become a CWSP, you must do the following three things:

- Agree that you have read and will abide by the terms and conditions of the CWNP Confidentiality Agreement.
- Pass the CWNA certification exam.
- Pass the CWSP certification exam.

The CWNA certification is a prerequisite for the CWSP certification. If you have purchased this book, there is a good chance that you have already passed the CWNA exam and are now ready to move to the next level of certification and plan to study and pass the CWSP exam. That is the usual recommended path to achieving CWSP certification; however, there is no requirement to take the exams in order. You can take the CWSP exam prior to passing the CWNA exam, but you will not become a certified CWSP until you have passed both exams.

A copy of the CWNP Confidentiality Agreement can be found online at the CWNP website.

When you sit to take any CWNP exam, you will be required to accept this confidentiality agreement before you can continue with the exam. Once you have agreed, you will be able to continue.

The information for the CWNA exam is as follows:

- Exam Name: Wireless LAN Administrator
- Exam Number: PW0-104
- Cost: $175.00 (in US dollars)
- Duration: 90 minutes
- Questions: 60
- Question Types: Multiple choice/multiple answer
- Passing Score: 70% (80% for instructors)
- Available Languages: English
- Availability: Register at Pearson VUE (`www.vue.com/cwnp`)

The information for the CWSP exam is as follows:

- Exam Name: Wireless Security Professional
- Exam Number: PW0-204
- Cost: $225.00 (in US dollars)
- Duration: 90 minutes
- Questions: 60

- Question Types: Multiple choice/multiple answer
- Passing Score: 70% (80% for instructors)
- Available Languages: English
- Availability: Register at Pearson VUE (`www.vue.com/cwnp`)

When you schedule the exam, you will receive instructions regarding appointment and cancellation procedures, ID requirements, and information about the testing center location. In addition, you will receive a registration and payment confirmation letter. Exams can be scheduled weeks in advance or, in some cases, even as late as the same day.

After you have successfully completed the CWSP certification requirements, the CWNP Program will award you the CWSP certification that is good for three years. To recertify, you will need to pass the current PW0-204 exam, or earn the CWNE certification. If the information you provided the testing center is correct, you will receive an e-mail from CWNP recognizing your accomplishment and providing you with a CWNP certification number. After you earn any CWNP certification, you can request a certification kit. The kit includes a congratulatory letter, a certificate, and a wallet-sized personalized ID card. You will need to log in to the CWNP tracking system, verify your contact information, and request your certification kit.

Who Should Buy this Book?

If you want to acquire a solid foundation in WLAN security and your goal is to prepare for the exam, this book is for you. You will find clear explanations of the concepts you need to grasp and plenty of help to achieve the high level of professional competency you need in order to succeed.

If you want to become certified as a CWSP, this book is definitely what you need. However, if you just want to attempt to pass the exam without really understanding WLAN security, this study guide is not for you. It is written for people who want to acquire hands-on skills and in-depth knowledge of wireless networking security.

How to Use this Book and the CD

We have included several testing features in the book and on the CD-ROM. These tools will help you retain vital exam content as well as prepare you to sit for the actual exam:

Before You Begin At the beginning of the book (right after this introduction) is an assessment test you can use to check your readiness for the exam. Take this test before you start reading the book; it will help you determine the areas in which you may need to brush up. The answers to the assessment test appear on a separate page after the last question of the test. Each answer includes an explanation and a note telling you the chapter in which the material appears.

Chapter Review Questions To test your knowledge as you progress through the book, there are review questions at the end of each chapter. As you finish each chapter, answer the review questions and then check your answers; the correct answers appear on the page following the last review question. You can go back and reread the section that deals with each question you answered wrong to ensure that you answer correctly the next time you are tested on the material.

Electronic Flashcards You will find flashcard questions on the CD for on-the-go review. These are short questions and answers, just like the flashcards you probably used in school. You can answer them on your PC or download them onto a handheld device for quick and convenient reviewing.

Test Engine The CD also contains the Sybex Test Engine. With this custom test engine, you can identify weak areas up front and then develop a solid studying strategy that includes each of the robust testing features described previously. Our thorough readme file will walk you through the quick, easy installation process.

In addition to the assessment test and the chapter review questions, you will find two bonus exams. Use the test engine (without any reference material) to take these practice exams just as if you were taking the actual exam. When you have finished the first exam, move on to the next one to solidify your test-taking skills. If you get more than 95 percent of the answers correct, you are ready to take the certification exam.

Hands-on Exercises Several chapters in this book have exercises that use software and videos that are also provided on the CD-ROM that is included with this book. These hands-on exercises will provide you with a broader learning experience by providing hands-on experience and step-by-step problem solving.

White Papers Several chapters in this book will reference WLAN security white papers that are also provided on the CD-ROM that is included with this book. These white papers serve as additional reference material for preparing for the CWSP exam.

Exam Objectives

The CWSP exam measures your understanding of the fundamentals of WLAN security as well as 802.11 and 802.1X/EAP security protocols. The CWSP exam also tests your knowledge of the skills needed to install, configure, and troubleshoot WLAN security architecture.

The skills and knowledge measured by this examination were derived from a survey of wireless networking experts and professionals. The results of this survey were used in weighing the subject areas and ensuring that the weighting is representative of the relative importance of the content.

The following chart provides the breakdown of the exam, showing you the weight of each section:

Wireless LAN Security Subject Area	% of Exam
Wireless Network Attacks and Threat Assessment	10%
Monitoring and Management	25%
Security Design and Architecture	50%
Security Policy	5%
Fast Secure Roaming	10%
Total	**100%**

Wireless Network Attacks and Threat Assessment — 10%

1.1 Demonstrate How to Recognize, Perform, and Prevent the Following Types of Attacks, and Discuss Their Impact on the Organization

- Information theft and placement
- Physical device damage or theft
- PHY and MAC denial of service (DoS)
- Client hijacking, phishing, and other peer-to-peer attacks
- Protocol analysis (eavesdropping)
- MAC layer protocol attacks
- Social engineering
- Man-in-the-middle
- Authentication and encryption cracking
- Infrastructure hardware theft
- Management interface exploits
- Rogue infrastructure hardware placement

1.2 Understand the Probability of, Demonstrate the Methodology of, and Execute the Preventative Measures Against the Following Attacks on Wireless Infrastructure Devices

- Weak/default passwords on wireless infrastructure equipment
- Misconfiguration of wireless infrastructure devices by administrative staff

1.3 Explain and Demonstrate the Use of Protocol Analyzers to Capture the Following Sensitive Information

- Usernames/Passwords/SNMP Community Strings/X.509 certificates
- Encryption keys/Passphrases
- MAC addresses/IP addresses
- Unencrypted data

1.4 Explain and/or Demonstrate Security Protocol Circumvention Against the Following Types of Authentication and/or Encryption

- WEP (Any key length)
- Shared Key Authentication
- WPA-Personal/WPA2-Personal
- LEAP
- PPTP

1.5 Explain a Risk Assessment for a WLAN

- Asset risk
- Legal implications
- Regulatory compliance

1.6 Explain and Demonstrate the Following Security Vulnerabilities Associated with Public Access or Other Unsecured Wireless Networks

- Spamming through the WLAN
- Malware (viruses/spyware/adware/remote control)
- Direct Internet attacks through the WLAN
- Placement of illegal content
- Information theft
- Peer-to-peer attack

Monitoring, Management, and Tracking — 20%

2.1 Understand How to Use Laptop-Based Protocol and Spectrum Analyzers to Effectively Troubleshoot and Secure Wireless Networks

2.2 Describe the Use, Configuration, and Components of an 802.11 Wireless Intrusion Prevention Systems (WIPS)

- WIPS server software or appliance
- Dedicated sensor hardware/software

- Access points as part-time sensors
- Access points with dedicated sensor radios
- Integration between WLAN controller and WIPS server
- Deployment strategies: overlay and integrated
- Performance and security analysis
- Protocol and spectrum analysis

2.3 Explain 802.11 WIPS Baselining and Demonstrate the Following Tasks

- Measuring performance parameters under normal network conditions
- Understanding common reasons for false positives and false negatives
- Configuring the WIPS to recognize all APs and client stations in the area as authorized, external, or rogue

2.4 Describe and Understand Common Security Features of 802.11 WIPS

- Device detection, classification, and behavior analysis
- Rogue Triangulation, RF Fingerprinting, and Time Difference of Arrival (TDoA) techniques for real-time device and interference tracking
- Event alerting, notification, and categorization
- Policy enforcement and violation reporting
- Wired/Wireless intrusion mitigation
- Protocol analysis with filtering
- Rogue containment and remediation
- Data forensics

2.5 Describe and Demonstrate the Different Types of WLAN Management Systems and Their Features

- Network discovery
- Configuration and firmware management
- Audit management and policy enforcement
- Network and user monitoring
- Rogue detection
- Event alarms and notification

2.6 Describe and Implement Compliance Monitoring, Enforcement, and Reporting

- Industry requirements (PCI)
- Government regulations

Security Design and Architecture — 50%

3.1 Describe Wireless Network Security Models

- Hotspot/Public Access/Guest Access
- Small Office/Home Office
- Small and Medium Enterprise
- Large Enterprise
- Remote Access: Mobile User and Branch Office

3.2 Recognize and Understand the Following Security Concepts:

- 802.11 Authentication and Key Management (AKM) components and processes
- Robust Security Networks (RSN) and RSN Associations (RSNA)
- Pre-RSNA Security
- Transition Security Networks (TSN)
- RSN Information Elements
- How WPA and WPA2 certifications relate to 802.11 standard terminology and technology
- Functional parts of TKIP and its differences from WEP
- The role of TKIP/RC4 in WPA implementations
- The role of CCMP/AES in WPA2 implementations
- TKIP compatibility between WPA and WPA2 implementations
- Appropriate use and configuration of WPA-Personal and WPA-Enterprise
- Appropriate use and configuration of WPA2-Personal and WPA2-Enterprise
- Appropriate use and configuration of Per-user Pre-shared Key (PPSK)
- Feasibility of WPA-Personal and WPA2-Personal exploitation

3.3 Identify the Purpose and Characteristics of 802.1X and EAP

- Supplicant, authenticator, and authentication server roles
- Functions of the authentication framework and controlled/uncontrolled ports

- How EAP is used with 802.1X port-based access control for authentication
- Strong EAP types used with 802.11 WLANs:
  - PEAPv0/EAP-TLS
  - PEAPv0/EAP-MSCHAPv2
  - PEAPv1/EAP-GTC
  - EAP-TLS
  - EAP-TTLS/MS-CHAPv2
  - EAP-FAST

3.4 Recognize and Understand the Common Uses of VPNs in Wireless Networks

- Remote AP
- VPN client software
- WLAN Controllers

3.5 Describe, Demonstrate, and Configure Centrally Managed Client-Side Security Applications

- VPN policies
- Personal firewall software
- Wireless client utility software

3.6 Describe and Demonstrate the Use of Secure Infrastructure Management Protocols

- HTTPS
- SNMPv3
- SFTP (FTP/SSL or FTP/SSH)
- SCP
- SSH2

3.7 Explain the Role, Importance, and Limiting Factors of VLANs and Network Segmentation in an 802.11 WLAN Infrastructure

3.8 Describe, Configure, and Deploy an AAA Server and Explain the Following Concepts Related to AAA Servers

- RADIUS server
- Integrated RADIUS services within WLAN infrastructure devices
- RADIUS deployment strategies

- RADIUS proxy services
- LDAP Directory Services integration deployment strategies
- EAP support for 802.11 networks
- Applying user and AAA server credential types (Username/Password, Certificate, Protected Access Credentials [PACs] & Biometrics)
- The role of AAA services in wireless client VLAN assignments
- Benefits of mutual authentication between supplicant and authentication server

3.9 Explain Frame Exchange Processes and the Purpose of Each Encryption Key within 802.11 Authentication and Key Management

- Master Session Key (MSK) generation
- PMK generation and distribution
- GMK generation
- PTK/GTK generation & distribution
- 4-Way Handshake
- Group Handshake
- Passphrase-to-PSK mapping

3.10 Describe and Configure Major Security Features in WLAN Infrastructure Devices

- Role-Based Access Control (RBAC) (per-user or per-group)
- Location Based Access Control (LBAC)
- Fast BSS transition in an RSN
- 802.1Q VLANs and trunking on Ethernet switches and WLAN infrastructure devices
- Hot standby/failover and clustering support
- WPA/WPA2 Personal and Enterprise
- Secure management interfaces (HTTPS, SNMPv3, SSH2)
- Intrusion detection and prevention
- Remote access (branch office and mobile users)

3.11 Explain the Benefits of and Configure Management Frame Protection (802.11w) in Access Points and WLAN Controllers

3.12 Explain the Purpose, Methodology, Features, and Configuration of Guest Access Networks

- Segmentation
- Captive Portal (Web) Authentication
- User-based authentication methods

Security Policy — 5%

4.1 Explain the Purpose and Goals of the Following WLAN Security Policies

- Password policy
- End-user and administrator training on security solution use and social engineering mitigation
- Internal marketing campaigns to heighten security awareness
- Periodic network security audits
- Acceptable network use & abuse policy
- Use of Role-Based Access Control (RBAC) and traffic filtering
- Obtaining the latest security feature sets through firmware and software upgrades
- Consistent implementation procedure
- Centralized implementation and management guidelines and procedures
- Inclusion in asset and change management programs

4.2 Describe Appropriate Installation Locations for and Remote Connectivity to WLAN Devices in Order to Avoid Physical Theft, Tampering, and Data Theft

- Physical security implications of infrastructure device placement
- Secure remote connections to WLAN infrastructure devices

4.3 Explain the Importance and Implementation of Client-Side Security Applications

- VPN client software and policies
- Personal firewall software
- 802.1X/EAP supplicant software

4.4 Explain the Importance of On-Going WLAN Monitoring and Documentation

- Explain the necessary hardware and software for on-going WLAN security monitoring
- Describe and implement WLAN security audits and compliance reports

4.5 Summarize the Security Policy Criteria Related to Wireless Public Access Network Use

- User risks related to unsecured access
- Provider liability, disclaimers, and acceptable use notifications

4.6 Explain the Importance and Implementation of a Scalable and Secure WLAN Solution that Includes the Following Security Parameters

- Intrusion detection and prevention
- Role-Based Access Control (RBAC) and traffic filtering
- Strong authentication and encryption
- Fast BSS transition

Fast Secure Roaming — 10%

5.1 Describe and Implement 802.11 Authentication and Key Management (AKM)

- Preauthentication
- PMK Caching

5.2 Describe and Implement Opportunistic Key Caching (OKC) and Explain its Enhancements Beyond 802.11 AKM

5.3 Describe and Implement 802.11r Authentication and Key Management (AKM) and Compare and Contrast 802.11r Enhancements with 802.11 AKM and Opportunistic Key Caching

- Fast BSS Transition (FT) Key Architecture
- Key Nomenclature
- Initial Mobility Domain Association
- Over-the-Air Transition
- Over-the-DS Transition

5.4 Describe Applications of Fast BSS Transition

5.5 Describe and Implement Non-Traditional Roaming Mechanisms

- Single Channel Architecture (SCA) WLAN controllers with controller-based APs
- Infrastructure-controlled handoff

5.6 Describe How 802.11k Radio Resource Measurement Factors into Fast BSS Transition

- Neighbor Reports
- Contrasting SCA and MCA Architectures

5.7 Describe the Importance, Application, and Functionality of Wi-Fi Voice-Personal Product Certification

CWSP Exam Terminology

The CWNP program uses very specific terminology when phrasing the questions on any of the CWNP exams. The terminology used most often mirrors the same language that is used in the IEEE 802.11-2007 standard. While technically correct, the terminology used in the exam questions often is not the same as the marketing terminology that is used by the Wi-Fi Alliance. The most current IEEE version of the 802.11 standard is the IEEE 802.11-2007 document, which includes all the amendments that have been ratified prior to the document's publication. Standards bodies like the IEEE often create several amendments to a standard before "rolling up" the ratified amendments (finalized or approved versions) into a new standard.

For example, you might already be familiar with the term *802.11g*, which is a ratified amendment that has now been integrated into the IEEE 802.11-2007 standard. The technology that was originally defined by the 802.11g amendment is called Extended Rate Physical (ERP). Although the name 802.11g effectively remains the more commonly used marketing terminology, any exam questions will use the technical term ERP instead of 802.11g.

To prepare properly for the CWSP exam, any test candidate should become 100 percent familiar with the terminology used by the CWNP program. This book will define and cover all terminology; however, the CWNP program maintains an updated current list of exam terms that can be downloaded from the following URL: `www.cwnp.com/exams/exam_terms.html`.

Tips for Taking the CWSP Exam

Here are some general tips for taking your exam successfully:

- Bring two forms of ID with you. One must be a photo ID, such as a driver's license. The other can be a major credit card or a passport. Both forms must include a signature.
- Arrive early at the exam center so you can relax and review your study materials, particularly tables and lists of exam-related information.
- Read the questions carefully. Do not be tempted to jump to an early conclusion. Make sure you know exactly what the question is asking.

- Many of the questions will be real-world scenarios. Scenario questions usually take longer to read and often have many distracters. There may be several correct answers to the scenario questions; however, you will be asked to choose the correct answer that best fits the presented scenario.
- There will be questions with multiple correct responses. When there is more than one correct answer, a message at the bottom of the screen will prompt you either to "choose two" or "choose all that apply." Be sure to read the messages displayed to know how many correct answers you must choose.
- When answering multiple-choice questions about which you are unsure, use a process of elimination to get rid of the obviously incorrect answers first. Doing so will improve your odds if you need to make an educated guess.
- Do not spend too much time on one question. This is a form-based test; however, you cannot move backward through the exam. You must answer the current question before you can move to the next question, and once you have moved to the next question, you cannot go back and change your answer to a previous question.
- Keep track of your time. Since this is a 90-minute test consisting of 60 questions, you have an average of 90 seconds to answer each question. You can spend as much or as little time on any one question, but when the 90 minutes is up, the test is over. Check your progress. After 45 minutes, you should have answered at least 30 questions. If you have not, do not panic. You will simply need to answer the remaining questions at a faster pace. If on average you can answer each of the remaining 30 questions 4 seconds quicker, you will recover 2 minutes. Again, do not panic; just pace yourself.
- For the latest pricing on the exams and updates to the registration procedures, visit CWNP's website at `www.cwnp.com`.

Assessment Test

1. At which layers of the OSI model does 802.11 technology operate? (Choose all that apply.)
   - **A.** Data-Link
   - **B.** Network
   - **C.** Physical
   - **D.** Presentation
   - **E.** Transport

2. PSK authentication is mandatory in which of the following? (Choose all that apply.)
   - **A.** WPA-Personal
   - **B.** WPA Enterprise
   - **C.** WPA-2 SOHO
   - **D.** WPA-2 Enterprise
   - **E.** WPA2-Personal

3. 802.11 pre-RSNA security defines which wireless security solution?
   - **A.** Dynamic WEP
   - **B.** 802.1X/EAP
   - **C.** 128-bit static WEP
   - **D.** Temporal Key Integrity Protocol
   - **E.** CCMP/AES

4. Which of these legacy security solutions provides Layer 3 data privacy?
   - **A.** Open System
   - **B.** IPsec VPN
   - **C.** PPTP VPN
   - **D.** Static WEP with IPsec VPN

5. What type of encryption is shown is this graphic?

A. TKIP/RC4

B. WEP

C. CCMP/AES

D. MPPE

E. Proprietary

6. Which of the following encryption methods use asymmetric communications?

A. WEP

B. TKIP

C. Public-key cryptography

D. CCMP

7. For an 802.1X/EAP solution to work properly with a WLAN, which two components must both support the same type of encryption? (Choose two.)

A. Supplicant

B. Authorizer

C. Authenticator

D. Authentication server

8. Which of these types of EAP do not use tunneled authentication? (Choose all that apply.)

A. EAP-LEAP

B. EAP-PEAPv0 (EAP-MSCHAPv2)

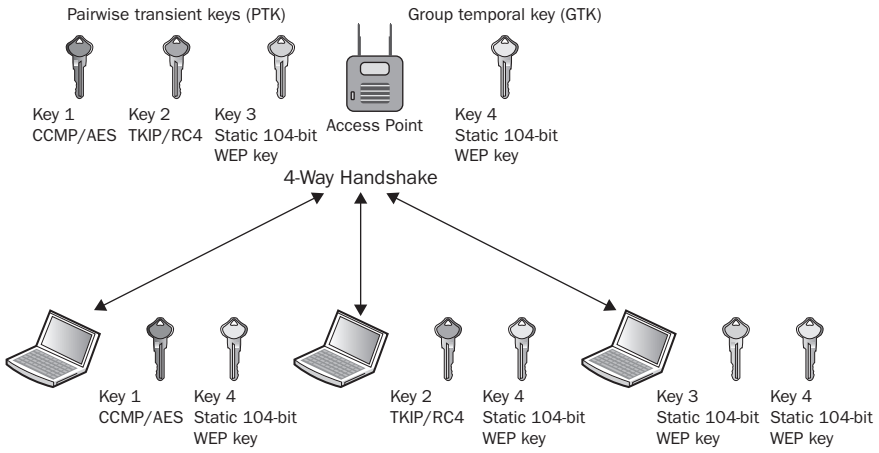
C. EAP-PEAPv1 (EAP-GTC)

D. EAP-FAST

E. EAP-TLS (normal mode)

F. EAP-MD5

9. What type of WLAN security is depicted by this graphic?



A. RSN

B. TSN

C. VPN

D. WPS

E. WMM

10. The 802.11-2007 standard defines authentication and key management (AKM) services. Which of these keys are part of the key hierarchy defined by AKM? (Choose all that apply.)

A. MSK

B. GTK

C. PMK

D. ACK

E. ATK

11. Which of these Wi-Fi Alliance security certifications are intended for use only in a home office environment? (Choose all that apply.)

A. WPA-Personal

B. WPA-Enterprise

C. WPA2-Personal

D. WPA2-Enterprise

E. WPS

12. Which of these fast secure roaming (FSR) methods requires an authenticator and supplicant to establish an entire 802.1X/EAP exchange prior to the creation of dynamic encryption keys when a supplicant is roaming?

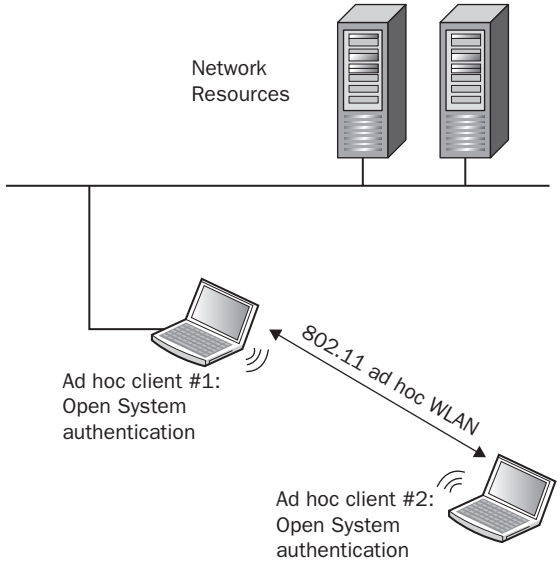
A. PMK caching

B. Opportunistic key caching

C. Fast BSS transition

D. Preauthentication

13. What is the main WLAN security risk shown in the graphic below?



A. The ad hoc clients are not using encryption.

B. The ad hoc clients are using weak authentication.

C. The ad hoc clients are not communicating through an access point.

D. The ad hoc client #1 Ethernet card is connected to an 802.3 wired network.

14. Which components of 802.11 medium contention can be compromised by a DoS attack? (Choose all that apply.)

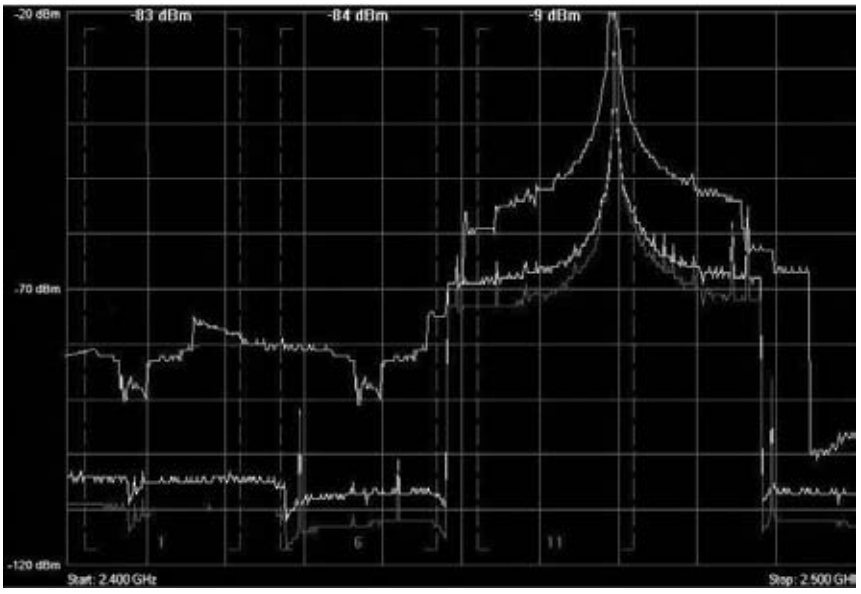
A. Physical carrier sense

B. Interframe spacing

C. Virtual carrier sense

D. Random backoff timer

15. After viewing this graphic, determine which type of WLAN attack tool could be used to create this Layer 1 denial of service to the WLAN.



A. All-band hopping jammer

B. Wide-band jammer

C. Narrow-band jammer

D. Queensland software utility

E. Packet generator

16. Bill is designing a WLAN that will use an integrated WIPS with dedicated full-time sensors. The WLAN predictive modeling software solution that Bill is using has recommended a ratio of one dedicated sensor for every six access points. Bill needs to make sure that the entire building can be monitored at all times, and he is also concerned about the accuracy of location tracking of rogue devices. What considerations should Bill give to sensor placement in order to properly meet his objectives? (Choose all that apply.)

A. Installing the sensors in a straight line

B. Installing the sensors in a staggered arrangement

C. Installing sensors around the building perimeter

D. Increasing the transmit power

E. Installing more sensors

17. Which of these WIDS/WIPS software modules allows an organization to monitor WLAN statistics on hidden nodes, excessive Layer 2 retransmissions, excessive wired to wireless traffic, and excessive client roaming? (Choose all that apply.)

A. Spectrum analysis

B. Protocol analysis

C. Forensic analysis

D. Signature analysis

E. Performance analysis

18. Kate has deployed a remote AP at her house. She wants to use the remote AP to send data back the corporate WLAN controller securely using the remote AP VPN capabilities. She also wants to access a local gateway to the Internet through the remote AP. How can Kate configure the remote AP to meet her needs? (Choose all that apply.)

A. Tunnel mode using the corporate SSID

B. Tunnel mode using the corporate SSID and a guest SSID

C. Bridge mode using the corporate SSID

D. Bridge mode using the corporate SSID and a guest SSID

E. Split-tunnel mode using the corporate SSID

F. Split-tunnel mode using the corporate SSID and a guest SSID

19. Identify the protocols that are normally used to manage WLAN infrastructure devices securely. (Choose all that apply.)

A. HTTPS

B. Telnet

C. SSH2

D. TLS

E. IPsec

F. CCMP/AES

20. What type of WLAN security policy defines WLAN security auditing requirements and policy violation report procedures?

A. Functional policy

B. General policy

C. Protocol policy

D. Performance policy

Answers to Assessment Test

1. A, C. The IEEE 802.11-2007 standard only defines communication mechanisms at the Physical layer and MAC sublayer of the Data-Link layer of the OSI model. For more information, see Chapter 1.

2. A, E. The security used in SOHO environments is preshared key (PSK) authentication. The Wi-Fi Alliance WPA-Personal and WPA2-Personal certifications both use the PSK authentication method; however, WPA-Personal specifies TKIP-RC4 encryption and WPA2-Personal specifies AES-CCMP. WLAN vendors have many names for PSK authentication, including WPA/WPA2-Passphrase, WPA/WPA2-PSK, and WPA/WPA2-Preshared Key. For more information, see Chapter 1.

3. C. The original 802.11 standard ratified in 1997 defined the use of a 64-bit or 128-bit static encryption solution called Wired Equivalent Privacy (WEP). WEP is considered pre-RSNA security. Dynamic WEP was never defined under any wireless security standard. The use of 802.1X/EAP, TKIP/RC4, and CCMP/AES are all defined under the current 802.11-2007 standard for robust network security (RSN). For more information, see Chapter 2.

4. D. IPsec and PPTP are considered Layer 3 VPN solutions. Layer 3 VPNs use secure tunneling, which is the process of encapsulating one IP packet within another IP packet. Layer 3 VPNs use Layer 3 encryption; therefore, the payload that is being encrypted is the Layer 4–7 information. The private tunnel IP addresses are encrypted; however, the public IP addresses are still seen in cleartext. WEP uses Layer 2 encryption, which protects Layers 3–7. Many legacy WLAN security solutions used an IPsec VPN combined with WEP encryption. The WEP encryption was used to protect the IPsec VPN's public IP addresses. For more information, see Chapter 2.

5. E. The graphic depicts a packet capture of an 802.11 data frame protected by the proprietary Fortress encryption protocol. In addition to the Layer 2 encryption defined by the 802.11-2007 standard, proprietary Layer 2 encryption solutions such as xSec and Fortress can also be used for WLAN data privacy. For more information, see Chapter 3.

6. C. WEP, TKIP, and CCMP use symmetric algorithms. WEP and TKIP use the RC4 algorithm. CCMP uses the AES cipher. Public-key cryptography is based on asymmetric communications. For more information, see Chapter 3.

7. A, C. An 802.1X/EAP solution requires that both the supplicant and the authentication server support the same type of EAP. The authenticator must be configured for 802.1X/EAP authentication, but does not care which EAP type passes through. The authenticator and the supplicant must support the same type of encryption. The 802.1X/EAP process provides the seeding material for the 4-Way Handshake process that is used to create dynamic encryption keys. For more information, see Chapter 4.

8. A, E, F. Tunneled authentication is used to protect the exchange of client credentials between the supplicant and the AS within an encrypted TLS tunnel. All flavors of EAP-PEAP use tunneled authentication. EAP-TTLS and EAP-FAST also use tunneled authentication. While EAP-TLS is highly secure, it rarely uses tunneled authentication. Although rarely supported, an optional privacy mode does exist for EAP-TLS, which can be used to establish a TLS tunnel. EAP-MD5 and EAP-LEAP do not use tunneled authentication. For more information, see Chapter 4.

9. B. A transition security network (TSN) supports RSN-defined security as well as legacy security such as WEP within the same BSS. Within a TSN, some client stations will use RSNA security using TKIP/RC4 or CCMP/AES for encrypting unicast traffic. However, some legacy stations might use static WEP keys for unicast encryption. All of the clients will use WEP encryption for the broadcast and multicast traffic. Because all the stations share a single group encryption key for broadcast and multicast traffic, the lowest common denominator must be used for the group cipher. For more information, see Chapter 5.

10. A, B, C. AKM services defines the creation of encryption keys. Some of the encryption keys are derived from the authentication process, some of the keys are master keys, and some are the final keys that are used to encrypt/decrypt 802.11 data frames. The keys include the master session key (MSK), group master key (GMK), pairwise master key (PMK), group temporal key (GTK), and pairwise transient key (PTK). For more information, see Chapter 5.

11. A, C, E. WPA/WPA2-Enterprise solutions use 802.1X/EAP methods for authentication in enterprise environments. Most SOHO wireless networks are secured with WPA/WPA2-Personal mechanisms. WPA-Personal and WPA2-Personal both use the PSK authentication methods. PSK authentication is sometimes used in the enterprise, but is not recommended due to known weaknesses. Wi-Fi Protected Setup (WPS) defines simplified and automatic WPA and WPA2 security configurations for home and small-business users. Users can easily configure a network with security protection by using a personal identification number (PIN) or a button located on the access point and the client device. WPS is intended only for SOHO environments and is not meant to be used in the enterprise. For more information, see Chapter 6.

12. D. The 802.11-2007 standard defines two fast secure roaming mechanisms called preauthentication and PMK caching. Most WLAN vendors currently use an enhanced method of FSR called opportunistic key caching. The 802.11r-2008 amendment defines more complex Fast BSS transition (FT) methods of FSR. PMK caching, opportunistic key caching (OKC), and fast BSS transition (FT) all allow for 802.1X/EAP authentication to be skipped when roaming. Preauthentication still requires another 802.1X/EAP exchange through the original AP prior to the client roaming to a new target AP. For more information, see Chapter 7.

13. D. Probably the most overlooked rogue device is the ad hoc wireless network. The technical term for an 802.11 ad hoc WLAN is an independent basic service set (IBSS). The radio cards that make up an IBBS network consist solely of client stations, and no access point is deployed. The more common name for an IBSS is an ad hoc wireless network. An Ethernet connection and a Wi-Fi card can be bridged together—an intruder might access the ad hoc wireless network and then potentially route their way to the Ethernet connection and get onto the wired network. For more information, see Chapter 8.

14. A, C. 802.11 uses a medium contention process called Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). To ensure that only one radio card is transmitting on the half-duplex RF medium, CSMA/CA uses four checks and balances. The four checks and balances are virtual carrier sense, physical carrier sense, the random backoff timer, and interframe spacing. Virtual carrier sense uses a timer mechanism known as the network allocation vector (NAV) timer. Physical carrier sense uses a mechanism called the clear channel assessment (CCA) to determine whether the medium is busy before transmitting. Virtual carrier sense is susceptible to a DoS attack when an attacker manipulates the duration value of 802.11 frames. Physical carrier sense is susceptible to DoS when there is a continuous transmitter on the frequency channel. For more information, see Chapter 8.

15. C. A Layer 1 DoS attack can be accomplished using a wide-band jamming device or narrow-band jamming device. A wide-band jammer transmits a signal that raises the noise floor for most of the entire frequency band and therefore disrupts communications across multiple channels. The graphic shows a spectrum analyzer view of the narrow-band jammer that is disrupting service on several channels but not the entire frequency band. For much less money, an attacker could also use the Queensland Attack to disrupt an 802.11 WLAN. A major chipset manufacturer of 802.11b radio cards produced a software utility that placed the radios in a continuous transmit state for testing purposes. This utility can also be used for malicious purposes and can send out a constant RF signal much like a narrow-band signal generator. For more information, see Chapter 9.

16. B, C, E. Every WLAN vendor has their own sensor deployment recommendations and guidelines; however, a ratio of one sensor for every three to five access points is highly recommended. Full-time sensors are often placed strategically at the intersection points of three AP coverage cells. A common mistake is placing the sensors in a straight line as opposed to staggered sensor arrangement, which will ensure a wider area of monitoring. Another common sensor placement recommendation is to arrange sensors around the perimeter of the building. Perimeter placement increases the effectiveness of triangulation and also helps to detect WLAN devices that might be outside the building. Some of the better WLAN predictive modeling software solutions will also create models for recommended sensor placement. For more information, see Chapter 10.

17. B, E. Although the main purpose of an enterprise WIDS/WIPS is security monitoring, information collected by the WIPS can also be used for performance analysis. Since everything WLAN devices transmit is visible to the sensors, the Layer 2 information gathered can be used to determine the performance level of a WLAN including capacity and latency. For more information, see Chapter 10.

18. D, E. Most WLAN vendors now offer remote AP solutions that allow the AP to send traffic back to a WLAN controller across the Internet via an IPsec VPN tunnel. A standard VPN tunnel sends all traffic back to the corporate network and uses corporate network's remote gateway to the Internet. A remote AP configured in bridge mode uses two independent SSIDs. All users who connect to the corporate SSID have their traffic tunnel backed to the corporate network. All users who connect to a guest SSID have their traffic sent to a locally bridged gateway to the Internet. A split-tunnel configuration uses a single corporate SSID. Based on firewall ACLS enforced on the remote AP, some user traffic is sent up the VPN tunnel while other traffic is routed to the local gateway to the Internet. For more information, see Chapter 11.

19. A, C. Secure Shell or SSH is typically used as the secure alternative to Telnet. SSH implements authentication and encryption using public-key cryptography of all network traffic traversing between a host and a WLAN infrastructure device. HTTPS is essentially an SSL session that uses the HTTP protocol and is implemented on network devices for management via a graphical user interface (GUI). For more information, see Chapter 12.

20. B. When establishing a wireless security policy, you must first define a general policy. A general wireless security policy establishes why a wireless security policy is needed for an organization. General policy defines a statement of authority and the applicable audience. General policy also defines threat analysis and risk assessments. General policy defines internal auditing procedures as well as the need for independent outside audits. WLAN security policy should be enforced, and clear definitions are needed to properly respond to policy violations. For more information, see Chapter 13.

Chapter 1

WLAN Security Overview

IN THIS CHAPTER, YOU WILL LEARN ABOUT THE FOLLOWING:

- ✓ **Standards organizations**
  - International Organization for Standardization (ISO)
  - Institute of Electrical and Electronics Engineers (IEEE)
  - Internet Engineering Task Force (IETF)
  - Wi-Fi Alliance
- ✓ **802.11 networking basics**
- ✓ **802.11 security basics**
  - Data Privacy
  - Authentication, authorization, accounting (AAA)
  - Segmentation
  - Monitoring
  - Policy
- ✓ **802.11 security history**
  - 802.11i security amendment and WPA certifications
  - RSN
  - The future of 802.11 security

The 802.11-2007 standard defines *wireless local area network (WLAN)* technology, including all Layer 2 security mechanisms. To better understand WLAN security, you need to have a general appreciation of computer security and the components that are used to provide computer security. Security should never be taken lightly for wired or wireless networks. Since the early days of Wi-Fi communications, there has been a concern about the ability to transmit data securely over a wireless medium and properly protect wired network resources. This concern is as valid now as it was in 1997 when 802.11 was introduced. The difference between then and now is that the technologies and standards for Wi-Fi communications are much more secure and easier to implement. In addition to the standards providing better WLAN security, the people who are installing and managing these networks are much more knowledgeable about the design and implementation of secure wireless networks.

Even with all of the advances in 802.11 WLAN security, it still has a bad reputation with some people because of the weak legacy 802.11 security mechanisms that were deployed in the past. In 2004, the 802.11i amendment was ratified by the IEEE, defining stronger encryption and better authentication methods. The 802.11i amendment, which is now part of the 802.11-2007 standard, fully defines a robust security network (RSN), which is discussed later in this chapter. If proper encryption and authentication solutions are deployed, a wireless network can be just as secure as, if not more secure than, the wired segments of a network.

Before you learn about the various wireless security methods, techniques, and tools, it is important to learn some of the basic terms and concepts of encryption and computer security. WLAN security is based on many of the same concepts and principles as hard-wired systems, with the main difference being the natural reduced security of the unbounded medium (RF waves) that are used in wireless communications. Because data is transmitted freely and openly in the air, proper protection is needed to ensure data privacy. Thus strong encryption is needed.

The function of most wireless networks is to provide a portal into some other network infrastructure, such as an 802.3 Ethernet backbone. The wireless portal must be protected, and therefore an authentication solution is needed to ensure that only authorized users can pass through the portal via a wireless access point. After users have been authorized to pass through the wireless portal, virtual local area networks (VLANs) and identity-based mechanisms are needed to restrict access, additionally, to network resources. 802.11 wireless networks can be further protected with continuous monitoring by a wireless intrusion detection system. All of these security components should also be cemented with policy enforcement.

In this chapter we'll explore the basic terminology of WLAN security. We'll discuss the organizations that create the standards, certifications, and recommendations that help guide and direct wireless security. In addition, you'll learn about these wireless security standards and certifications.

Standards Organizations

Each of the standards organizations discussed in this chapter help guide a different aspect of security that is used in wireless networking.

The International Organization for Standardization (ISO) created the Open Systems Interconnection (OSI) model, which is an architectural model for data communications.

The Institute of Electrical and Electronics Engineers (IEEE) creates standards for compatibility and coexistence between networking equipment, not just wireless networking equipment. However, in this book we are concerned primarily with its role in wireless networking and more specifically wireless security.

The Internet Engineering Task Force (IETF) is responsible for creating Internet standards. Many of these standards are integrated into the wireless networking and security protocols and standards.

The Wi-Fi Alliance performs certification testing to make sure wireless networking equipment conforms to the 802.11 WLAN communication guidelines, similar to the IEEE 802.11-2007 standard.

You will look at each of these organizations in the following sections.

International Organization for Standardization (ISO)

The *International Organization for Standardization*, or *ISO,* is a global, nongovernmental organization that identifies business, government, and society needs and develops standards in partnership with the sectors that will put them to use. The ISO is responsible for the creation of the Open Systems Interconnection (OSI) model, which has been a standard reference for data communications between computers since the late 1970s.

Why Is It ISO and Not IOS?

ISO is not a mistyped acronym. It is a word derived from the Greek word *isos,* meaning *equal*. Because acronyms can vary among languages, the ISO decided to use a word instead of an acronym for its name. With this in mind, it is easy to see why a standards organization would give itself a name that means *equal.*

The OSI model is the cornerstone of data communications. Becoming familiar with it is one of the most important and fundamental tasks a person in the networking industry can undertake.

The layers of the OSI model are as follows:

- Layer 7, Application
- Layer 6, Presentation
- Layer 5, Session
- Layer 4, Transport
- Layer 3, Network
- Layer 2, Data-Link
  - LLC sublayer
  - MAC sublayer
- Layer 1, Physical

The IEEE 802.11-2007 standard defines communication mechanisms only at the Physical layer and MAC sublayer of the Data-Link layer of the OSI model. By design, the 802.11 standard does not address the upper layers of the OSI model, although there are interactions between the 802.11 MAC layer and the upper layers for parameters such as quality of service (QoS).

You should have a working knowledge of the OSI model for both this book and the CWSP exam. Make sure you understand the seven layers of the OSI model and how communication takes place at the different layers. If you are not comfortable with the concepts of the OSI model, spend some time reviewing it on the Internet or from a good networking fundamentals book prior to taking the CWSP exam. More information about the ISO can be found at `www.iso.org`.

Institute of Electrical and Electronics Engineers (IEEE)

The Institute of Electrical and Electronics Engineers, commonly known as the IEEE, is a global professional society with more than 350,000 members. The IEEE's mission is to "foster technological innovation and excellence for the benefit of humanity." To networking professionals, that means creating the standards that we use to communicate.

The IEEE is probably best known for its LAN standards, the IEEE 802 project. IEEE projects are subdivided into working groups to develop standards that address specific problems or needs. For instance, the IEEE 802.3 working group was responsible for the creation of a standard for Ethernet, and the IEEE 802.11 working group was responsible for creating the WLAN standard. The numbers are assigned as the groups are formed, so the 11 assigned to the wireless group indicates that it was the 11th working group

formed under the IEEE 802 project. IEEE 802.11, more commonly referred to as Wi-Fi, is a standard technology for providing local area network (LAN) communications using radio frequencies (RF). The IEEE designates the 802.11-2007 standard as the most current guideline to provide operational parameters for WLANs.

As the need arises to revise existing standards created by the working groups, task groups are formed. These task groups are assigned a sequential single letter (multiple letters are assigned if all single letters have been used) that is added to the end of the standard number (for example, 802.11g, 802.11i, and 802.3af). Some letters are not assigned. For example, o and l are not assigned to prevent confusion with the numbers 0 and 1. Other letters may not be assigned to task groups to prevent confusion with other standards. For example, 802.11x has not been assigned because it can be easily confused with the 802.1X standard and because 802.11x has become a common casual reference to the 802.11 family of standards.

More information about the IEEE can be found at `www.ieee.org`.

It is important to remember that the IEEE standards, like many other standards, are written documents describing how technical processes and equipment should function. Unfortunately, this often allows for different interpretations when the standard is being implemented, so it is common for early products to be incompatible between vendors, as was the case with early 802.11 products.

The CWSP exam is based on the most recently published version of the standard, 802.11-2007. The 802.11-2007 standard can be downloaded from `http://standards.ieee.org/getieee802/802.11.html`.

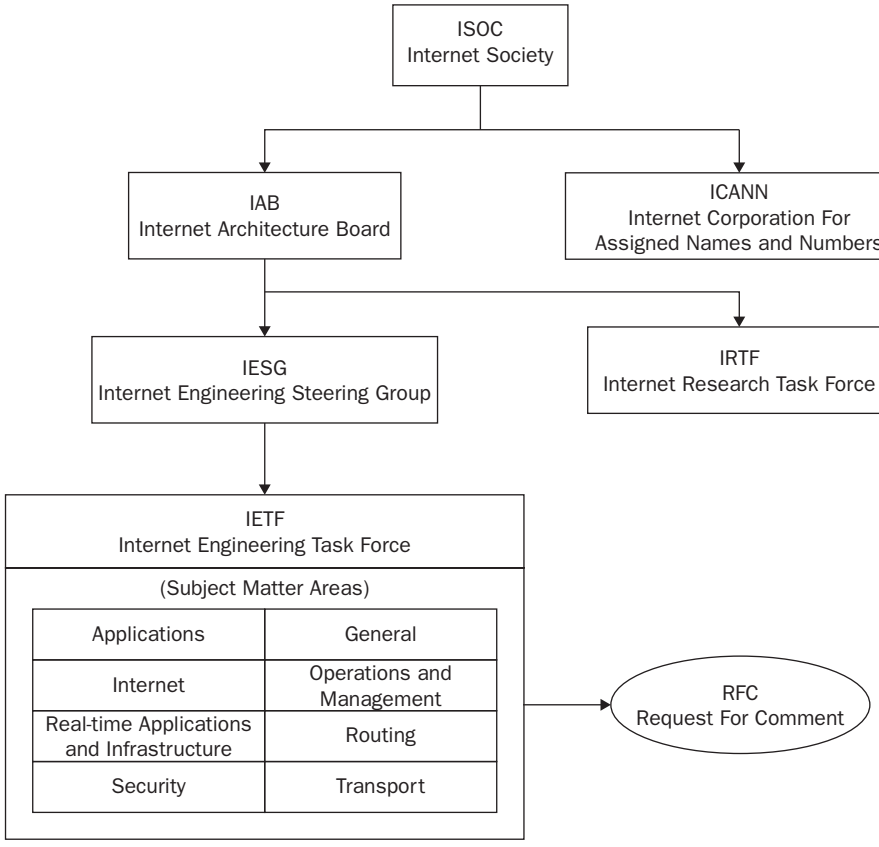
Internet Engineering Task Force (IETF)

The Internet Engineering Task Force, commonly known as the IETF, is an international community of people in the networking industry whose goal is to make the Internet work better. The mission of the IETF, as defined by the organization in a document known as RFC 3935, is "to produce high quality, relevant technical and engineering documents that influence the way people design, use, and manage the Internet in such a way as to make the Internet work better. These documents include protocol standards, best current practices, and informational documents of various kinds." The IETF has no membership fees, and anyone may register for and attend an IETF meeting.

The IETF is one of five main groups that are part of the Internet Society (ISOC). The ISOC groups include the Internet Architecture Board (IAB), the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Engineering Steering Group (IESG), the Internet Research Task Force (IRTF), and the IETF. The IETF is broken into eight

subject matter areas: Applications, General, Internet, Operations and Management, Real-Time Applications and Infrastructure, Routing, Security, and Transport. Figure 1.1 shows the hierarchy of the ISOC and a breakdown of the IETF subject matter areas.

FIGURE 1.1 ISOC hierarchy



The IESG provides technical management of the activities of the IETF and the Internet standards process. The IETF is made up of a large number of groups, each addressing specific topics. An IETF working group (WG) is created by the IESG and is given a specific charter or specific topic to address. There is no formal voting process for the working groups. Decisions in working groups are made by rough consensus, or basically a general sense of agreement among the working group.

The results of a working group are usually the creation of a document known as a Request for Comments (RFC). Contrary to its name, an RFC is not actually a request for

comment, but a statement or definition. Most RFCs describe network protocols, services, or policies and may evolve into an Internet standard. RFCs are numbered sequentially, and once a number is assigned it is never reused. RFCs may be updated or supplemented by higher numbered RFCs. As an example, Mobile IPv4 is described in RFC 3344 and updated in RFC 4721. When RFC 3344 was created, it made RFC 3220 obsolete. At the top of the RFC document, it states whether it is updated by another RFC and also if it makes any other RFCs obsolete.

Not all RFCs are standards. Each RFC is given a status, relative to its relationship with the Internet standardization process: Informational, Experimental, Standards Track, or Historic. If it is a Standards Track RFC, it could be a Proposed Standard, Draft Standard, or Internet Standard. When an RFC becomes a standard, it still keeps its RFC number, but it is also given an "STD xxxx" label. The relationship between the STD numbers and the RFC numbers is not one to one. STD numbers identify protocols whereas RFC numbers identify documents.

Many of the protocol standards, best current practices, and informational documents produced by the IETF affect WLAN security. In Chapter 4, "Enterprise 802.11 Layer 2 Authentication Methods," you will learn about the many varieties of the Extensible Authentication Protocol (EAP) that is defined by the IETF RFC 3748.

More information about the IETF can be found at `www.ietf.org`.

Wi-Fi Alliance

The Wi-Fi Alliance, originally named the Wireless Ethernet Compatibility Alliance (WECA), was founded in August 1999. Its name was changed to the Wi-Fi Alliance in October 2002. The Wi-Fi Alliance is a global, nonprofit industry association of more than 300 member companies devoted to promoting the growth of WLANs. One of the primary tasks of the Wi-Fi Alliance is to market the Wi-Fi brand and raise consumer awareness of new 802.11 technologies as they become available. Because of the Wi-Fi Alliance's overwhelming marketing success, the majority of the worldwide 450 million Wi-Fi users immediately recognize the Wi-Fi logo (see Figure 1.2).

FIGURE 1.2 Wi-Fi Alliance logo

The Wi-Fi Alliance's main task is to ensure the interoperability of WLAN products by providing certification testing. During the early days of the 802.11 standard, the Wi-Fi Alliance further defined some of the ambiguous standards requirements and

provided a set of guidelines to ensure compatibility between different vendors. Products that pass the Wi-Fi certification process receive a Wi-Fi Interoperability Certificate that provides detailed information about the individual product's Wi-Fi certifications (see Figure 1.3). This certification includes not only radio interoperability such as 802.11a and 802.11b, but also certification of additional capabilities such as security, multimedia, convergence, and supported special features.

FIGURE 1.3 Wi-Fi Interoperability Certificate

The Wi-Fi Alliance has certified more than 4,600 Wi-Fi products for interoperability since testing began in April 2000. Multiple Wi-Fi CERTIFIED programs exist that cover basic connectivity, security, quality of service (QoS), and more. Testing of vendor Wi-Fi products is performed in 12 independent authorized test laboratories worldwide. The interoperability guidelines for each Wi-Fi CERTIFIED program are usually based on key components and functions that are defined in the IEEE 802.11-2007 standard and various 802.11 amendments. In fact, many of the same engineers who belong to 802.11 task groups are also contributing members of the Wi-Fi Alliance. However, it is important to understand that the IEEE and the Wi-Fi Alliance are two separate organizations—the IEEE 802.11 task group defines the WLAN standards, and the Wi-Fi Alliance defines interoperability certification programs. The Wi-Fi CERTIFIED programs include the following:

802.11a, b, or g—IEEE 802.11 Baseline The baseline program certifies 802.11a, b, and/or g interoperability to ensure that the essential wireless data transmission works as

expected. 802.11b and 802.11g utilize frequencies in the 2.4 GHz band. 802.11g has a higher data rate (54 Mbps) than 802.11b (11 Mbps). 802.11a utilizes frequencies in the 5 GHz band and has a maximum data rate of 54 Mbps. Each certified product is required to support one frequency band at a minimum, but it can support more. The CWSP exam will not use the terms 802.11 a/b/g; however, the a/b/g terminology is commonplace within the industry because of the Wi-Fi Alliance baseline certifications.

802.11n—IEEE 802.11 Baseline This certification program is based on the recently ratified 802.11n-2009 amendment that defines a High Throughput (HT) wireless network utilizing multiple-input multiple-output (MIMO) technology. High Throughput (HT) provides PHY (physical layer of the OSI model) and MAC (Media Access Control) enhancements to support throughput of 100 Mbps and greater.

Wi-Fi Protected Access 2 (WPA2)—Security WPA2 is based on the security mechanisms that were originally defined in the IEEE 802.11i amendment that defines a robust security network (RSN). Two versions of WPA2 exist: WPA2-Personal defines security for a SOHO (Small Office/Home Office) environment, and WPA2-Enterprise defines stronger security for enterprise corporate networks. Each certified product is required to support WPA2-Personal or WPA2-Enterprise. A more detailed discussion of WPA2 security can be found later in this chapter.

Wi-Fi Protected Setup—Security Wi-Fi Protected Setup (WPS) defines simplified and automatic WPA and WPA2 security configurations for home and small-business users. Users can easily configure a network with security protection by using a personal identification number (PIN) or a button located on the access point and the client device. Wi-Fi Protected Setup mechanisms are discussed in greater detail in Chapter 6, "SOHO 802.11 Security."

Wi-Fi Multimedia (WMM)—Multimedia WMM is based on the QoS mechanisms that were originally defined in the IEEE 802.11e amendment. WMM enables Wi-Fi networks to prioritize traffic generated by different applications. In a network where WMM is supported by both the access point and the client device, traffic generated by time-sensitive applications such as voice or video can be prioritized for transmission on the half-duplex RF medium.

WMM Power Save (WMM-PS)—Multimedia WMM-PS helps conserve battery power for devices using Wi-Fi radios by managing the time the client device spends in sleep mode. Conserving battery life is critical for handheld devices such as barcode scanners and Voice over Wi-Fi (VoWiFi) phones. To take advantage of power-saving capabilities, both the device and the access point must support WMM Power Save.

CWG-RF—Multimedia Converged Wireless Group-RF Profile (CWG-RF) was developed jointly by the Wi-Fi Alliance and the Cellular Telecommunications and Internet Association (CTIA), now known as The Wireless Association. CWG-RF defines performance metrics for Wi-Fi and cellular radios in a converged handset to help ensure that both technologies perform well in the presence of the other. All CTIA-certified handsets now include this certification.

Voice Personal—Application Voice Personal offers enhanced support for voice applications in residential and small-business Wi-Fi networks. These networks include one access point, mixed voice and data traffic from multiple devices (such as phones, PCs, printers, and other consumer electronic devices), and support for up to four concurrent phone calls. Both the access point and the client device must be certified to achieve performance matching the certification metrics.

As 802.11 technologies evolve, new Wi-Fi CERTIFIED programs will be detailed by the Wi-Fi Alliance. The next certification will probably be Voice Enterprise, which will define enhanced support for voice applications in the enterprise environment. Some aspects of the 802.11r (secure roaming) and 802.11k (resource management) amendments will probably be tested in Voice Enterprise.

Wi-Fi Alliance and Wi-Fi CERTIFIED

More information about the Wi-Fi Alliance can be found at `www.wi-fi.org`. The following seven white papers from the Wi-Fi Alliance are also included on the CD that accompanies this book:

- *The State of Wi-Fi Security*
- *Wi-Fi CERTIFIED for Wi-Fi Protected Setup: Easing the User Experience for Home and Small Office Wi-Fi Networks*
- *Wi-Fi CERTIFIED for WMM: Support for Multimedia Applications with Quality of Service in Wi-Fi Networks*
- *WMM Power Save for Mobile and Portable Wi-Fi CERTIFIED Devices*
- *Wi-Fi CERTIFIED n: Longer-Range, Faster-Throughput, Multimedia-Grade Wi-Fi Networks*
- *Wi-Fi CERTIFIED Voice-Personal: Delivering the Best End-User Experience for Voice over Wi-Fi*

802.11 Networking Basics

In addition to understanding the OSI model and basic networking concepts, you must broaden your understanding of many other networking technologies in order to design, deploy, and administer an 802.11 wireless network properly. For instance, when administering an Ethernet network, you typically need a comprehension of TCP/IP, bridging, switching, and routing. The skills to manage an Ethernet network will also aid you as a WLAN administrator, because most 802.11 wireless networks act as "portals"

into wired networks. The IEEE defines the 802.11 communications at the Physical layer and the MAC sublayer of the Data-Link layer.

To understand the 802.11 technology completely, you need to have a clear concept of how wireless technology works at the Physical layer of the OSI model, and at the heart of the Physical layer is *radio frequency (RF)* communications. A clear concept of how wireless works at the second layer of the OSI model is also needed. The 802.11 *Data-Link layer* is divided into two sublayers. The upper portion is the IEEE 802.2 *Logical Link Control (LLC)* sublayer, which is identical for all 802-based networks, although not used by all of them. The bottom portion of the Data-Link layer is the *Media Access Control (MAC) sublayer*, which is identical for all 802.11-based networks. The 802.11-2007 standard defines operations at the MAC sublayer.

Because the main focus of this study guide is WLAN security, it is beyond the scope of this book to discuss general 802.11 networking topics in great detail. For a broad overview of 802.11 technology, we suggest *CWNA: Certified Wireless Network Administrator Official Study Guide: (Exam PW0-104)*, by David D. Coleman and David A. Westcott (Sybex, 2009).

If you have ever taken a networking class or read a book about network design, you have probably heard the terms *core*, *distribution*, and *access* when referring to networking architecture. Proper network design is imperative no matter what type of network topology is used. The core of the network is the high-speed backbone or the superhighway of the network. The goal of the core is to carry large amounts of information between key data centers or distribution areas, just as superhighways connect cities and metropolitan areas.

The core layer does not route traffic or manipulate packets but rather performs high-speed switching. Redundant solutions are usually designed at the core layer to ensure fast and reliable delivery of packets. The distribution layer of the network routes or directs traffic toward the smaller clusters of nodes or neighborhoods of the network.

The distribution layer routes traffic between virtual LANs (VLANs) and subnets. The distribution layer is akin to the state and county roads that provide medium travel speeds and distribute the traffic within a city or metropolitan area.

The access layer of the network is responsible for a delivery of the traffic directly to the end user or end node. The access layer mimics the local roads and neighborhood streets that are used to reach your final address; thus the speed of delivery in this layer is slower than at the core and distribution layers. (Remember that speed is a relative concept.) The access layer ensures the final delivery of packets to the end user.

Because of traffic load and throughput demands, speed and throughput capabilities increase as data moves from the access layer to the core layer. Additional speed and throughput tend to also mean higher cost.

Just as it would not be practical to build a superhighway so that traffic could travel between your neighborhood and the local school, it would not be practical or efficient to build a two-lane road as the main thoroughfare to connect two large cities such as New York and Boston. These same principles apply to network design. Each of the network

layers—core, distribution, and access—are designed to provide a specific function and capability to the network. It is important to understand how wireless networking fits into this network design model.

Wireless networking can be implemented as either point-to-point or point-to-multipoint solutions. Most wireless networks are used to provide network access to the individual client stations and are designed as point-to-multipoint networks. This type of implementation is designed and installed on the access layer, providing connectivity to the end user. 802.11 wireless networking is most often implemented at the access layer. In Chapter 12, "Wireless Security Infrastructure," you will learn about the difference between *autonomous access points* and the centralized *WLAN controller* solutions that utilize *controller-based access points*. All access points are deployed at the access layer; however, controller-based access points tunnel 802.11 wireless traffic to WLAN controllers which are typically deployed at the distribution or core layer.

Wireless bridge links are generally used to provide connectivity between buildings in the same way that county or state roads provide distribution of traffic between neighborhoods. The purpose of wireless bridging is to connect two separate, wired networks wirelessly. Routing data traffic between networks is usually associated with the distribution layer. Wireless bridge links cannot typically meet the speed or distance requirements of the core layer, but they can be very effective at the distribution layer. An 802.11 bridge link is an example of wireless technology being implemented at the distribution layer.

Throughout this study guide, you will learn how to provide proper 802.11 wireless security integration at the access, distribution, and core layers of network design.

802.11 Security Basics

When you're securing a wireless 802.11 network, five major components are typically required:

- Data privacy
- Authentication, authorization, and accounting (AAA)
- Segmentation
- Monitoring
- Policy

Because data is transmitted freely and openly in the air, proper protection is needed to ensure *data privacy*, so strong encryption is needed. The function of most wireless networks is to provide a portal into some other network infrastructure, such as an 802.3 Ethernet backbone. The wireless portal must be protected, and therefore an authentication solution is needed to ensure that only authorized users can pass through the portal via a wireless access point. After users have been authorized to pass through the wireless portal, VLANs and identity-based mechanisms are needed to further restrict access to network resources. 802.11 wireless networks can be further protected with continuous monitoring

by a wireless intrusion detection system. All of these security components should also be cemented with policy enforcement. If properly implemented, these five components of 802.11 security discussed throughout this book will lay a solid foundation for protecting your WLAN.

Data Privacy

The history of secure communications is as old as the history of communications itself. Sharing ideas and thoughts with specific people but not others is a natural human desire. The task of sharing a thought is easy when the person you want to share it with is nearby. A quiet, private conversation is often all that is needed to do this. Sharing an idea in a secure way starts to become a problem when you need to send your message over a longer distance. Whether you have to yell the message to the other person from a distance, send it to the other person via a courier, or write it down on a piece of paper and send it, all of these methods run a risk of being intercepted. Because of these types of risks, methods of encrypting or encoding messages were created. The goal of encrypting a message, even if it is overheard or intercepted, is for it to be legible only to the person who created the message and the person for whom the message is intended—or at least, that's the intent.

802.11 wireless networks operate in license-free frequency bands, and all data transmissions travel in the open air. Protecting data privacy in a wired network is much easier because physical access to the wired medium is more restricted. However, physical access to wireless transmissions is available to anyone in listening range. Therefore, using cipher encryption technologies to obscure information is mandatory to provide proper data privacy in wireless networks. A *cipher* is an algorithm used to perform encryption.

Along with the desire by some to keep things a secret, there is often an equal desire by others to reveal these secrets. The techniques needed to encrypt and decrypt information forms the science known as *cryptology*. As you would expect, the science of cryptology uses specific words and phrases, many of which you will learn about in this section.

The term *cryptology* is derived from the Greek language and translates to mean "hidden word." The goal of cryptology is to take a piece of information, often referred to as *plaintext*, and, using a process or algorithm, also referred to as a *key* or *cipher*, to transform the plaintext into encrypted text, also known as *ciphertext*. The process of encrypting plaintext is shown in Figure 1.4. This ciphertext could then only be decrypted, converted back into plaintext, by someone who knows the key or cipher. The process of decrypting the ciphertext is shown in Figure 1.5.

FIGURE 1.4 The encryption process

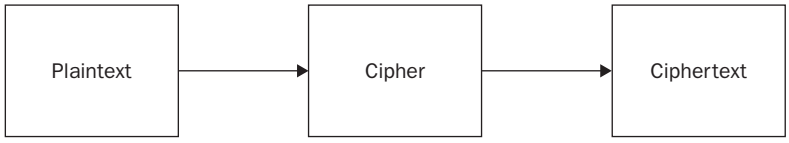
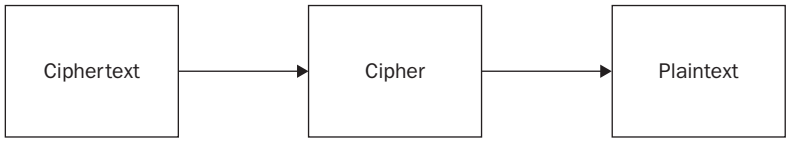


FIGURE 1.5 The decryption process



When a plaintext message is encrypted, the encrypted message is referred to as ciphertext. A detailed discussion about encryption methods used for WLAN security can be found in Chapter 3, "Encryption Ciphers and Methods."

When discussing cryptology, it is important to use the term *cipher* instead of *code*, as a code is simply a way of representing information in a different way. For example, the American Standard Code for Information Interchange (ASCII) represents information as letters, numbers, and other characters, or the way that Morse code uses dots and dashes to represent letters. Like a code, a cipher also represents information in a different way. However, a cipher uses a secret technique of representing the information in a different way, with this technique known only to a select few.

The science of concealing the plaintext and then revealing it is known as *cryptography*. In the computer and networking industries, the process of converting plaintext into ciphertext is commonly referred to as *encryption*, and the process of converting ciphertext back to plaintext is commonly referred to as *decryption*. The science of decrypting the ciphertext without knowledge of the key or cipher is known as *cryptanalysis*. If cryptanalysis is successful in decrypting the ciphertext, then that key or cipher is considered to be broken, cracked, or not secure.

The term *steganography* is also derived from the Greek language and is translated as "concealed writing." Unlike cryptography, where the goal is to make the message unreadable to someone without access to the key or cipher, steganography strives to hide the fact that there is a message. This is often referred to as "security through obscurity" or "hiding a message in plain sight." A classic example of using steganography to hide a message is to write a document with the first letter of each sentence or word as the hidden message (see Figure 1.6).

FIGURE 1.6 Steganography example

Sent Message: Here is my obscure message. Saturday evening nobody dared make outbursts, not even Yolanda.

Here **i**s **m**y **o**bscure **m**essage. **S**aturday **e**vening **n**obody **d**ared **m**ake **o**utbursts, **n**ot **e**ven **Y**olanda.

Hidden Message: Hi mom send money

Steganography is often used for digital watermarking, which embeds an artist or photographer's information in an image so that ownership can be proven in case someone tries to use the image without permission. Steganography is useful for hiding a message where one would not be expected, which is why it is not used in environments like wireless networking where data communications is the key objective.

Authentication, Authorization, Accounting (AAA)

Authentication, authorization, and accounting (AAA) is a common computer security concept that defines the protection of network resources.

Authentication is the verification of user identity and credentials. Users must identify themselves and present credentials, such as usernames and passwords or digital certificates. More secure authentication systems use multifactor authentication, which requires at least two sets of different credentials to be presented.

Authorization involves granting access to network resources and services. Before authorization to network resources can be granted, proper authentication must occur.

Accounting is tracking the use of network resources by users. It is an important aspect of network security that is used to keep a paper trail of who used which resource and when. A record is kept of user identity, which resource was accessed, and at what time. Keeping an accounting trail is often a requirement of many industry regulations, such as the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Remember that the usual purpose of an 802.11 wireless network is to act as a portal into an 802.3 wired network. It is therefore necessary to protect that portal with very strong authentication methods so that only legitimate users with the proper credentials will be authorized to access network resources.

Segmentation

Although it is of the utmost importance to secure an enterprise wireless network by utilizing both strong encryption and an AAA solution, an equally important aspect of wireless security is segmentation. Before the introduction of stronger authentication and encryption techniques, wireless was viewed as an untrusted network segment. Therefore, before the ratification of the 802.11i security amendment, the entire wireless segment of a network was commonly treated as the untrusted segment, while the wired 802.3 network was considered the trusted segment.

Now that better security solutions exist, properly secured WLANs are more seamlessly and securely integrated into the wired infrastructure. It is still important to separate users into proper groups, much like what is done on any traditional network. Once authorized onto network resources, users can be further restricted as to what resources they may access and where they can go. Segmentation can be achieved through a variety of means, including firewalls, routers, VPNs, and VLANs. The most common wireless segmentation strategy used in 802.11 enterprise WLANs is Layer 3 segmentation using VLANs. Segmentation is also intertwined with role-based access control (RBAC), commonly used by WLAN controllers.

Monitoring

After you have designed and installed your wireless network, it is important to monitor it. In addition to monitoring it to make sure that it is performing up to your expectations and those of your users, it is necessary to monitor it for attacks and intrusions constantly. Similar to a business placing a video camera on the outside of its building to monitor the traffic going in and out of a locked door, it is important for the wireless network administrator to monitor the wireless traffic of a secured network. To monitor potentially malicious wireless activity on your network, you should install a wireless intrusion detection system (WIDS).

In addition to a WIDS, you could implement a wireless intrusion prevention system (WIPS). Both WIDSs and WIPSs have the ability to classify valid and invalid devices on the network. WIPS can also mitigate attacks from rogue access points and rogue clients by performing attacks against the rogue devices, effectively disabling their ability to communicate with your network. WIPSs will be discussed in detail in Chapter 10, "Wireless Security Monitoring."

Policy

Securing a wireless network and monitoring for threats are absolute necessities, but both are worthless unless proper security policies are in place. What good is an 802.1X/EAP solution if the end users share their passwords? Why purchase an intrusion detection system if a policy has not been established for dealing with rogue access points? WLAN security policies must be clearly defined and enforced to solidify the effectiveness of all WLAN security components.

In most countries, mandated regulations exist for protecting and securing data communications within all government agencies. In the United States, the National Institute of Standards and Technology (NIST) maintains the *Federal Information Processing Standards (FIPS)*. Of special interest to wireless security is the FIPS 140-2 standard, which defines security requirements for cryptography modules. Additionally, other legislation and regulations exist for protecting information and communications in certain industries such as healthcare and banking. WLAN policy enforcement is needed to meet compliance mandates set forth by these regulations. Policies and compliance regulations will be discussed in greater detail in Chapter 13, "Wireless Security Policies."

802.11 Security History

From 1997 to 2004, not much was defined in terms of security in the original IEEE 802.11 standard. Two key components of any wireless security solution are data privacy (encryption) and authentication (identity verification). For seven years, the only defined method of encryption in an 802.11 network was the use of 64-bit static encryption called *Wired Equivalent Privacy (WEP)*.

WEP encryption has long been cracked and is not considered an acceptable means of providing data privacy. The original 802.11 standard defined two methods of authentication. The default method is *Open System authentication*, which verifies the identity of everyone regardless. Another defined method is called *Shared Key authentication*, which opens up a whole new can of worms and potential security risks. Outdated 802.11 security mechanisms will be discussed in detail in Chapter 2, "Legacy 802.11 Security."

802.11i Security amendment and WPA Certifications

The 802.11i amendment, which was ratified and published as IEEE Std. 802.11i-2004, defined stronger encryption and better authentication methods. The 802.11i amendment defined a *robust security network (RSN)*.The intended goal of an RSN was to hide the data flying through the air better while at the same time placing a bigger guard at the front door. The 802.11i security amendment was without a doubt one of the most important enhancements to the original 802.11 standard because of the seriousness of properly protecting a wireless network. The major security enhancements addressed in the 802.11i amendment are as follows:

Enhanced Data Privacy Confidentiality needs have been addressed in 802.11i with the use of a stronger encryption method called *Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)*, which uses the *Advanced Encryption Standard (AES)* algorithm. The encryption method is often abbreviated as CCMP/AES, AES CCMP, or often just CCMP. The 802.11i supplement also defines an optional encryption method known as *Temporal Key Integrity Protocol (TKIP)*, which uses the RC-4 stream cipher algorithm and is basically an enhancement of WEP encryption.

Enhanced Authentication 802.11i defines two methods of authentication using either an IEEE *802.1X* authorization framework or *preshared keys (PSKs)*. An 802.1X solution requires the use of an *Extensible Authentication Protocol (EAP)*, although the 802.11i amendment does not specify what EAP method to use.

In 2004, the 802.11i security amendment was ratified and is now part of the 802.11-2007 standard. All aspects of the 802.11i ratified security amendment can now be found in clause 8 of the 802.11-2007 standard.

The current 802.11-2007 standard defines an enterprise authentication method as well as a method of authentication for home use. The current standard requires the use of an 802.1X/EAP authentication method in the enterprise and the use of a preshared key or a passphrase in a SOHO environment. The 802.11-2007 standard also requires the use of strong, dynamic encryption-key generation methods. CCMP/AES encryption is the default encryption method, while TKIP/RC4 is an optional encryption method.

Prior to the IEEE ratification of the 802.11i amendment, the Wi-Fi Alliance introduced the *Wi-Fi Protected Access (WPA)* certification as a snapshot of the not-yet-released 802.11i

amendment, supporting only TKIP/RC4 dynamic encryption-key generation. 802.1X/EAP authentication was required in the enterprise, and passphrase authentication was required in a SOHO environment.

After 802.11i was ratified by the IEEE, the Wi-Fi Alliance introduced the *Wi-Fi Protected Access 2 (WPA2)* certification. WPA2 is a more complete implementation of the 802.11i amendment and supports both CCMP/AES and TKIP/RC4 dynamic encryption-key generation. 802.1X/EAP authentication is required in the enterprise, and passphrase authentication is required in a SOHO environment. WPA version 1 was considered a preview of 802.11i, whereas WPA version 2 is considered more of a mirror of the 802.11i security amendment. Once again, you should understand that all aspects of the 802.11i ratified security amendment are now defined as part of the 802.11-2007 standard. Table 1.1 compares the various security standards and certifications.

TABLE 1.1 Security Standards and Certifications

802.11 Standard	Wi-Fi Alliance Certification	Authentication Method	Encryption Method	Cipher	Key Generation
802.11 legacy		Open System or Shared Key	WEP	RC4	Static
	WPA-Personal	WPA Passphrase (also known as WPA PSK and WPA Pre-Shared Key)	TKIP	RC4	Dynamic
	WPA-Enterprise	802.1X/EAP	TKIP	RC4	Dynamic
802.11- 2007	WPA2-Personal	WPA2 Pass-phrase (also known as WPA2 PSK and WPA2 Pre-Shared Key)	CCMP (mandatory)	AES (manda-tory)	Dynamic
			TKIP (optional)	RC4 (optional)	
802.11-2007	WPA2-Enterprise	802.1X/EAP	CCMP (mandatory)	AES (manda-tory)	Dynamic
			TKIP (optional)	RC4 (optional)	

Robust Security Network (RSN)

The 802.11-2007 standard defines what is known as a *robust security network (RSN)* and *robust security network associations (RSNAs)*. Two stations (STAs) must establish a procedure to authenticate and associate with each other as well as create dynamic encryption keys through a process known as the 4-Way Handshake. This association between two stations is referred to as an RSNA. In other words, any two radios must share dynamic encryption keys that are unique between those two radios. CCMP/AES encryption is the mandated encryption method, while TKIP/RC4 is an optional encryption method. A robust security network (RSN) is a network that allows for the creation of only robust security network associations (RSNAs). The 802.11-2007 standard does allow for the creation of pre-robust security network associations (pre-RSNAs) as well as RSNAs. In other words, legacy security measures can be supported in the same *basic service set (BSS)* along with RSN-security-defined mechanisms. A *transition security network (TSN)* supports RSN-defined security as well as legacy security such as WEP within the same BSS.

Robust network security, the 4-Way Handshake, and dynamic encryption are discussed in more detail in Chapter 5, "802.11 Dynamic Encryption Key Generation."

The Future of 802.11 Security

Several recently ratified IEEE 802.11 amendments offer even further enhancements to robust security network (RSN) mechanisms defined by the 802.11-2007 standard. The 802.11r amendment is known as the *fast basic service set transition (FT)* amendment. The technology is more often referred to as *fast secure roaming* because it defines faster handoffs when roaming occurs between cells in a WLAN using the strong security defined by a robust secure network (RSN). 802.11r was proposed primarily because of the time constraints of applications such as Voice over IP (VoIP). Average time delays of hundreds of milliseconds occur when a client station roams from one access point to another access point.

Roaming can be especially troublesome when using an 802.11 WPA-Enterprise or a WPA2-Enterprise security solution, which requires the use of a RADIUS server for 802.1X/EAP authentication and often takes 700 milliseconds or greater for the client to authenticate. VoWiFi requires a handoff of 150 milliseconds or less to avoid a degradation of the quality of the call, or, even worse, a loss of connection. Currently 802.1X/EAP security solutions are rare in time-critical environments because of the latency problems caused by the long roaming handoff times.

The 802.11r amendment is not part of the 802.11-2007 standard. However, it was ratified in July 2008 and is published as IEEE 802.11r-2008. Tactical enterprise deployments of this technology will be extremely important for providing more secure communications for VoWiFi.

The recently ratified 802.11k amendment in conjunction with the recently ratified 802.11r "fast roaming" amendment have the potential to improve roaming performance greatly in secure 802.11 wireless networks. As defined by 802.11k amendment, an access point or WLAN controller will request a station to listen for neighbor access points on other channels and gather information. The current AP or WLAN controller will then process that information and generate a *neighbor report* detailing available access points from best to worst. Before a station roams, it will request the neighbor report from the current AP or controller and then decide whether to roam to one of the access points on the neighbor report.

The 802.11k amendment is not part of the 802.11-2007 standard. However, it was ratified in June 2008 and is published as IEEE 802.11k-2008.

A detailed discussion of 802.11r mechanisms can be found in Chapter 7, "802.11 Fast Secure Roaming."

A common type of attack on an 802.11 WLAN is a denial-of-service attack (DoS). There are a multitude of DoS attacks that can be launched against a wireless network; however, a very common DoS attack occurs at layer 2 using 802.11 management frames. Currently, it is simple for an attacker to edit deauthentication or disassociation frames and then retransmit the frames into the air, effectively shutting down the wireless network.

The 802.11w amendment is also known as the "protected" management frame amendment because of the goal of delivering certain 802.11 management frames in a secure manner. The end result will hopefully prevent some but not all of the Layer 2 DoS attacks that currently exist. The 802.11w amendment is not part of the 802.11-2007 standard. However, it was ratified in September 2009 and is published as IEEE 802.11w-2009.

A discussion about both Layer 1 and Layer 2 DoS attacks can be found in Chapter 8, "Wireless Security Risks." More information about the 802.11w-2009 amendment can be found in Chapter 10.

Where Else can I Learn More about 802.11 Security and the Wi-Fi Industry?

Reading this book from cover to cover is a great way to start understanding WLAN security. In addition, because of the rapidly changing nature of 802.11 WLAN technologies, the authors of this book would like to recommend these additional resources:

WNN Wi-Fi Net News (WNN) is a highly respected blog and daily newsletter about all the latest events and happenings in the Wi-Fi industry. WNN is maintained by blogger Glenn Fleishman, and it has more than 100,000 subscribers. Do yourself a favor and subscribe to Wi-Fi Net News at `www.wifinetnews.com`.

Wi-Fi Alliance As mentioned earlier in this chapter, the Wi-Fi Alliance is the marketing voice of the Wi-Fi industry and maintains all the industry's certifications. The knowledge center section of the Wi-Fi Alliance website, `www.wi-fi.org`, is an excellent resource.

CWNP The Certified Wireless Networking Professional program maintains learning resources such as user forums and a WLAN white paper database. The website `www.cwnp.com` is also the best source of information about all the vendor-neutral CWNP wireless networking certifications.

WLAN Vendor Websites Although the CWSP exam and this book take a vendor-neutral approach to 802.11 security, the various WLAN vendor websites are often an excellent resource for information about specific Wi-Fi security solutions. Many of the major WLAN vendors are mentioned throughout this book, and a complete listing of most of the major WLAN vendor websites can be found in this book's appendix.

Summary

This chapter explained the roles and responsibilities of four key organizations involved with wireless security and networking:

- ISO
- IEEE
- IETF
- Wi-Fi Alliance

To provide a basic understanding of the relationship between networking fundamentals and 802.11 technologies, we discussed these concepts:

- OSI model
- Core, distribution, and access

To provide a basic knowledge of data privacy, we introduced some of the basic components of security:

- Cryptology
- Cryptography
- Cryptanalysis
- Steganography
- Plaintext
- Key
- Cipher
- Ciphertext

Five major components that are typically required to secure an 802.11 network were also discussed:

- Data privacy
- Authentication, authorization, and accounting (AAA)
- Segmentation
- Monitoring
- Policy

To provide an initial foundation, we reviewed the 802.11 security history, including:

- 802.11 legacy, WEP
- WPA-Personal
- WPA-Enterprise
- 802.11-2007 (RSN) - WPA2-Personal
- 802.11-2007 (RSN) - WPA2-Enterprise

Exam Essentials

Know the four industry organizations. Understand the roles and responsibilities of the ISO, the IEEE, the IETF, and the Wi-Fi Alliance.

Understand data privacy, AAA, segmentation, monitoring, and policy. Know the five major components typically required to secure a wireless network.

Understand cryptology, cryptography, cryptanalysis, steganography, plaintext, cipher, and ciphertext. Know the definition of each of these security terms, how they relate to each other, and the differences between them.

Know the history of 802.11 security. Know the history of wireless security and the differences between the different IEEE standards and Wi-Fi Alliance certifications.

Key Terms

802.1X

access

accounting

Advanced Encryption Standard (AES)

authentication

Authentication, authorization, and accounting (AAA)

authorization

autonomous access points

cipher

ciphertext

core

Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)

cryptanalysis

cryptography
cryptology
data privacy
Data-Link layer
decryption
distribution
encryption
Extensible Authentication Protocol (EAP)
fast basic service set transition (FT)
fast secure roaming
Federal Information Processing Standards (FIPS)
International Organization for Standardization (ISO)
key
lightweight access points
Logical Link Control (LLC)
Media Access Control (MAC) sublayer
Open System authentication
plaintext
preshared keys (PSKs)
robust security network (RSN)
robust security network associations (RSNAs)
Shared Key authentication
steganography
Temporal Key Integrity Protocol (TKIP)
transition security network (TSN)
Wi-Fi Protected Access (WPA)
Wi-Fi Protected Access 2 (WPA2)
Wi-Fi Protected Setup (WPS)
Wired Equivalent Privacy (WEP)
WLAN controller

Review Questions

1. The IEEE 802.11-2007 standard mandates _____ encryption for robust security network associations and the optional use of _____ encryption.
   - **A.** WEP, AES
   - **B.** IPsec, AES
   - **C.** MPPE, TKIP
   - **D.** TKIP, WEP
   - **E.** CCMP, TKIP

2. What wireless security solutions are defined by Wi-Fi Protected Access? (Choose all that apply.)
   - **A.** Passphrase authentication
   - **B.** LEAP
   - **C.** TKIP/RC4
   - **D.** Dynamic WEP
   - **E.** CCMP/AES

3. Which wireless security standards and certifications call for the use of CCMP/AES encryption? (Choose all that apply.)
   - **A.** WPA
   - **B.** 802.11-2007
   - **C.** 802.1X
   - **D.** WPA2
   - **E.** 802.11 legacy

4. A robust security network (RSN) requires the use of which security mechanisms? (Choose all that apply.)
   - **A.** 802.11x
   - **B.** WEP
   - **C.** IPSec
   - **D.** CCMP/AES
   - **E.** CKIP
   - **F.** 802.1X

5. The Wi-Fi Alliance is responsible for which of the following certification programs? (Choose all that apply.)
   - **A.** WPA2
   - **B.** WEP
   - **C.** 802.11-2007
   - **D.** WMM
   - **E.** PSK

6. Which sublayer of the OSI model's Data-Link layer is used for communication between 802.11 radios?
   - **A.** LLC
   - **B.** WPA
   - **C.** MAC
   - **D.** FSK

7. What encryption methods are defined by the IEEE 802.11-2007 standard? (Choose all that apply.)
   - **A.** 3DES
   - **B.** WPA-2
   - **C.** SSL
   - **D.** TKIP
   - **E.** CCMP
   - **F.** WEP

8. Which organization is responsible for the creation of documents known as Requests for Comments?
   - **A.** IEEE
   - **B.** ISO
   - **C.** IETF
   - **D.** Wi-Fi Alliance
   - **E.** RFC Consortium

9. Which of the following is not a standard or amendment created by the IEEE? (Choose all that apply.)
   - **A.** 802.11X
   - **B.** 802.1x
   - **C.** 802.3af
   - **D.** 802.11N
   - **E.** 802.11g

10. TKIP can be used with which of the following? (Choose all that apply.)

- **A.** WEP
- **B.** WPA-Personal
- **C.** WPA-Enterprise
- **D.** WPA-2 Personal
- **E.** WPA-2 Enterprise
- **F.** 802.11-2007 (RSN)

11. Which of the following is simply a way of representing information in a different way?

- **A.** Cryptography
- **B.** Steganography
- **C.** Encryption
- **D.** Cipher
- **E.** Code

12. What wireless security components are mandatory under WPA version 2? (Choose all that apply.)

- **A.** 802.1X/EAP
- **B.** PEAP
- **C.** TKIP/RC4
- **D.** Dynamic WEP
- **E.** CCMP/AES

13. The 802.11i ratified security amendment can now be found in which clause of the 802.11-2007 standard?

- **A.** Clause 8
- **B.** Clause 14
- **C.** Clause 15
- **D.** Clause 17
- **E.** Clause 33

14. The science of concealing plaintext and then revealing it is known as _____, and the science of decrypting the ciphertext without knowledge of the key or cipher is known as _____.

- **A.** encryption, decryption
- **B.** cryptanalysis, cryptology
- **C.** cryptology, cryptanalysis
- **D.** cryptography, cryptanalysis
- **E.** cryptography, steganography

15. What is the chronological order in which the following security standards and certifications were defined?

1. 802.11-2007

2. 802.11i

3. WEP

4. WPA-2

5. WPA

A. 3, 5, 2, 4, 1

B. 3, 2, 5, 4, 1

C. 3, 5, 2, 1, 4

D. 1, 3, 2, 5, 4

E. 1, 3, 5, 4, 2

16. The 802.11 legacy standard defines which wireless security solution?

A. Dynamic WEP

B. 802.1X/EAP

C. 64-bit static WEP

D. Temporal Key Integrity Protocol

E. CCMP/AES

17. These qualifications for interoperability are usually based on key components and functions that are defined in the IEEE 802.11-2007 standard and various 802.11 amendments.

A. Request for comments

B. Wi-Fi Alliance

C. Federal Information Processing Standards

D. Internet Engineering Task Force

E. Wi-Fi CERTIFIED

18. Which of the following can be used with a wireless network to segment or restrict access to parts of the network? (Choose all that apply.)

A. VLANs

B. WPA-2

C. Firewall

D. 802.11i

E. RBAC

19. 802.1X/EAP is mandatory in which of the following? (Choose all that apply.)

- **A.** WPA SOHO
- **B.** WPA Enterprise
- **C.** WPA-2 SOHO
- **D.** WPA-2 Enterprise
- **E.** WPA2-PSK

20. The objective of delivering management frames in a secure manner is defined by which 802.11 amendment?

- **A.** 802.11r-2008
- **B.** 802.11w-2009
- **C.** 802.11n-2009
- **D.** 802.11x-2009
- **E.** 802.11k-2008

Answers to Review Questions

1. E. The 802.11-2007 standard defines what is known as a robust security network (RSN) and robust security network associations (RSNAs). CCMP/AES encryption is the mandated encryption method, while TKIP/RC4 is an optional encryption method.

2. A, C. The Wi-Fi Protected Access (WPA) certification was a snapshot of the not-yet-released 802.11i amendment, supporting only the TKIP/RC4 dynamic encryption-key generation. 802.1X/EAP authentication was required in the enterprise, and passphrase authentication was required in a SOHO or home environment. LEAP is Cisco-proprietary and is not specifically defined by WPA. Neither dynamic WEP nor CCMP/AES were defined for encryption. CCMP/AES dynamic encryption is mandatory under the WPA2 certification.

3. B, D. The 802.11-2007 standard defines CCMP/AES encryption as the default encryption method, while TKIP/RC4 is the optional encryption method. This was originally defined by the 802.11i amendment, which is now part of the 802.11-2007 standard. The Wi-Fi Alliance created the WPA2 security certification, which mirrors the robust security defined by the IEEE. WPA2 supports both CCMP/AES and TKIP/RC4 dynamic encryption-key management.

4. D, F. The required encryption method defined by an RSN wireless network is Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), which uses the Advanced Encryption Standard (AES) algorithm. An optional choice of encryption is the Temporal Key Integrity Protocol (TKIP). The 802.11-2007 standard also requires the use of an 802.1X/EAP authentication solution or the use of preshared keys for robust security.

5. A, D. 802.11-2007 is the IEEE standard, and WEP (Wired Equivalent Privacy) is defined as part of the IEEE 802.11-2007 standard. PSK is not a standard; it is an encoding technique. Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance certification program that enables Wi-Fi networks to prioritize traffic generated by different applications. WPA2 is a certification program that defines Wi-Fi security mechanisms.

6. C. The IEEE 802.11-2007 standard defines communication mechanisms at only the Physical layer and MAC sublayer of the Data-Link layer of the OSI model. The Logical Link Control (LLC) sublayer of the Data-Link layer is not defined by the 802.11-2007 standard. WPA is a security certification. FSK is a modulation method.

7. D, E, F. WPA-2 is a Wi-Fi Alliance certification and not an encryption method. The WPA-2 certification does mandate the use of CCMP encryption and TKIP is optional. The IEEE 802.11-2007 standard defines the use of both CCMP and TKIP dynamic encryption methods. Also defined by the IEEE is the use of static WEP encryption.

8. C. Requests for Comments are known as RFCs and are created by the Internet Engineering Task Force (IETF), which is guided and directed by the Internet Engineering Steering Group (IESG).

9. A, B, D. There is no 802.11X amendment. 802.1x should be capitalized (802.1X), and 802.11N should not be capitalized (802.11n). These are not trivial errors. Standards and amendments should be written and used with the proper capitalization.

10. B, C, D, E, F. By default, WPA-Personal and WPA-Enterprise use TKIP for encryption. WPA-2 Personal, WPA-2 Enterprise, and 802.11-2007 (RSN) mandate the use of CCMP, but TKIP is optional.

11. E. A code is simply a way of representing information in a different way, such as ASCII or Morse code.

12. A, E. Wi-Fi Protected Access (WPA) version 2 mirrors the 802.11i security amendment, mandating CCMP/AES dynamic encryption key management. TKIP/RC4 dynamic encryption key management is optional. 802.1X/EAP authentication is required in the enterprise and passphrase authentication in a SOHO environment. PEAP can be used for 802.1X/EAP authentication, but is not specifically defined by WPA. Dynamic WEP is not defined for encryption.

13. A. Clause 8 defines security. Clause 14 defines frequency-hopping spread spectrum (FHSS) PHY. Clause 15 defines direct sequence spread spectrum (DSSS) PHY. Clause 17 defines orthogonal frequency division multiplexing (OFDM) PHY. Clause 33 hasn't been defined yet in 802.11, but in 802.3 it defines Power over Ethernet (PoE).

14. D. Cryptography is the science of concealing the plaintext and then revealing it. Cryptanalysis is the science of decrypting the ciphertext without knowledge of the key or cipher. Cryptology is the practice or science that includes the techniques to encrypt and decrypt information. Steganography strives to hide the fact that there is a message by concealing it.

15. A. WEP was defined in the original 802.11 standard. WPA was considered a partial preview of the 802.11i amendment. WPA-2 was defined as somewhat of a mirror of 802.11i. 802.11i and seven other amendments were incorporated into the revised 802.11-2007 standard.

16. C. The original 802.11 standard ratified in 1997 defined the use of a 64-bit or 128-bit static encryption solution called Wired Equivalent Privacy (WEP). Dynamic WEP was never defined under any wireless security standard. The use of 802.1X/EAP, TKIP/RC4, and CCMP/AES are all defined under the current 802.11-2007 standard.

17. E. The IEEE 802.11 task group defines the WLAN standards, and the Wi-Fi Alliance defines interoperability certification programs.

18. A, C, E. WPA-2 and 802.11i are used to allow or deny access to the network, but not to limit access to parts of it. VLANs, firewalls, and role-based access control (RBAC) can all limit or restrict access to parts or segments of the network.

19. B, D. When a wireless network is implemented in an enterprise environment, the use of 802.1X/EAP is mandatory. When used in a SOHO environment, preshared keys are used.

20. B. The 802.11w-2009 amendment defines the delivery of some 802.11 management frames in a secure manner. This will hopefully prevent some (but not all) of the Layer 2 DoS attacks that currently exist.

Chapter 2

Legacy 802.11 Security

IN THIS CHAPTER, YOU WILL LEARN ABOUT THE FOLLOWING:

- ✓ **Authentication**
  - Open System Authentication
  - Shared Key Authentication
- ✓ **Wired Equivalent Privacy (WEP) Encryption**
- ✓ **Virtual Private Networks (VPNs)**
  - Point-to-Point Tunneling Protocol (PPTP)
  - Layer 2 Tunneling Protocol (L2TP)
  - Internet Protocol Security (IPsec)
  - Configuration Complexity
  - Scalability
- ✓ **MAC Filters**
- ✓ **SSID Segmentation**
- ✓ **SSID Cloaking**

There have been many changes to the security mechanisms of the 802.11 standard since its ratification in 1997. There are three pre-RSNA or legacy security mechanisms: Open System authentication, Shared Key authentication, and WEP encryption. These pre-RSNA security mechanisms are currently defined in clause 8.2 of the 802.11-2007 standard. It should be noted that the current 802.11-2007 standard also defines the more current *robust security network (RSN)* operations that are meant to replace legacy 802.11 security. Even though these legacy security mechanisms have been superseded and should be avoided, they are still integrated into most, if not all 802.11 devices to provide backward compatibility with existing equipment. It is important to understand these security methods and to understand why Open System authentication is still valid and why Shared Key authentication and WEP encryption should be avoided.

If this chapter was strictly about legacy 802.11 security as defined by the standard, then it would be a very short chapter indeed, since Open System authentication, Shared Key authentication, and WEP encryption are the only legacy security methods originally defined by the IEEE. So why is it there is more to this chapter than just that? Well, two types of standards exist in the world of technology; *de jure* standards and *de facto* standards. Essentially de jure (Latin for "concerning law") standards are typically defined and ratified by a standards body, such as the IEEE, whereas de facto (Latin for "concerning fact") standards are established by practice or usage.

Over the years, different nonstandard security solutions have been implemented to enhance the wireless network security, or make up for shortcomings in the standard. Some of these, such as VPN over wireless, provided solutions to overcome flaws that arose in the standard. Others, such as MAC filtering, SSID segmentation, and SSID cloaking, provided enhancements or additional capabilities that were not in the standard. Although all of these may still have their place in some environments, for the most part they should be avoided as the newer security mechanisms are capable of providing a faster and more secure wireless network.

Authentication

Authentication is the first of two steps required to connect to the 802.11 basic service set. Both authentication and association must occur, in that order, before an 802.11 client can pass traffic through the access point to another device on the network. Authentication is

a process that is often misunderstood. When many people hear authentication, they think of what is commonly referred to as network authentication, entering a username and password in order to get access to the network. In this chapter, we are referring to 802.11 authentication that occurs at Layer 2 of the OSI model. When an 802.3 device needs to communicate with other devices, the first step is to plug the Ethernet cable into a wall jack. When this cable is plugged in, the client creates a physical link to the wired switch and is now able to start transmitting frames. When an 802.11 device needs to communicate, it must first authenticate with the access point. This authentication is not much more of a task than plugging the Ethernet cable into the wall jack. The 802.11 authentication merely establishes an initial connection between the client and the access point. The 802.11-2007 standard specifies two different methods of authentication: Open System authentication and Shared Key authentication.

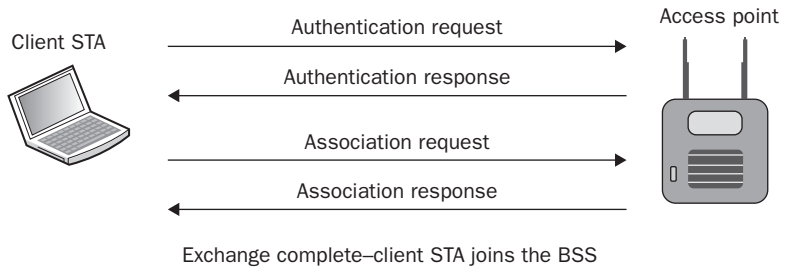
Open System Authentication

Open System authentication is the only pre-RSNA security mechanism that has not been deprecated. Open System authentication is the simpler of the two authentication methods. It provides authentication without performing any type of client verification. It is essentially an exchange of hellos between the client and the access point. It is considered a null authentication because there is no exchange or verification of identity between the devices. It is assumed that the devices already have all of the appropriate information to authenticate to the network. In other words, every station (STA) is validated during Open System authentication.

Within a basic service set (BSS), Open System authentication occurs with an exchange of frames between the client station and the access point station. Open System authentication utilizes a two-message authentication transaction sequence. The first message asserts identity and requests authentication. The second message returns the authentication result. If the result is "successful," the STAs will be declared mutually authenticated. Open System authentication is also used by STAs in an independent basic service set (IBSS), which is more commonly known as an ad hoc WLAN.

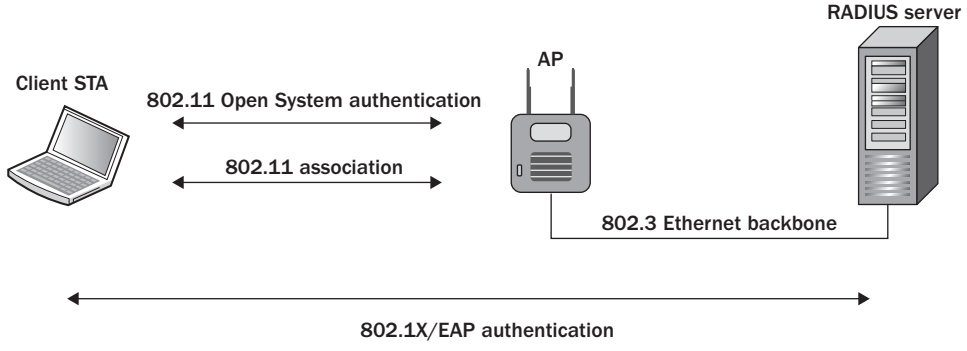
Open System authentication occurs after a client STA knows about the existence of an access point (AP) by either passive or active scanning. The client STA can passively find out about the parameters of the BSS from the AP's beacon management frame or extract the same information during the active probing process from the AP's probe response frame. An Open System authentication frame exchange process then begins with the goal of eventually joining the BSS. As shown in Figure 2.1, the client STA must first become authenticated before exchanging two more association frames. Once Open System authentication and association occurs, the client STA establishes a Layer 2 connection to the AP and is a member of the BSS.

FIGURE 2.1 Open System authentication



WEP encryption is optional with Open System authentication. For data privacy, Wired Equivalent Privacy (WEP) encryption can be used with Open System authentication, but WEP is used only to encrypt the Layers 3–7 MAC Service Data Unit (MSDU) payload of 802.11 data frames and only after the client station is authenticated and associated. In other words, WEP is not used as part of the Open System authentication process, but WEP encryption can be used to provide data privacy after authentication and association occur. So, if Open System authentication is so simple and basic—providing no verification of identity—then why is it still used when security is so important? The answer to this question is simple. It doesn't need to be secure, because other more advanced overlay security authentication methods such as 802.1X/EAP are now being implemented. As you can see in Figure 2.2, Open System authentication and association between the client STA and AP still occurs prior to the 802.1X/EAP authentication exchange between the client STA and a RADIUS server. In Exercise 2.1, you will look at a packet capture containing Open System authentication frames.

FIGURE 2.2 Open System and 802.1X/EAP authentication



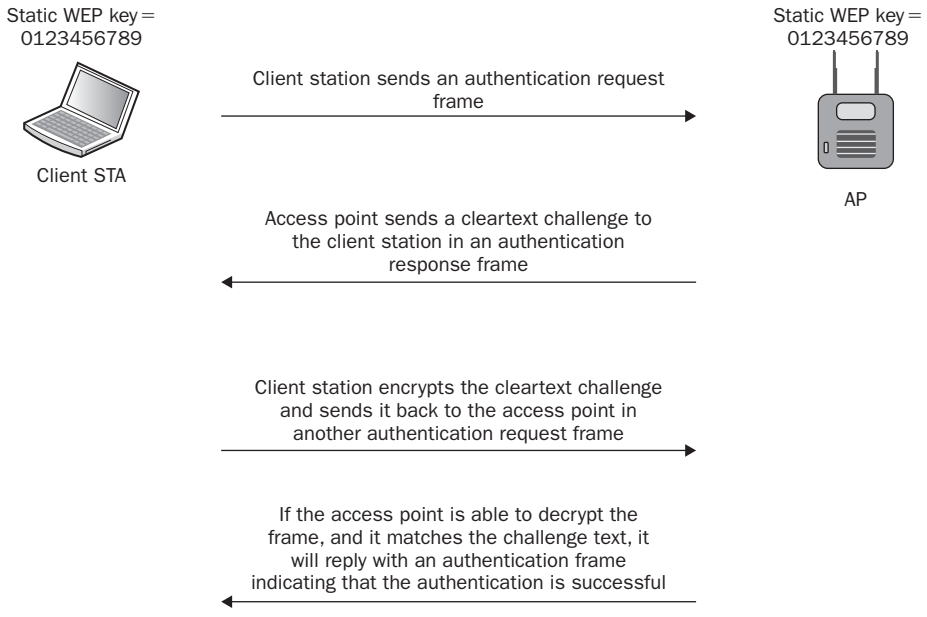
The 802.11-2007 standard now defines more advanced authentication methods. A detailed discussion about 802.1X/EAP can be found in Chapter 4, "Enterprise 802.11 Layer 2 Authentication Methods."

Shared Key Authentication

Shared Key authentication uses WEP to authenticate client stations and requires that a static WEP key be configured on both the client STA and the access point. In addition to WEP being mandatory, authentication will not work if the static WEP keys do not match. The authentication process is similar to Open System authentication but includes a challenge and response between the AP station and client station within the BSS. Shared Key authentication can also be used between two STAs in an IBSS.

Shared Key authentication is a four-way authentication frame exchange, as shown in Figure 2.3. The client station sends an authentication request to the AP, and the AP sends a cleartext challenge to the client station in an authentication response. The client station then encrypts the cleartext challenge and sends it back to the AP in the body of another authentication request frame. The AP decrypts the station's response and compares it to the challenge text. If they match, the AP will respond by sending a fourth and final authentication frame to the station, confirming successful authentication. If they do not match, the AP will respond negatively. If the AP cannot decrypt the challenge, it will also respond negatively. If Shared Key authentication is successful, the same static WEP key that was used during the Shared Key authentication process will also be used to encrypt the 802.11 data frames.

FIGURE 2.3 Shared Key authentication exchange



Although it might seem that Shared Key authentication is a more secure solution than Open System authentication, in reality Shared Key could be the bigger security risk. Anyone who captures the cleartext challenge phrase and then captures the encrypted challenge phrase in the response frame could potentially derive the static WEP key. If the static WEP key is compromised, a whole new can of worms has been opened because now all the data frames can be decrypted.

Do not confuse the Shared Key authentication with Preshared Key (PSK) authentication. Shared Key authentication is a legacy method defined as a pre-RSNA security method. The 802.11-2007 standard defines robust security that requires either 802.1X/EAP authentication or PSK authentication. PSK authentication methods are discussed in greater detail in Chapters 5 and 6.

In Exercise 2.1, you will look at packet captures containing encrypted and decrypted Shared Key authentication frames. Since it is our own network, and we know the WEP key, we can look at the decrypted authentication frames.

Which Legacy Authentication Method is Better?

On the surface, Shared Key authentication may appear to be the more secure solution because the static WEP key is also being used for credentials during the authentication process. Open System authentication, on the other hand, does not require credentials. However, if the static WEP key is compromised from the Shared Key authentication process, all 802.11 data frames encrypted with that same static WEP key are at risk. In reality, static WEP encryption should never be used because WEP can easily be cracked using hacker tools such as Aircrack-ng. Much better dynamic encryption methods such as CCMP-AES are widely available. However, if WEP is the only encryption option available, using simple Open System authentication together with WEP encryption instead of Shared Key authentication is probably the better choice. Also be aware that it is common for end-users to change the configuration settings on a client station from Open System to Shared Key, especially when they are having trouble configuring their wireless client software utility. Improperly configured legacy authentication settings are something to watch for when troubleshooting client problems

EXERCISE 2.1

Viewing Open System and Shared Key Authentication Frames

In this exercise, you will use a protocol analyzer to view the 802.11 frame exchanges used to authenticate a client to the access point. The following directions should assist you with the installation and use of WildPackets' OmniPeek protocol analyzer demo software. If you have already installed OmniPeek, you can skip steps 1–5.

1. In your web browser, go to the following URL: `www.wildpackets.com/support/downloads`.
2. Under Product Evals, choose OmniPeek Professional. Fill out the OmniPeek evaluation request. A WildPackets representative will send an email message with a private download URL.
3. Proceed to the private download URL. Download the OmniPeek Professional demo software to your desktop using FTP. This evaluation copy of OmniPeek will be licensed to work for 30 days. Write down the evaluation license serial number.
4. Double-click the installation file `omnp602.exe`, and follow the installation prompts. You will need to be connected to the Internet to activate the license. You will be asked to enter the evaluation copy serial number.
5. The exercise will use frame captures that are on the CD that came with this book. If you would like to use OmniPeek for live captures, install the proper drivers for your Wi-Fi radio card. Verify that you have a supported Wi-Fi card. Review the system requirements and supported operating systems. OmniPeek requires you to install the proper drivers for the supported Wi-Fi cards. Information about the drivers can be found at `www.wildpackets.com/support/downloads/drivers`.
6. In Windows, choose Start ➢ Programs ➢ Wildpackets OmniPeek and then click the OmniPeek icon. The OmniPeek application should appear.
7. Click the Open Capture File icon and browse the book's CD. Open the packet capture file called `OPEN_SYSTEM_AUTHENTICATION.PCAP`.
8. When you double-click on packet 1, OmniPeek will open the packet in a new tabbed window. Scroll down to the 802.11 Management-Authentication section, and you will see the Auth Algorithm is Open System and the Auth Seq Num is 1. This indicates that it is an Open System authentication request frame.
9. If you click the OPEN_SYSTEM-AUTHENTICATION.PCAP tab, you can then double-click on packet 3 and another tab will be created. Scroll down to the 802.11 Management-Authentication section, and you will see the Auth Algorithm is Open System and the Auth Seq Num is 2. This indicates that it is an Open System authentication reply frame. You can also see that the Status Code indicates that the authentication was successful.

EXERCISE 2.1 *(continued)*

10. Close all of the tabs except for the Start Page. Click the Open Capture File icon and browse the book's CD. Open the packet capture file called SHARED_KEY_AUTHENTICATION_ENCRYPTED.PCAP.
11. The two packets of most interest are packets 3 and 5. In packet 3, the access point is responding to the authentication request and including the challenge text unencrypted. Scroll down to the 802.11 Management-Authentication section, and you will see the challenge text.
12. If you click the SHARED_KEY_AUTHENTICATION_ENCRYPTED.PCAP tab, you can then double-click on packet 5 and another tab will be created. This frame is the response from the client to the access point. The client has taken the challenge text and encrypted it. Scroll down to the section WEP Data, and you will see 136 bytes of encrypted data.
13. Close all of the tabs except for the Start Page. Click the Open Capture File icon, and browse the book's CD. Open the packet capture file called SHARED_KEY_AUTHENTICATION_DECRYPTED.PCAP.
14. This file is a decrypted version of the file at which you were just looking. Repeat steps 11 and 12 using the decrypted file.
15. If you are interested in decrypting the file yourself, open the encrypted file; then, from the Tools menu, select Decrypt WLAN Packets. You will need to create a key set by clicking on the box with the three dots in it. The encryption key that was used in this exercise was a 64-bit WEP key entered as a hexadecimal (hex) value of 0102030405.

Wired Equivalent Privacy (WEP) Encryption

Wired Equivalent Privacy (WEP) is a Layer 2 encryption method that uses the ARC4 streaming cipher. Because WEP encryption occurs at Layer 2, the information that is being protected is the upper layers of 3–7. The payload of an 802.11 data frame is called the *MAC Service Data Unit (MSDU)*. The MSDU contains data from the LLC and Layers 3–7. A simple definition of the MSDU is that it is the data payload that contains the IP packet plus some LLC data. WEP and other Layer 2 encryption methods encrypt the MSDU payload of an 802.11 data frame. The original 802.11 standard defined both 64-bit WEP and 128-bit WEP as supported encryption methods. The three main intended goals of WEP encryption include confidentiality, access control, and data integrity. The primary goal of confidentiality was to provide data privacy by encrypting the data before transmission.

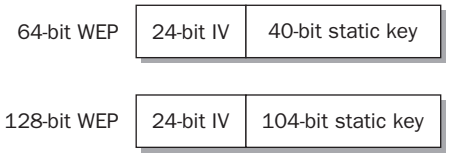
WEP also provides access control, which is basically a crude form of authorization. Client stations that do not have the same matching static WEP key as an access point are refused access to network resources. A data integrity checksum, known as the Integrity Check Value (ICV), is computed on data before encryption and used to prevent data from being modified. The current 802.11-2007 standard still defines WEP as a legacy encryption method for pre-RSNA security.

If You Thought WEP Used RC4 Encryption, You are Right and Wrong!

RC4 is also known as ARC4 or ARCFOUR. ARC4 is short for Alleged RC4. RC4 was created in 1987 by Ron Rivest of RSA Security. It is known as either "Rivest Cipher 4" or "Ron's Code 4." RC4 was initially a trade secret; however, in 1994, a description of it was leaked onto the Internet. Comparison testing confirmed that the leaked code was genuine. RSA has never officially released the algorithm, and the name "RC4" is trademarked, thus the reference to it as ARCFOUR or ARC4.

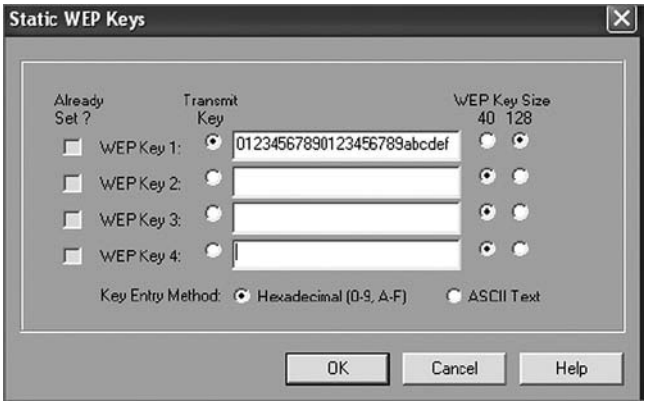
Although both 64-bit and 128-bit WEP were defined in 1997 in the original IEEE 802.11 standard, the U.S. government initially allowed the export of only 64-bit technology. After the U.S. government loosened export restrictions on key size, radio card manufacturers began to produce equipment that supported 128-bit WEP encryption. The 802.11-2007 standard refers to the 64-bit version as WEP-40 and the 128-bit version as WEP-104. As shown in Figure 2.4, 64-bit WEP uses a secret 40-bit static key, which is combined with a 24-bit number selected by the card's device drivers. This 24-bit number, known as the *Initialization Vector (IV)*, is sent in cleartext and a new IV is created for every frame. Although the IV is said to be new for every frame, there are only 16,777,216 different IV combinations; therefore, you are forced to reuse the IV values. The standard also does not define what algorithm to use to create the IV. The effective key strength of combining the IV with the 40-bit static key is 64-bit encryption. 128-bit WEP encryption uses a 104-bit secret static key that is also combined with a 24-bit IV.

FIGURE 2.4 Static WEP encryption key and initialization vector



A static WEP key can usually be entered as hex characters (0–9 and A–F) or ASCII characters. The static key must match on both the access point and the client device. A 40-bit static key consists of 10 hex characters or 5 ASCII characters, while a 104-bit static key consists of 26 hex characters or 13 ASCII characters. Not all client stations or access points support both hex and ASCII. Most clients and access points support the use of up to four separate static WEP keys from which a user can choose one as the default transmission key (Figure 2.5 shows an example of one such client).

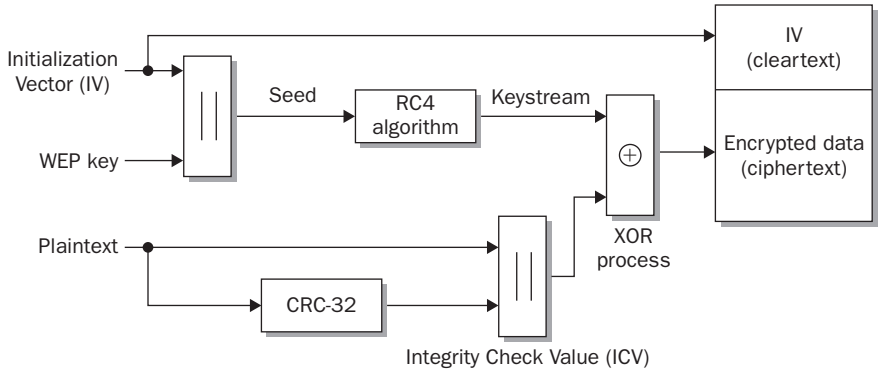
FIGURE 2.5 WEP transmission key



The transmission key is the static key that is used to encrypt data by the transmitting radio. A client or access point may use one key to encrypt outbound traffic and a different key to decrypt received traffic. However, each key used must match exactly on both sides of a link for encryption/decryption to work properly. When a device creates a WEP encrypted frame, a key identifier is added to the IV field indicating which of the four possible static keys was used to encrypt the data and which key will be used to decrypt the data. As an example, if a transmitting device uses key 3 to encrypt the data, the receiving device will use key 3 to decrypt the data. If the receiving device does not have key 3 defined, or does not have the same WEP key entered in key 3, the data will not be decrypted.

How does WEP work? WEP runs a *cyclic redundancy check (CRC)* on the plaintext data that is to be encrypted and then appends the *Integrity Check Value (ICV)* to the end of the plaintext data. The ICV is used for data integrity and should not be confused with the initialization vector (IV). A 24-bit cleartext IV is generated and combined with the static secret key. WEP then uses both the static key and the IV as seeding material through a pseudorandom algorithm that generates random bits of data known as a *keystream*. These pseudorandom bits are equal in length to the plaintext data that is to be encrypted. The pseudorandom bits in the keystream are then combined with the plaintext data bits by using a Boolean XOR process. The end result is the WEP *ciphertext*, which is the encrypted data. The encrypted data is then prefixed with the cleartext IV. Figure 2.6 illustrates this process.

FIGURE 2.6 WEP encryption process



To decrypt a frame, WEP first extracts the IV and the key identifier, recognizing which key to use. WEP then uses the static key and the IV as seeding material through the pseudorandom algorithm to generate the keystream. The keystream is combined with the ciphertext using a Boolean XOR process. The end result is the decryption of the ciphertext and the creation of the plaintext data. WEP runs a CRC on the plaintext data and compares it to the decrypted ICV from the ciphertext. If the two are bit-wise identical, the frame is considered valid.

Unfortunately, WEP has quite a few weaknesses, which is why it has been deprecated. Its weaknesses include the following four main attacks:

IV Collisions Attack Because the 24-bit Initialization Vector is in cleartext and a new IV is generated for every frame, all 16 million IVs will eventually be used and will be forced to repeat themselves in a busy WEP-encrypted network. Because of the limited size of the IV space, IV collisions occur and an attacker can recover the secret key much easier when IV collisions occur in wireless networks.

Weak Key Attack Because of the ARC4 key-scheduling algorithm, weak IV keys are generated. An attacker can recover the secret key much easier by recovering the known weak IV keys.

Reinjection Attack Hacker tools exist that implement a packet reinjection attack to accelerate the collection of weak IVs on a network with little traffic.

Bit-Flipping Attack The ICV data integrity check is considered weak. WEP encrypted packets can be tampered with.

Current WEP cracking tools may use a combination of the first three mentioned attacks and can crack WEP in less than 5 minutes. After an attacker has compromised the static WEP key, any data frame can be decrypted with the newly discovered key. As defined by

the 802.11-2007 standard, WEP encryption is considered a legacy pre-RSNA security method. Although WEP encryption has indeed been cracked and is viewed as unacceptable in the enterprise, it is still better than using no encryption at all. If legacy WEP is the only encryption solution available, it should be deployed. Many legacy devices that only support static WEP are still deployed in enterprise environments.

Are all WEP Keys Static?

As defined by the 802.11-2007 standard, WEP uses either a 40-bit static key or a 104-bit static key. These keys are combined with a 24-bit IV to bring the effective key strength to 64-bit and 128-bit. Before the Wi-Fi Alliance created the Wi-Fi Protected Access (WPA) security certification, various WLAN vendors offered a dynamic key generation security solution using WEP encryption. Dynamic WEP was never defined as any part of the 802.11 security and was intended only as a stop-gap dynamic encryption solution until the stronger encryption methods of TKIP/RC4 or CCMP/AES became available. Dynamic WEP is discussed in Chapter 5, "802.11 Dynamic Encryption Key Generation.

EXERCISE 2.2

Viewing Encrypted MSDU Payload of 802.11 Data Frames

In this exercise, you will use a protocol analyzer to view an FTP file transfer of a text file. You will look at the MAC Service Data Unit (MSDU) payload of 802.11 data frames. The following directions should assist you with the installation and use of WildPackets' OmniPeek protocol analyzer demo software. If you have already installed OmniPeek, you can skip steps 1–5.

1. In your web browser, go to the following URL: `www.wildpackets.com/support/downloads`.
2. Under Product Evals, choose OmniPeek Professional. Fill out the OmniPeek evaluation request. A WildPackets representative will send an email message with a private download URL.
3. Proceed to the private download URL. Download the OmniPeek Professional demo software to your desktop using FTP. This evaluation copy of OmniPeek will be licensed to work for 30 days. Write down the evaluation license serial number.
4. Double-click the installation file `omnp602.exe`, and follow the installation prompts. You will need to be connected to the Internet to activate the license. You will be asked to enter the evaluation serial number.
5. The exercise will use frame captures that are on the CD that came with this book. If you would like to use OmniPeek for live captures, you must install the proper drivers for your Wi-Fi radio card. Verify that you have a supported Wi-Fi card. Review the system

requirements and supported operating systems. OmniPeek requires you to install the proper drivers for the supported Wi-Fi cards. Information about the drivers can be found at www.wildpackets.com/support/downloads/drivers.

6. In Windows, choose Start ➢ Programs ➢ Wildpackets OmniPeek, and then click the OmniPeek icon. The OmniPeek application should appear.
7. Click the Open Capture File icon and browse the book's CD. Open the packet capture file called NON_ENCRYPTED_MSDU.PCAP. You will now view an MSDU payload of an 802.11 data frame that is not encrypted.
8. Double-click on packet #16, and OmniPeek will open the packet in a new tabbed window. Scroll down to the TCP section of the frame. Notice that the source port is 20 and the application is FTP. Look at the hex view of the frame at the bottom of the window. Notice that you can read the text file. The cleartext data is not encrypted and reads, "These are the times that try men's souls."
9. Click the Open Capture File icon, and browse the book's CD. Open the packet capture file called ENCRYPTED_MSDU.PCAP. You will now view an MSDU payload of an 802.11 data frame that is encrypted.
10. Double-click on packet #15; OmniPeek will open the packet in a new tabbed window. Scroll down to the WEP Data section. Notice the 636 bytes of encrypted data. All the 3–7 information of the MSDU is now encrypted and cannot be seen. Notice that the Initialization Vector (IV) and Integrity Check Value (ICV) can be seen.
11. If you are interested in decrypting the file, open the encrypted file, and then from the Tools menu, select Decrypt WLAN Packets. You will need to create a key set by clicking on the box with the three dots in it. The encryption key that was used in this exercise was a 64-bit WEP key entered as a hex value of 5555555555.

Virtual Private Networks (VPNs)

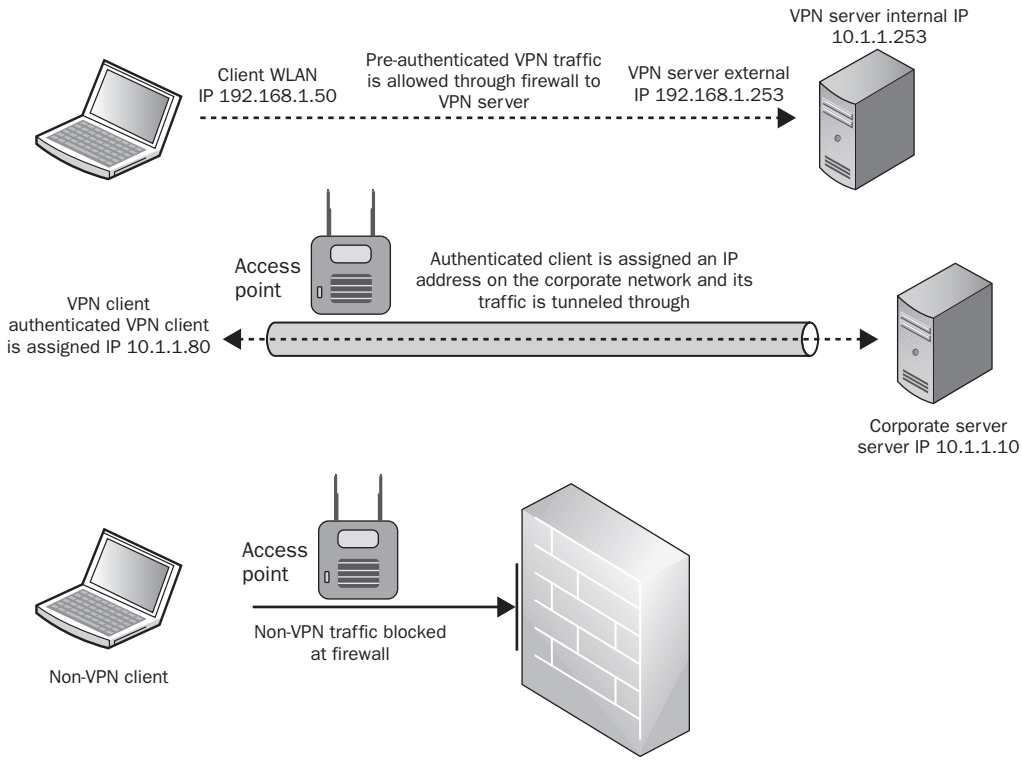
Although the 802.11-2007 standard clearly defines Layer 2 security solutions, the use of upper-layer *virtual private network (VPN)* solutions can also be deployed with WLANs. VPNs are typically no longer recommended to provide security for client access in the enterprise due to the extra overhead from VPN encryption and the sometimes complex configuration. Furthermore, because faster, more secure Layer 2 solutions are now available for securing WLAN client access, use of Layer 3 VPNs for client WLAN client access is outdated.

VPNs still have their place in Wi-Fi security and should definitely be used for remote access. They are also often used in wireless bridging environments and for branch office connectivity. Use of VPN technology is mandatory for remote access. Your end users will take their laptops off site and will most likely use public access Wi-Fi hot spots. Since there is no security at most hot spots, a VPN solution is a necessity. The VPN user will need to bring the security to the hot spot in order to provide a secure connection. It is imperative that users implement a VPN solution coupled with a personal firewall whenever accessing any public access Wi-Fi networks.

The two major types of VPN topologies are router-to-router or client/server based. Router-to-router VPNs are used to protect communications between two separate networks. Client/server VPNs are used to protect client communication to and from a network. VPNs have several major characteristics. They provide encryption, encapsulation, authentication, and data integrity. A simple definition of a Layer 3 VPN is that it is a router that also provides data privacy with encryption. VPNs use secure tunneling, which is the process of encapsulating one IP packet within another IP packet. The first packet is encapsulated inside the outer packet. The original destination and source IP address of the first packet is encrypted along with the data payload of the first packet. VPN tunneling therefore protects your original Layer 3 addresses and also protects the data payload of the original packet. Layer 3 VPNs use Layer 3 encryption; therefore, the payload that is being encrypted is the Layer 4 to 7 information. The IP addresses of the second packet are seen in cleartext and are used for communications between the tunnel end points. The destination and source IP addresses of the outer second packet will point to the virtual IP address of the VPN server and VPN client software.

Although no longer a recommended practice, VPNs were often used for WLAN security for client access because a VPN server was already deployed within the wired infrastructure. Since the VPN server already existed, the company only needed to install the WLAN on a network with a firewall between the WLAN and the corporate network. As mentioned earlier, a Layer 3 VPN has both routing and encryption capabilities. The encryption component of the VPN is used to provide data privacy. The Layers 4–7 payload of an 802.11 data frame will be encrypted across the wireless and wired medium. The VPN client software on the WLAN client station encrypts and decrypts at one end of the tunnel and the VPN server encrypts and decrypts at the other end of the tunnel. A firewall sits between the WLAN client and the VPN server. As shown in Figure 2.7, the firewall is configured to allow only VPN traffic to pass through the firewall. Once the VPN traffic passes through the firewall, the VPN server terminates it. If the traffic is a VPN client attempting to connect, and if the client credentials are valid, the client will be authenticated and assigned an IP address on the internal network. A VPN tunnel is created between the client and the VPN server. When the VPN tunnel passes through the firewall, the tunnel terminates at the VPN server, and the traffic is decrypted and routed to network resources. The VPN provides data privacy and the firewall is used together with the VPN to segment the WLAN from network resources.

FIGURE 2.7 VPN and WLAN client access security



The three major protocols used in Layer 3 VPN technologies are *Point-to-Point Tunneling Protocol (PPTP)*, *Internet Protocol Security (IPsec)*, and *Layer 2 Tunneling Protocol (L2TP)*. Unlike 802.1X/EAP solutions, an IP address is needed before a VPN tunnel can be established. A downside to using a VPN solution is that access points are potentially open to attack because a potential attacker can get both a Layer 2 and a Layer 3 connection before the VPN tunnel is established. WEP, which encrypts at Layer 2, was often used together with VPN security to protect the Layer 3 information. The problem with this strategy is that a double-encryption solution was being used which created overhead that negatively affected the throughput and performance of the WLAN. Furthermore, as mentioned earlier in this chapter, WEP encryption can be cracked. A better solution would be 802.1X/EAP which requires that all security credentials and transactions be completed before any Layer 3 connectivity is even possible.

Point-to-Point Tunneling Protocol (PPTP)

Point-to-Point Tunneling Protocol (PPTP) does not provide encryption or confidentiality, relying on the tunneled protocol to provide it. PPTP typically uses 128-bit *Microsoft Point-to-Point Encryption (MPPE)*, which uses the RC4 algorithm. PPTP encryption

is considered adequate but not strong. PPTP uses MS-CHAP version 2 for user authentication. Unfortunately, MS-CHAP version 2 can be compromised with offline dictionary attacks, using auditing software such as *Asleap*. VPNs using PPTP technology typically are used in smaller SOHO environments and are easy to configure. Due to its inherent insecurity, VPNs using PPTP should be replaced with VPNs using L2TP/IPsec.

Layer 2 Tunneling Protocol (L2TP)

As its name implies, Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol and is used to create VPNs. Like PPTP, L2TP does not provide encryption or confidentiality, relying on the tunneled protocol to provide it. IPsec is often used with L2TP to provide confidentiality, authentication, and integrity. When the two protocols are used together, they are typically referred to as L2TP/IPsec. The L2TP packets from one network are transported over IP to another network. IPsec provides a secure channel or connection between the two systems, and L2TP provides the tunnel.

Internet Protocol Security (IPsec)

Internet Protocol Security (IPsec) is a bundle of different security protocols, hashing techniques, and encryption algorithms. IPsec is flexible and allows vendors and users to select the different protocols that they want to use. IPsec VPNs use stronger encryption methods and more secure methods of authentication than PPTP. IPsec uses this assortment of protocols to perform the functions that are often linked to it. IPsec can be configured for transport mode or tunnel mode. Transport mode only encrypts the payload of the message and is typically used for host-to-host communications. In tunnel mode, the payload, header, and routing information are all encrypted, and it is typically used for gateway to gateway communications. IPsec VPNs use public and private key cryptography to establish a connection.

Internet Security Association and Key Management Protocol (ISAKMP) is a protocol that is used to establish *security associations (SA)* and cryptographic keys. ISAKMP typically uses the *Internet Key Exchange (IKE and IKEv2)* protocol to set up security associations (SA). SAs are unidirectional, with one SA needing to be created for each direction of the link. IKE uses a *Diffie-Hellman* key exchange to establish a shared session secret. Diffie-Hellman key exchange is a protocol that allows two devices to exchange a secret key across an insecure communications channel, without any prior knowledge. The type of encryption used is determined by the SA.

When configuring IPsec, you can choose *Authentication Header (AH)* or *Encapsulating Security Payload (ESP)*. AH only provides authentication. As part of the authentication, AH guarantees connectionless integrity of the packets along with authentication of their data origin. This helps to protect against replay attacks. Encapsulating Security Payload (ESP) is used for both encryption and authentication of the IP packet. ESP provides origin confidentiality, integrity, and authenticity of packets. ESP does not protect the IP packet header, but protects the entire inner IP packet, including the header.

IPsec uses *Message Digest 5 (MD5)* or *Secure Hash Algorithm 1 (SHA-1)* hash functions in the IKE Authentication. Both of these hash algorithms are cryptographically secure. These hash algorithms have evolved into what is known as *Hashed Message Authentication Codes (HMAC)*, combining additional cryptographic functions to the algorithm. IPsec supports multiple ciphers, including *Data Encryption Standard (DES)*, *Triple DES (3DES)*, and *Advanced Encryption Standard (AES)*. Device authentication is achieved by using either a server-side certificate or a preshared key.

When configuring IPsec, you must define a *transform set*. A transform set is a combination of the security protocols and algorithms that will be used to protect your data. This transform set is the used in the configuration of the VPN server.

Configuration Complexity

As stated earlier in this chapter, the installation of a VPN is not the optimal way of securing your WLAN. There are many components that have to be installed and configured. Because most VPNs operate at Layer 3, static routes often have to be configured and advanced routing skills may be required of the administrator. The configuration would consist of a VPN server, which often is sized by the number of simultaneous connections. The VPN server would have to be configured to authenticate all of the WLAN users as they log on, so the VPN server would either need to have an internal user database, or more likely be configured to authenticate against an external database, such as a RADIUS server. If the number of clients on the WLAN grows, you might have to upgrade your VPN server or add an additional one. You may also have a firewall between the VPN server and the WLAN. This may be necessary because the WLAN itself has no security on it, allowing anyone to connect to it. You would need to have VPN software installed and configured on each wireless client, and you would have to train users how to connect to the WLAN and then log on to the VPN server using the VPN dialer.

Scalability

Scaling a VPN secured WLAN compared to scaling an 802.1X/EAP secured WLAN requires more effort and resources. When scaling an 802.1X/EAP network, the addition of new users only requires an account on the authentication server and the configuration of the 802.1X client, which nowadays is often built into the operating system. The addition of new users in a VPN-secured WLAN also requires the addition of new users on the authentication server. In addition to adding the user, at some point the VPN server will need to be upgraded or expanded to support the additional users. Also, the VPN client will need to be configured and installed on each of the computers that will be used to connect to the WLAN. Any firewalls that the VPN tunnel traverses will have to be configured so the proper ports are open to allow the VPN packets to pass through. Also, if the VPN clients will need to roam across Layer 3 boundaries, the VPN tunnel will collapse. A complex MobileIP solution will have to be put in place along with the VPN infrastructure. As the size of the network grows,

more resources will be used as new users are added to the network, making it a less flexible and scalable solution for WLAN client access.

When Should VPNs be Used with a WLAN?

Although VPN security is an outdated solution for WLAN client access security in the enterprise, many scenarios exist where VPNs can and still be used as part of WLAN security. As mentioned earlier, use of VPN technology is mandatory for remote access when end users connect to public access WLANs. Since there is no encryption used at public access WLANs, a VPN solution is needed to provide for data privacy. Router-to-router VPNs are also used between WLAN controllers across wide area network (WAN) links. VPNs are used for secure connectivity between branch offices and the corporate office. VPN tunnels are also often used to secure point-to-point WLAN bridge links used for wireless backhaul between buildings. Finally, split-tunnel VPNs are also used for *remote AP* solutions across WAN links. A more detailed discussion of how VPNs are still used in WLAN security can be found in Chapter 11, "VPNs, Remote Access, and Guest Access Services."

MAC Filters

Every network card has a physical address known as a *media access control (MAC)* address. This address is a 12-character hex number. 802.11 client stations, like all network-enabled devices, each have unique MAC addresses, and 802.11 access points use MAC addresses to direct frame traffic. Most vendors provide MAC filtering capabilities on their access points and WLAN controllers. MAC filters can be configured either to allow or deny traffic from specific MAC addresses.

Most MAC filters apply restrictions that only allow traffic from specific client stations to pass through based on their unique MAC addresses. Any other client stations whose MAC addresses are not on the allowed list will not be able to pass traffic through the virtual port of the access point and onto the distribution system medium. It should be noted, however, that MAC addresses can be *spoofed*, or impersonated, and any amateur hacker can easily bypass any MAC filter by spoofing an allowed client station's address. Many network adapters have the ability to change the MAC address as an option built into the advanced configuration window for the adapter, as shown in Figure 2.8. Entering the new address and re-enabling the network card is all that is needed to change the MAC identity of the computer. Because of spoofing and because of all the administrative work that is involved

with setting up MAC filters, MAC filtering is not considered a reliable means of security for wireless enterprise networks. The 802.11 standard does not define MAC filtering, and any implementation of MAC filtering is vendor specific.

FIGURE 2.8 Changing a MAC address

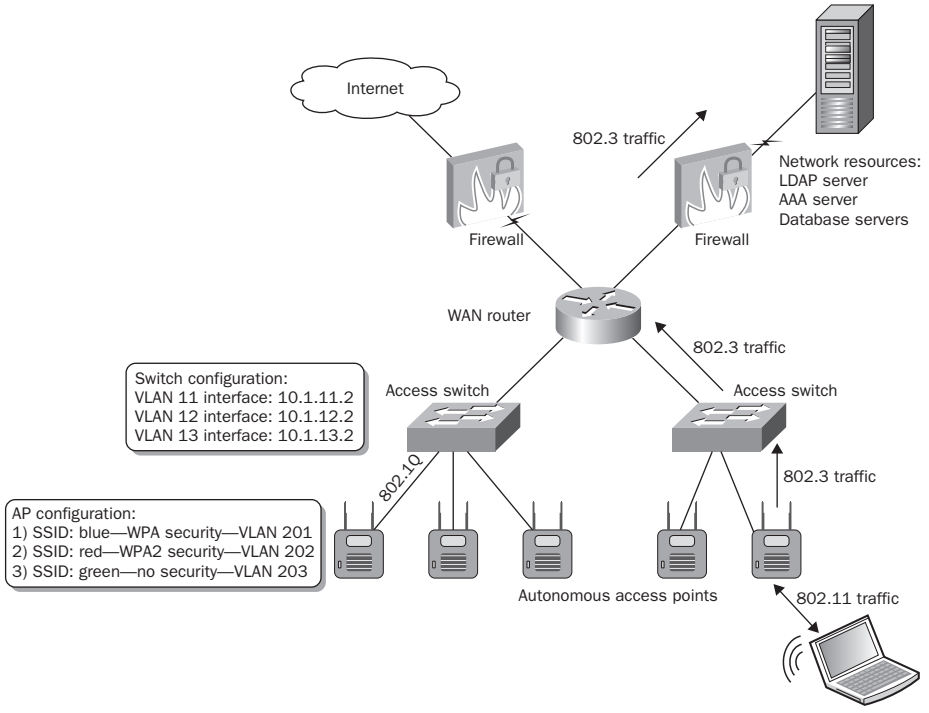
MAC filters are often used as a security measure to protect legacy radios that do not support stronger security. For example, older handheld barcode scanners may use 802.11 radios that support only static WEP. Best practices dictate an extra layer of security by segmenting the handheld devices in a separate VLAN with a MAC filter based on the manufacturer's *organizationally unique identifier (OUI)* address (the first three octets of the MAC address that are manufacturer specific).

SSID Segmentation

Another technique to provide security in a WLAN environment using older autonomous access points was through SSID and VLAN segmentation. It was common for companies to create different SSIDs for different types of users. Companies would set up different SSIDs for many different departments or groups of users. In a WLAN environment using enterprise class autonomous APs, SSIDs can typically be mapped to individual VLANs, and users can be segmented by the SSID/VLAN pair, all while communicating through a single access point. Each SSID can also be configured with separate security settings. As you

can see in Figure 2.9, the autonomous AP would need to be configured to support VLAN tagging using a protocol such as 802.1Q, and the autonomous AP would be connected to an upstream Layer 2 or Layer 3 switch using a trunked connection. Most vendors can have as many as 16 wireless VLANs with the capability of segmenting the users into separate Layer 3 domains.

FIGURE 2.9 Autonomous AP security topology



A common strategy, even with newer WLAN controller technology, is to create a guest, voice, and data VLAN. The SSID mapped to the guest VLAN will have limited or no security, and all users are restricted away from network resources and routed off to an Internet gateway. The SSID mapped to the voice VLAN might be using a security solution such a WPA2-Personal, and the VoWiFi client phones are routed to a VoIP server that provides proprietary QoS services through the VLAN. The SSID mapped to the data VLAN uses a stronger security solution such as WPA2-Enterprise, and the data users are allowed full access to network resources once authenticated.

Some of the downfall of using SSID segmentation with autonomous APs is the amount of configuration required. Each autonomous AP needs to be configured separately for each

SSID and VLAN, along with trunking it to a Layer 2 or Layer 3 switch. Another concern is the amount of additional management frames that are typically transmitted. Each SSID is often treated like a separate AP, generating its own set of beacon frames and responding to probe requests. Some people would go overboard and have eight, ten, or even sixteen different SSIDs. The MAC Layer overhead generated by using too many SSIDs can affect the throughput and performance of the WLAN.

SSID and VLAN segmentation is still in use and highly recommended today with controller based WLANs, and is discussed in detail in Chapter 12, "Wireless Security Infrastructure." Incorporated with a central WLAN controller, role-based access control (RBAC), and sometimes firewall technology, segmentation has become easier, more powerful, and much more flexible.

SSID Cloaking

Remember in *Star Trek* when the Romulans "cloaked" their spaceship but somehow Captain Kirk always found the ship anyway? Well, there is a way to "cloak" your service set identifier (SSID). Access points typically have a setting called *Closed Network* or *Broadcast SSID*. By either enabling a closed network or disabling the broadcast SSID feature, you can hide, or cloak, your wireless network name.

The *service set identifier (SSID)*, which is also often called the *extended service set identifier (ESSID)*, is the logical identifier, or logical name, of a WLAN. The SSID WLAN name is comparable to a Windows workgroup name. The SSID is a configurable setting on all radio cards, including access points and client stations. The SSID can be made up of as many as 32 characters and the SSID is case sensitive.

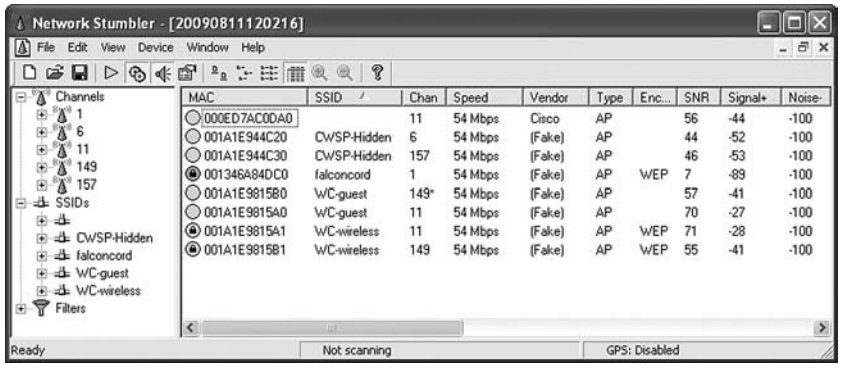
When you implement a closed network, the SSID field in the beacon frame is null (empty), and therefore passive scanning will not reveal the SSID to client stations that are listening to beacons. The idea behind cloaking the SSID is that any client station that does not know the SSID of the WLAN will not be able to associate.

Many wireless client software utilities transmit probe requests with null SSID fields when actively scanning for access points. Additionally, there is a popular and freely available software program called NetStumbler that is used by individuals to discover wireless networks.

NetStumbler also sends out null probe requests actively scanning for access points. When you implement a closed network, the access point responds to null probe requests with probe responses; however, as in the beacon frame, the SSID field is null, and therefore the SSID is hidden to client stations that are using active scanning. Effectively, your wireless network is temporarily invisible, or cloaked. It should be noted that an access point in a closed network will respond to any configured client station that transmits directed probe requests with the properly configured SSID. This ensures that legitimate end users will be able to authenticate and associate to the AP. However, any stations that

are not configured with the correct SSID will not be able to authenticate or associate. Although implementing a closed network will indeed hide your SSID from NetStumbler and other WLAN discovery tools, anyone with a WLAN protocol analyzer can capture the frames transmitted by any legitimate end user and discover the SSID, which is transmitted in cleartext. In Exercise 2.3 you will search through a packet capture to see some of the different types of frames that include the SSID, even when it is hidden. In other words, a hidden SSID can be usually found in seconds with a WLAN protocol analyzer. Many wireless professionals will argue that hiding the SSID is a waste of time, while others view a closed network as just another layer of security. Cloaking the SSID usually keeps the SSID hidden from most WLAN discovery tools that use null probe requests. However, even some of the WLAN discovery tools use alternate methods of discovering a SSID. As shown in Figure 2.10, NetStumbler was able to identify the hidden network with an SSID of CWSP-Hidden2 and was also able to identify that another hidden network exists, but was not able to determine its SSID.

FIGURE 2.10 NetStumbler



Although you can hide your SSID to cloak the identity of your WLAN from novice hackers (often referred to as *script kiddies*) and nonhackers, it should be clearly understood that SSID cloaking is by no means an end-all wireless security solution. The 802.11-2007 standard does not define SSID cloaking, and therefore all implementations of a closed network are vendor specific. As a result, incompatibility can potentially cause connectivity problems. Some wireless clients will not connect to a hidden SSID, even when the SSID is manually entered in the client software. Therefore, be sure to know the capabilities of your devices before implementing a closed network. Cloaking the SSID can also become an administrative and support issue. Requiring end users to configure the SSID in the radio software interface often results in more calls to the help desk because of misconfigured SSIDs.

EXERCISE 2.3

Viewing Hidden SSIDs

In this exercise, you will use a protocol analyzer to view a 70-second packet capture. You will search through this packet capture for the name of a hidden SSID. You will see that even though an SSID is hidden, it is contained in many different types of packets, and can be easily found. The following directions should assist you with the installation and use of WildPacket's OmniPeek protocol analyzer demo software. If you have already installed OmniPeek, you can skip steps 1–5.

1. In your web browser, go to the following URL: `www.wildpackets.com/support/downloads`.
2. Under Product Evals, choose OmniPeek Professional. Fill out the OmniPeek evaluation request. A WildPackets representative will send an email message with a private download URL.
3. Proceed to the private download URL. Download the OmniPeek Professional demo software to your desktop using FTP. This evaluation copy of OmniPeek will be licensed to work for 30 days. Write down the evaluation license serial number.
4. Double-click the installation file `omnp602.exe`, and follow the installation prompts. You will need to be connected to the Internet to activate the license. You will be asked to enter the evaluation serial number.
5. The exercise will use frame captures that are on the CD that came with this book. If you would like to use OmniPeek for live captures, you will need to install the proper drivers for your Wi-Fi radio card. Verify that you have a supported Wi-Fi card. Review the system requirements and supported operating systems. OmniPeek requires you to install the proper drivers for the supported Wi-Fi cards. Information about the drivers can be found at `www.wildpackets.com/support/downloads/drivers`.
6. From Windows, choose Start ➢ Programs ➢ WildPackets OmniPeek, and then click the OmniPeek icon. The OmniPeek application should appear.
7. Click the Open Capture File icon and browse the book's CD. Open the packet capture file called `CWSP_HIDDEN2_SSID.PCAP`.
8. After the capture file loads, double-click on packet 1, which is a beacon frame. OmniPeek will open the frame in a new tabbed window. Scroll down until you find the SSID field. Notice that the SSID field is null (empty). The AP is cloaking the SSID.
9. From the main OmniPeek window, double-click on packet 58, which is a null probe request from a client station. Scroll down until you find the SSID field. Notice that the SSID field is null (empty). The client is sending a null probe request looking for any and all access points. Now double-click on the packet 59, which is the probe response frame from the AP. Scroll down until you find the SSID field. Notice that the SSID field is null (empty). The AP is cloaking the SSID.

EXERCISE 2.3 *(continued)*

10. Select Edit ➢ Find Pattern. The Find In field should be Packet ASCII data. The SSID that you are searching for is CWSP-Hidden2, so you will need to type that in the Find What field. Remember, SSIDs are case sensitive, so you want to make sure that you type it correctly and that you have the Match Case radio button checked. If you unchecked the Match Case radio button, you do not have to be exact with the entry.
11. After you have entered the SSID that you are searching, click the Find Next button and the program will highlight the next frame that matches your search. As it discovers each matching frame, look at the protocol column to see the different types of frames that contain the SSID. These are frame exchanges between the AP and legitimate clients that are preconfigured with the SSID.
12. You can also double-click on any of the frames to see more detail.

Real World Scenario

Should Legacy Security Still be Used?

The simple answer to this question is "yes," if the situation warrants the use of legacy security. Many legacy devices that do not support WPA or WPA2 are still deployed in the enterprise. Common examples are older wireless barcode scanners and other handheld devices that still only support static WEP encryption. The preferred scenario is to replace all of the legacy devices with new devices that support WPA2-Enterprise or WPA2-Personal. However, budgetary reasons often prevent an upgrade to better security. The bottom line is that some security is better than no security. If static WEP encryption is the strongest solution available, it should still be used even though WEP has been cracked.

An often quoted security concept is the concept of the "lowest hanging fruit." If someone walks up to an apple tree and wants an apple to eat, they will usually pick an apple that is eye-level and within arms reach. They will probably not pick an apple that is hanging from a branch 20 feet above the ground. Think of a WLAN using no security as an apple within arms' reach and think of a WLAN using WEP encryption as an apple that is on a branch 20 feet from ground level. The passing individual can still get a ladder if they really want the apple that is 20 feet in the air, but chances are they will ignore the higher apple and still choose to pick an apple that in within arms' reach. If a hacker is determined to crack WEP, they will do it. However, if WEP is used on legacy devices, chances are the hacker will try to access a WLAN with no security as opposed to the WLAN using WEP.

If you're using legacy security, we highly recommend that you to segment the legacy devices in a separate VLAN with a separate SSID. Some legacy devices do not even support static WEP. Those devices should also be put in a separate VLAN on a separate SSID and a MAC filter should be used for security. Any hacker can get around a MAC filter, but at least the apple is higher on the tree.

Summary

In this chapter, you learned about the different de jure and de facto standards that have been used to secure legacy 802.11 networks. We discussed Open System and Shared Key authentication and why Shared Key authentication should no longer be used. We also looked at the encryption and decryption processes of WEP and explained some of its shortcomings that have led to it being deprecated.

It is important to remember that, although VPN technology is widely used and a recommended technology to provide secure communications between networks and between individual clients and networks, it has fallen out of favor for securing WLAN users. Remember that the reason for this is because there are easier and faster security solutions that require less configuration and that can scale up better. VPN solutions can and will still provide secure access for a WLAN, but with an ease, speed, and growth penalty when compared to an 802.1X/EAP solution.

It is important to remember that over the years, in attempts to provide more security to the WLAN, vendors have included many features with their products to allow users to try to secure their networks. MAC filters and SSID cloaking are two legacy features that are both easily bypassed. Both techniques add a level of inconvenience to the network, to the user, and to a potential intruder, but neither adds any level of additional security.

SSID segmentation is one of the legacy security solutions that, if properly configured, has provided security to the network. By integrating SSIDs with VLANs, the flow of traffic can be controlled and isolated. This solution is still used today with wireless controllers, and has been enhanced with the integration of firewalls and identity-based access control.

Exam Essentials

Understand pre-RSNA authentication methods. Be able to explain the differences between Open System authentication and Shared Key authentication.

Describe the WEP encryption and decryption process. Explain the components and process used to encrypt and decrypt a WEP packet. Identify and describe each of the fields that make up a WEP-encrypted 802.11 data frame.

Understand VPN technology and how it is used in a WLAN. Know the differences between the different types of VPN technology that has been used with WLANs. Know the benefits and detriments of each.

Define other non-802.11 WLAN security mechanisms. Explain the other non 802.11 security mechanisms, such as MAC filters, SSID segmentation, and SSID cloaking.

Key Terms

Before you take the exam, be certain you are familiar with the following terms:

Advanced Encryption Standard (AES)
Authentication
Authentication Header (AH)
Broadcast SSID
Ciphertext
Closed Network
cyclic redundancy check (CRC)
Data Encryption Standard (DES)
Diffie-Hellman
Encapsulating Security Payload (ESP)
extended service set identifier (ESSID)
Hashed Message Authentication Codes (HMAC)
Initialization Vector (IV)
Integrity Check Value (ICV)
Internet Key Exchange (IKE and IKEv2)
Internet Protocol Security (IPsec)
Internet Security Association and Key Management Protocol (ISAKMP)
Keystream
Layer 2 Tunneling Protocol (L2TP)
MAC Service Data Unit (MSDU)
media access control (MAC)
Message Digest 5 (MD5)
Open System authentication
organizationally unique identifier (OUI)
Point-to-Point Tunneling Protocol (PPTP)
remote AP
robust security network (RSN)
Secure Hash Algorithm 1 (SHA-1)
security associations (SA)
service set identifier (SSID)
Shared Key authentication
spoofed
transform set
Triple DES (3DES)
virtual private network (VPN)
Wired Equivalent Privacy (WEP)

Review Questions

1. Before an 802.11 client STA can pass traffic through the AP, which two of the following must occur? (Choose two answers.)
   - **A.** 802.1X
   - **B.** EAP
   - **C.** Association
   - **D.** Authentication
   - **E.** WEP keys must match

2. Which of the following is contained in a WEP encrypted frame? (Choose all that apply.)
   - **A.** IV in cleartext format
   - **B.** IV in encrypted format
   - **C.** Key Identifier
   - **D.** WEP key in encrypted format
   - **E.** 64-bit Initialization Vector

3. 128-bit WEP encryption uses a user-provided static key of what size?
   - **A.** 64 bits
   - **B.** 104 bits
   - **C.** 104 bytes
   - **D.** 128 bits
   - **E.** 128 bytes

4. When SSID cloaking is enabled, which of the following occurs? (Choose all that apply.)
   - **A.** The SSID field is set to null in the beacon frame.
   - **B.** The SSID field is set to null in the probe request frame.
   - **C.** The SSID field is set to null in the probe response frame.
   - **D.** The AP stops transmitting beacon frames.
   - **E.** The AP stops responding to probe request frames.

5. Which technologies use the RC4 or ARC4 cipher? (Choose all that apply.)
   - **A.** Static WEP
   - **B.** Dynamic WEP
   - **C.** PPTP
   - **D.** L2TP
   - **E.** MPPE

6. Which of the following is not defined by the 802.11-2007 standard? (Choose all that apply.)
   - **A.** WEP
   - **B.** VPN
   - **C.** MAC filtering
   - **D.** SSID segmentation
   - **E.** SSID cloaking

7. 802.11 pre-RSNA security defines which wireless security solution?
   - **A.** Dynamic WEP
   - **B.** 802.1X/EAP
   - **C.** 64-bit static WEP
   - **D.** Temporal Key Integrity Protocol
   - **E.** CCMP/AES

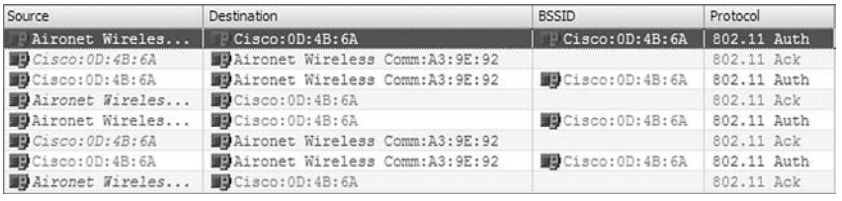
8. Which of the following have been deprecated in the 802.11-2007 standard? (Choose all that apply.)
   - **A.** Wired Equivalent Privacy
   - **B.** Temporal Key Integrity Protocol
   - **C.** Point-to-Point Tunneling Protocol
   - **D.** Shared Key authentication
   - **E.** Open System authentication

9. Peter is configuring an autonomous AP to provide segmentation of three groups of wireless user traffic on the corporate network. Which of the following are recommended ways of doing this? (Choose all that apply.)
   - **A.** Create a single SSID and have the traffic from each of the groups of users placed on a separate VLAN.
   - **B.** Create three separate SSIDs, one for each group, and have each SSID linked with a separate VLAN.
   - **C.** Create a trunk for each of the VLANs between the AP and the upstream switch.
   - **D.** Create a single trunk for all of the VLANs between the AP and the upstream switch.
   - **E.** Configure each of the SSIDs with the same encryption keys for easier management and administration.
   - **F.** Configure each of the SSIDs with different encryption keys, even though it will be more difficult to manage and administer.

10. Evan has configured a laptop and an AP, each with two WEP keys. WEP key 1 is the same on both devices, and WEP key 2 is the same on both devices. He configured the laptop to use WEP key 1 to encrypt its data. He configured the AP to use WEP key 2 to encrypt its data. Will this configuration work?
    - **A.** No, since there is only one WEP key on each device.
    - **B.** No, since the value of the WEP key must be identical on both the laptop and the AP.
    - **C.** Yes, as long as the value of WEP key 1 is identical on both computers and the value of WEP key 2 is identical on both computers.
    - **D.** Yes. The laptop and AP will only use the first WEP key, so as long as the value of these keys is identical, the configuration will work.
    - **E.** Yes. The laptop and AP will attempt to use each of the WEP keys when decrypting a frame.

11. Laura is attempting to diagnose a WLAN by using a packet analyzer to capture the exchange of frames and packets between a wireless client and the AP. In the process of analyzing the packets, she sees two 802.11 authentication frames, two 802.11 association frames, DHCP requests and responses, and then she begins to see encrypted data. Which of the following could the client be using? (Choose all that apply.)
    - **A.** Open System authentication
    - **B.** Shared Key authentication
    - **C.** 802.1X/EAP
    - **D.** WEP
    - **E.** PPTP
    - **F.** L2TP/IPsec

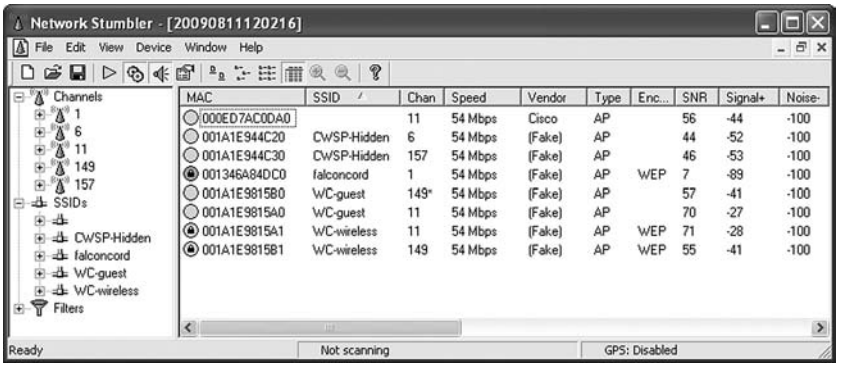
12. This graphic shows a packet capture of a successful 802.11 authentication. In which of the following types of client connections could this authentication not occur? (Choose all that apply.)



Source	Destination	BSSID	Protocol
Aironet Wireles...	Cisco:0D:4B:6A	Cisco:0D:4B:6A	802.11 Auth
Cisco:0D:4B:6A	Aironet Wireless Comm:A3:9E:92		802.11 Ack
Cisco:0D:4B:6A	Aironet Wireless Comm:A3:9E:92	Cisco:0D:4B:6A	802.11 Auth
Aironet Wireles...	Cisco:0D:4B:6A		802.11 Ack
Aironet Wireles...	Cisco:0D:4B:6A	Cisco:0D:4B:6A	802.11 Auth
Cisco:0D:4B:6A	Aironet Wireless Comm:A3:9E:92		802.11 Ack
Cisco:0D:4B:6A	Aironet Wireless Comm:A3:9E:92	Cisco:0D:4B:6A	802.11 Auth
Aironet Wireles...	Cisco:0D:4B:6A		802.11 Ack

    - **A.** 802.1X/EAP
    - **B.** VPN
    - **C.** WEP with Shared Key authentication
    - **D.** WEP with Open System authentication
    - **E.** Open System authentication with WEP

13. This graphic shows a NetStumbler screen. How many SSIDs are configured with cloaking enabled? (Choose all that apply.)



A. None

B. At least one

C. Two

D. Three

E. Exact number cannot be determined

14. 128-bit WEP encryption uses a _____ IV and a _____ static key.

A. 64 bit and 64 bit

B. 24 bit and 104 bit

C. 28 bit and 100 bit

D. 20 bit and 108 bit

E. None of the above

15. The graphic shows a packet capture of a successful 802.11 authentication. In which of the following types of client connections could this not occur?

A. 802.1X/EAP

B. VPN

C. WEP with Shared Key authentication

D. WEP with Open System authentication

E. Unencrypted

16. Which hash algorithms can be used in the IKE Authentication process? (Choose all that apply.)
    - **A.** Diffie-Hellman
    - **B.** MS-CHAPv2
    - **C.** MD5
    - **D.** ISAKMP
    - **E.** SHA-1

17. What is a possible vulnerability when deploying a Layer 3 IPsec VPN as a security solution for an 802.11 wireless network? (Choose all that apply.)
    - **A.** Layer 3 VPNs use weak encryption that can be cracked.
    - **B.** Layer 3 VPNs provide no segmentation solution.
    - **C.** Layer 3 VPNs break up collision domains but not broadcast domains.
    - **D.** Access points are still open to attack.
    - **E.** A WLAN controller is still open to attack.

18. Which of these authentication methods is the most secure?
    - **A.** Open System authentication with WEP
    - **B.** Open System authentication without WEP
    - **C.** Shared Key authentication
    - **D.** 802.1X/EAP authentication

19. Which of the following specifications are true for an SSID? (Choose all that apply.)
    - **A.** Up to 20 characters
    - **B.** Up to 32 characters
    - **C.** Case sensitive
    - **D.** Spaces are allowed
    - **E.** Spaces are not allowed

20. Which 802.11 Layer 2 protocol is used for authentication in an 802.1X framework?
    - **A.** Extensible Authentication Protocol
    - **B.** Extended Authentication Protocol
    - **C.** MS-CHAP
    - **D.** Open System
    - **E.** Shared Key

Answers to Review Questions

1. C, D. In order for a client to connect to the WLAN and pass data, the client must authenticate and associate. The other three choices could occur, but do not have to.

2. A, C. When a WEP encrypted frame is created, the 24-bit Initialization Vector is included in the Layer 2 header of the 802.11 data frame in cleartext format. A Key Identifier is also included, indicating to the receiving computer which of the 4 potential WEP keys it should use to decrypt the frame.

3. B. 128-bit WEP is known as WEP-104 in the 802.11-2007 standard. A 104-bit WEP key is provided by the user and the system adds to it the 24-bit Initialization Vector to equal 128 bits.

4. A, C. When SSID cloaking, or Hidden SSID, is enabled, beacon management frames are still transmitted, but the SSID field is set to null. The probe response frame is almost identical to the beacon frame, and it too has the SSID field set to null. In any environment, the probe request frame may or may not contain a value for the SSID field, depending on whether the client knows the SSID of the network to which it is connecting. The AP cannot stop transmitting beacons because the frames contain additional information that is critical to the functioning of the network. When an AP receives a probe request frame, by default it will respond with a probe response frame.

5. A, B, E. WEP, whether it is statically configured or whether it changes periodically, uses this cipher to encrypt and decrypt frames. MPPE (Microsoft Point-to-Point Encryption) uses the RC4 algorithm. TKIP (Temporal Key Integrity Protocol), which is covered in later chapters, also uses ARC4.

6. B, C, D, E. WEP is the only option that is actually defined by the 802.11-2007 standard. All the other options are considered to be non-802.11 security measures.

7. C. The original 802.11 standard ratified in 1997 defined the use of a 64-bit or 128-bit static encryption solution called Wired Equivalent Privacy (WEP). WEP is considered pre-RSNA security. Dynamic WEP was never defined under any wireless security standard. The use of 802.1X/EAP, TKIP/RC4, and CCMP/AES are all defined under the current 802.11-2007 standard for robust network security.

8. A, D. Temporal Key Integrity Protocol (TKIP) is defined in the 802.11-2007 standard and is still considered to be an RSN mechanism. Point-to-Point Tunneling Protocol (PPTP) is a VPN technology that is not part of the 802.11-2007 standard. Shared Key authentication and Wired Equivalent Privacy (WEP) are the two pre-RSNA (robust security network association) security mechanisms that have been deprecated. Deprecated technologies have been superseded by new technologies and should be avoided. Open System authentication is the one pre-RSNA security mechanism that has not been deprecated.

9. B, D, F. Each group should be configured with a separate SSID and a separate VLAN. With autonomous APs, it is not possible to have traffic connect to a single SSID and be assigned to different VLANs. There will be one trunk connection from the autonomous AP to the upstream switch. This trunk will carry the traffic from all of the VLANs that are supported on the AP. Since each group of users has different requirements and are being placed on different VLANs, they should also be configured with different encryption keys so that they cannot connect to the other networks.

10. C. There are up to four WEP keys that can be entered on a Wi-Fi device. In addition to entering the four WEP keys, one will be designated to be used to encrypt all transmitted data. When the encrypted frame is received, part of the frame tells the receiving system which key (1, 2, 3, or 4) was used to encrypt the frame. The receiving system then attempts to decrypt the frame using the specified key. If the value of the key is the same on the receiving system, then the frame will be decrypted. Each system can use a separate key to encrypt the data.

11. A, E, F. Since there are only two 802.11 authentication frames, Open System authentication is being used. Shared Key authentication would generate four 802.11 authentication frames. If 802.1X/EAP or WEP were being used, then the client would be doing L2 encryption and the DHCP frames would be encrypted and not visible. Therefore 802.1X/EAP and WEP are not being used. Both PPTP and L2TP/IPsec perform Layer 3 encryption that would allow Laura to see the DHCP exchange and any other IP traffic.

12. A, D, E. The graphic shows an 802.11 Shared Key authentication that is made up of four authentication frames; an Authentication Request followed by a cleartext challenge frame, followed by a challenge response with the cleartext data encrypted, and then followed by an Authentication Response. 802.1X/EAP works together with Open System authentication, but cannot be deployed when WEP is used. In order to use Shared Key authentication, WEP must be enabled. A VPN can be used with Shared Key or Open System authentication. Companies would use a VPN for data privacy because WEP has been cracked, but they often would still use WEP as an added layer of security. Shared Key authentication is optional with WEP, although not recommended.

13. B, E. Looking at the NetStumbler screen, the first line displays a network, but it is unable to determine the SSID. This is a hidden or cloaked network. Cloaking the SSID usually keeps the SSID hidden from most WLAN discovery tools that use null probe requests. Any of the SSIDs shown could be hidden; however, since hiding an SSID does not guarantee that it cannot be seen, from this screen there is no way of knowing which, if any, of the other SSIDs are configured for cloaking. Because hidden SSIDs are still transmitted in cleartext in some 802.11 management frames, a protocol analyzer can always find a hidden SSID. Even simple WLAN discovery tools such as NetStumbler may sometimes discover hidden SSIDs.

14. B. 128-bit WEP encryption uses a secret 104-bit static key that is combined with a 24-bit Initialization Vector for an effective key strength of 128 bits.

15. C. The graphic shows a two-frame Open System authentication. 802.1X/EAP works together with Open System authentication. VPN can be configured with either Open System or Shared Key authentication. An unencrypted session uses Open System authentication.

16. C, E. Message Digest 5 (MD5) and Secure Hash Algorithm 1 (SHA-1) are both hash algorithms. Diffie-Hellman is a protocol that allows two devices to exchange a secret key across an insecure communications channel. MS-CHAPv2 is used for authentication with Point-to-Point Tunneling protocol (PPTP). Internet Security Association and Key Management Protocol (ISAKMP) uses IKE to set up security associations.

17. D, E. Unlike 802.1X/EAP solutions, an IP address is needed before a VPN tunnel can be established. A downside to using a VPN solution is that access points and WLAN controllers are potentially open to attack because a potential attacker can get both a Layer 2 and Layer 3 connection before the VPN tunnel is established. An unsecured management interface on either an autonomous AP or a WLAN controller could be accessed if Layer 3 connectivity is established prior to security transactions. 802.1X/EAP requires that all security credentials and transactions are completed before any Layer 3 connectivity is even possible.

18. D. When Open System authentication is used without WEP, all client stations are allowed to join the BSS and no data privacy is provided. WEP encryption is used as part of the Shared Key authentication process, but the WEP key could potentially be exposed and the 802.11 data frames are at risk. If static WEP is the chosen encryption solution, the WEP key is slightly safer when used with Open System authentication. Because WEP has been cracked, it should be avoided entirely. 802.1X/EAP provides the strongest authentication solution and is used together with dynamic encryption such as TKIP/RC4 and CCMP/AES.

19. B, C, D. SSIDs can be up to 32 characters long, they are case sensitive, and they can have spaces in them, although we do not recommend putting spaces in an SSID.

20. D. Open System authentication and Shared Key authentication are both Layer 2 authentication methods defined by the 802.11-2007 standard. Open System authentication must be used in an 802.1X framework. Shared Key authentication requires WEP, which cannot be used with 802.1X. Extensible Authentication Protocol is a universal authentication framework, but is not defined by 802.11. MS-CHAP is also not defined by 802.11.

Chapter 3

Encryption Ciphers and Methods

IN THIS CHAPTER, YOU WILL LEARN ABOUT THE FOLLOWING:

- ✓ **Encryption basics**
  - Symmetric and asymmetric algorithms
  - Stream and block ciphers
  - RC4
  - RC5
  - DES
  - 3DES
  - AES
- ✓ **WLAN Encryption methods**
- ✓ **WEP**
  - WEP MPDU
- ✓ **TKIP**
  - TKIP MPDU
- ✓ **CCMP**
  - CCMP MPDU
- ✓ **WPA/WPA2**
- ✓ **Proprietary Layer 2 implementations**

Over the years people have created many ways to secure data for many purposes. In this chapter, you will learn about the different encryption algorithms that are used to secure wireless networks. You will see how encryption ciphers work to create encrypted data from plaintext data. This chapter will also discuss the encryption methods that are part of the 802.11-2007 standard, and the ciphers that they use. When data is encrypted, additional overhead is added to the frames. In this chapter, you will also see the MAC Protocol Data Unit (MPDU) format of Wired Equivalent Privacy (WEP), Temporal Key Integrity Protocol (TKIP), and Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) encrypted frames.

Encryption Basics

One of the major concerns with wireless networking has always been the fact that wireless communications use what is referred to as an *unbounded medium*. The wireless signal radiates away from the transmitting device in all directions, unlike a wired signal, which travels along the path of the cable. In other words, the RF physical medium is not limited to a cable and has no set boundaries. Since wireless is unbounded, and the signal can essentially be heard by anyone within listening range, measures need to be taken to secure the transmission so that only the intended recipients can understand the message. Therefore, data privacy should be considered mandatory. All essential data must be encrypted prior to transmission and then decrypted after being received.

Chapter 1, "WLAN Security Overview," introduced the concept of cryptology. To review this concept briefly, the goal of cryptology is to process a piece of information, often referred to as *plaintext*, through an algorithm, often referred as a *cipher*, and transform the plaintext into encrypted text, which is also known as *ciphertext*. This ciphertext can then be decrypted, or converted back into plaintext, only by someone who knows the cipher.

The cipher is the process or algorithm that transforms the plaintext into encrypted text. One of the earliest ciphers, the Caesar cipher, is named after Julius Caesar. The Caesar cipher is a type of substitution cipher in which each letter of the alphabet is replaced by a different letter. When writing a message, Caesar shifted the alphabet by three characters to encrypt and protect his messages. Figure 3.1 shows the plaintext alphabet along with the shifted cipher key. The figure also shows a sample message in both plaintext and its ciphertext.

FIGURE 3.1 Example of the Caesar cipher

```
Plaintext Key:       ABCDEFGHIJKLMNOPQRSTUVWXYZ
Ciphertext Key:      DEFGHIJKLMNOPQRSTUVWXYZABC

Plaintext  Message: CWSP IS A GREAT CERTIFICATION TO EARN
Ciphertext Message: FZVS LV D JUHDW FHUWLILFDWLRQ WR HDUQ
```

Ciphers have come a long way since the Caesar cipher. Present-day ciphers use mathematical calculations along with multiple repetitions or transformation rounds, with each round typically consisting of multiple processing steps.

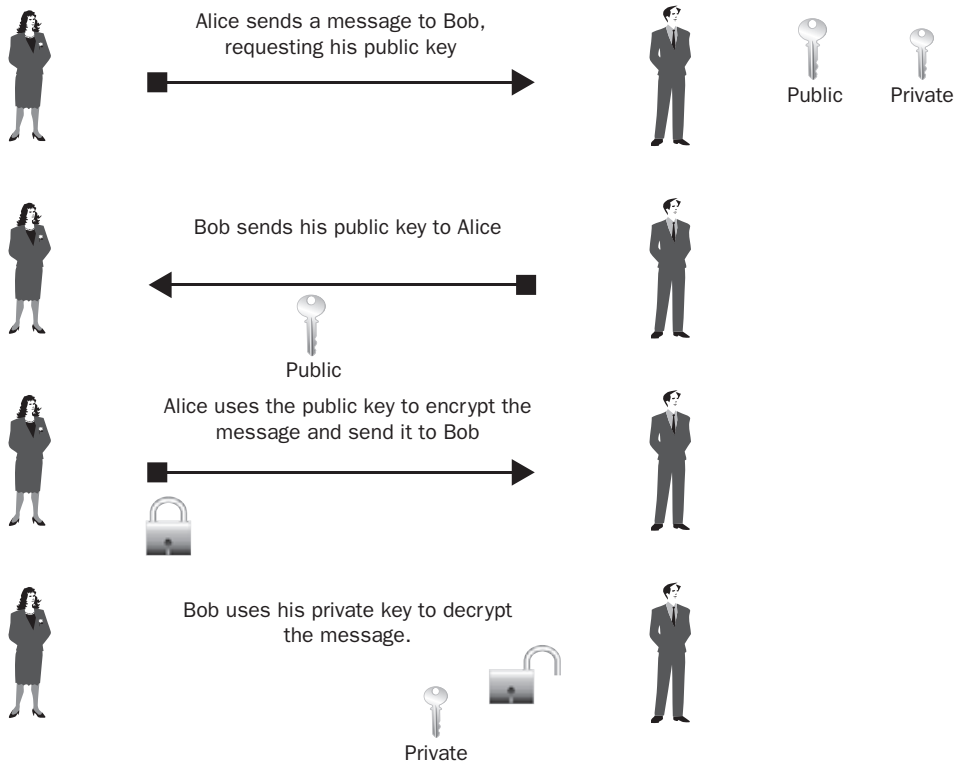
Symmetric and Asymmetric Algorithms

Most cipher algorithms can be categorized as either a *symmetric algorithm* or an *asymmetric algorithm*. When using a symmetric algorithm, both the encrypting and decrypting parties share the same key. To ensure the privacy of a symmetric algorithm encrypted communication, the key needs to be kept secret. A potential problem with this is that the key must be shared between two or more parties prior to establishing the secure communications channel. Therefore, it is necessary to have a secure method of sharing the key. WEP, TKIP, and CCMP are encryption methods that all use symmetric algorithms.

Instead of using a single shared key, asymmetric algorithms use a pair of keys. As shown in Figure 3.2, one key is used for encryption and the other is used for decryption. The decryption key is typically kept secret and is known as the *private key*, or "secret key." The encryption key is shared and is referred to as the *public key*. The premise is that if you wanted to send someone an encrypted message, you would obtain and use the public key to encrypt the message. The public key is only good for encrypting the message and cannot be used to decrypt the message. So even though many people could have the public key, none of them would be able to decrypt your message. Only someone with the private key would be able to decrypt it. Public key cryptography builds on the use of asymmetric encryption and digital signatures. Some methods of EAP authentication use digital certificates based on the X.509 standard for a *public key infrastructure (PKI)*.

Symmetric algorithms generally require less computer processing power than asymmetric algorithms and, therefore, are typically much faster. However, the problem still exists that, with a symmetric algorithm, the key must be exchanged prior to the establishment of the secure communications, whereas with an asymmetric algorithm, the shared key that is used to decrypt the message never needs to be disclosed. Each method has benefits and drawbacks.

FIGURE 3.2 Asymmetric keys



EAP and Digital Certificates

You can find a more detailed explanation about EAP authentication methods in Chapter 4, "Enterprise 802.11 Layer 2 Authentication Methods." A more detailed discussion about digital certificates and public key infrastructure (PKI) can be found in Chapter 12, "Wireless Security Infrastructure and Capabilities."

Stream and Block Ciphers

During the cryptographic process, the plaintext needs to be combined with random data bits to create the ciphertext. One common way of performing this task is sequentially, on a bit-by-bit basis. Ciphers that use this technique are known as stream ciphers. A *stream cipher* is a symmetric key cipher where plaintext bits are combined with a pseudorandom

cipher bit stream called the *keystream*. The keystream is generated when some sort of seed is used to feed the stream cipher algorithm. For example, WEP encryption uses a static key that feeds the RC4 stream cipher, which then generates the pseudorandom keystream. The stream cipher then combines the plaintext with the keystream, typically using a Boolean *Exclusive-OR (XOR)* operation. Stream ciphers are often used when the plaintext is not consistently one size, such as the data transmitted on a wireless LAN.

Boolean logic is a mathematical way to compare or combine bits. As shown in Table 3.1, an Exclusive Or (XOR) will generate a 0 when both of the input values are the same and will generate a 1 when both of the input values are different. When an XOR is used with a shared key, the same key will successfully encrypt and then decrypt the data.

TABLE 3.1 Exclusive OR (XOR)

Input 1	Input 2	XOR Output
0	0	0
0	1	1
1	0	1
1	1	0

Another common method of creating the ciphertext is using a *block cipher*. Unlike stream ciphers, which operate on one bit at a time, a block cipher takes a fixed-length block of plaintext and generates a block of ciphertext of the same length. A block cipher is a symmetric key cipher operating on fixed-length groups of bits, called *blocks*. For example, a block cipher will use a 128-bit block of input of plaintext, and the resulting output would be a 128-bit block of ciphertext. The fixed length of the blocks is referred to as the *block size*, with block sizes often ranging from 64 bits up to 256 bits. Most block ciphers are designed to apply a simpler function repeatedly to the block. Each iterative process or function is referred to as a round. Depending on the specific block cipher, the *round function* could be repeated as many as a few dozen times. In most instances, the greater the number of rounds, the greater the level of security; however, performance will be effected due to the time needed to perform the rounds.

RC4

RC4 is a stream cipher that was designed by Ron Rivest of RSA Security in 1987. The RC in RC4 stands for Rivest Cipher or Ron's Code. RC4 was originally a trade secret;

however, a description of it was anonymously leaked on the Internet in September 1994. After the code was leaked and confirmed to be genuine, and the algorithm was known, it was clearly no longer a trade secret. Although the algorithm was no longer a trade secret, the name "RC4" was trademarked and could only be used with permission. RSA never released the algorithm, so unofficial versions of it are often referred to as *Arcfour* or *ARC4*, which stands for "Alleged RC4." RC4 is fast and simple, and it is widely used in protocols such as WEP and Secure Sockets Layer (SSL). Due to weaknesses in the cipher, it is not recommended for use in newer networks.

RC5

RC5 is a symmetric block cipher that was designed by Ron Rivest in 1994, and a U.S. patent was granted for it in May 1997. RC5 allows for a variable block size, a variable key size, and a variable number of rounds. The block size can be set to 32, 64, or 128 bits; the key size can range from 0 bits to 2040 bits; and the number of rounds can range from 0 to 255. A key table is created, with the size of the table varying depending on the number of rounds that will be performed. When the user-provided secret key is entered, a key-expansion routine will expand the user-provided key to fill the key table. This key table is used for both encryption and decryption.

DES

Data Encryption Standard (DES) is a symmetric block cipher that was developed in the early 1970s. In 1976, it was selected by the National Bureau of Standards (NBS), currently known as the National Institute of Standards and Technology (NIST), as part of the official Federal Information Processing Standards (FIPS) for the United States. DES uses a 56-bit symmetric key, and it is now considered to be insecure primarily due to the key size being too small. Multiple groups have successfully cracked DES using what are known as *brute-force attacks*, sequentially trying every possible key. DES has a 64-bit block size and a 64-bit key; however, 8 bits are used for checking parity and are discarded, so the effective key length is 56 bits. DES performs 16 identical rounds on each block.

The history of DES is very interesting. A quick search on the Internet will reveal that the National Security Agency (NSA) was accused of tampering with it and covertly weakening the algorithm. These accusations were later shown to be false.

3DES

Triple Data Encryption Algorithm (TDEA), also known as *Triple DES (3DES)*, is a symmetric block cipher published in 1998. 3DES uses a key bundle, which is made up of three DES keys (K1, K2, and K3), each with an effective key length of 56 bits. Like DES, each key is made up of 64 bits; however, 8 bits are used for checking parity and are discarded. 3DES is essentially DES run three different times using three keys. Therefore, it performs 48 DES-equivalent rounds on each block. 3DES defines three keying options:

Keying Option 1 All three keys are unique.

Keying Option 2 K1 and K2 are unique, but K3 = K1.

Keying Option 3 All three keys are identical; K1 = K2 = K3.

Keying option 1 is the strongest, because all three keys are unique, giving it an effective key size of 168 bits. Keying option 3 is the weakest, and it is essentially equal to very slow DES. Remember that with a symmetric algorithm, the same key that encrypts the data also decrypts the data. With 3DES, after the first pass with K1 encrypts the data, the second pass with K2 actually decrypts the data, and the third pass with K3 encrypts the data again. Keying option 2 provides an effective key size of 112 bits. In 1999, DES was reaffirmed by FIPS for the fourth time, with 3DES the preferred method and single DES permitted only in legacy systems.

AES

Advanced Encryption Standard (AES) is an encryption standard adopted by the U.S. government. AES uses an algorithm that is a symmetric block cipher which supports three key sizes of 128, 192, and 256 bits. These different key lengths are referred to as AES-128, AES-192, and AES-256. AES was announced in November 2001 by the National Institute of Standards and Technology (NIST) as the Federal Information Processing Standards (FIPS) 197. Although FIPS 197 specifies AES, it is just an algorithm that can be incorporated into many different types of security solutions. For example, AES can be used by an IPSec VPN as well as in WPA2 security. It is based on the *Rijndael* algorithm, which was developed by two Belgian cryptographers, Vincent Rijmen and Joan Daemen. AES is used by the 802.11 encryption protocol CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), which officially became part of wireless security when 802.11i was ratified in June 2004. Remember that 802.11i is now part of the 802.11-2007 standard.

AES uses a fixed block size of 128 bits, which is actually a 434 array of bytes, called a *state*. The number of rounds performed on the block varies depending on the key sizes. AES-128 performs 10 rounds, AES-192 performs 12 rounds, and AES-256 performs 14 rounds.

Real World Scenario

802.11 WLANs and FIPS Validation

Security is the number one concern when deploying wireless technology in government environments. In most countries, there are mandated regulations on how to protect and secure data communications within all government agencies. In the United States, the *National Institute of Standards and Technologies (NIST)* maintains the *Federal Information Processing Standards (FIPS)*. FIPS 197 defines the Advanced Encryption Standard (AES). However, of special interest to wireless security is the FIPS 140-2 standard, which defines security requirements for cryptography modules. The use of validated cryptographic modules is required by the US government for all unclassified communications. A WLAN infrastructure cannot be deployed in most US government agencies unless the solution has been FIPS 140-2–validated by NIST. WLAN vendors spend a lot of time and money getting their WLAN security solutions FIPS 140-2–validated. Local governments and other nations also recognize the FIPS 140-2 requirements or have similar regulations. Both the FIPS 197 and FIPS 140-2 publications can be downloaded in PDF format from the NIST website at `http://csrc.nist.gov/publications/PubsFIPS.html`.

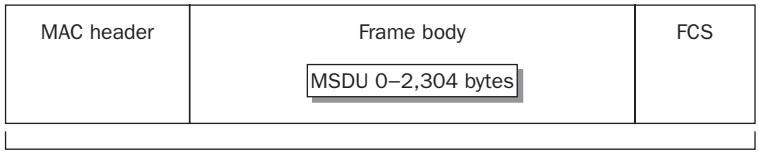
WLAN Encryption Methods

The 802.11-2007 standard defines three encryption methods that operate at Layer 2 of the OSI model: WEP, TKIP, and CCMP. The information that is being protected by these Layer 2 encryption methods is data found in the upper layers of 3–7. Layer 2 encryption methods are used to provide data privacy for 802.11 data frames.

The technical name for an 802.11 data frame is a *MAC Protocol Data Unit (MPDU)*. The 802.11 data frame, as shown in Figure 3.3, contains a Layer 2 MAC header, a frame body, and a trailer, which is a 32-bit CRC known as the *frame check sequence (FCS)*. The Layer 2 header contains MAC addresses and the duration value. Encapsulated inside the frame body of an 802.11 data frame is an upper-layer payload called the *MAC Service Data Unit (MSDU)*. The MSDU contains data from the Logical Link Control (LLC) and Layers 3–7. A simple definition of the MSDU is that it is the data payload that contains an IP packet plus some LLC data. The 802.11-2007 standard states that the MSDU payload can be anywhere from 0 to 2,304 bytes. The frame body may actually be larger due to encryption overhead.

WEP, TKIP, CCMP, and other proprietary Layer 2 encryption methods are used to encrypt the MSDU payload of an 802.11 data frame. Therefore, the information that is being protected is the upper layers of 3–7, which is more commonly known as the IP packet.

FIGURE 3.3 802.11 MAC Protocol Data Unit (MSDU)



It should be noted that many types of 802.11 frames are never encrypted. 802.11 management frames only carry a Layer 2 payload in their frame body, so encryption is not needed. 802.11 control frames only have a header and a trailer; therefore, encryption is not necessary. Some 802.11 data frames, such as the null function frame, actually do not have an MSDU payload. Non-data-carrying data frames have a specific function, but they do not require encryption. Only 802.11 data frames with an MSDU payload can be encrypted. As a matter of corporate policy, 802.11 data frames should always be encrypted for data privacy and security purposes.

WEP, TKIP, and CCMP are encryption methods that all use symmetric algorithms. WEP and TKIP use the RC4 cipher, while CCMP uses the AES cipher. The current 802.11-2007 standard defines WEP as a legacy encryption method for pre-RSNA security. TKIP and CCMP are considered to be compliant *robust security network (RSN)* encryption protocols.

How are 802.11 Encryption Keys Created?

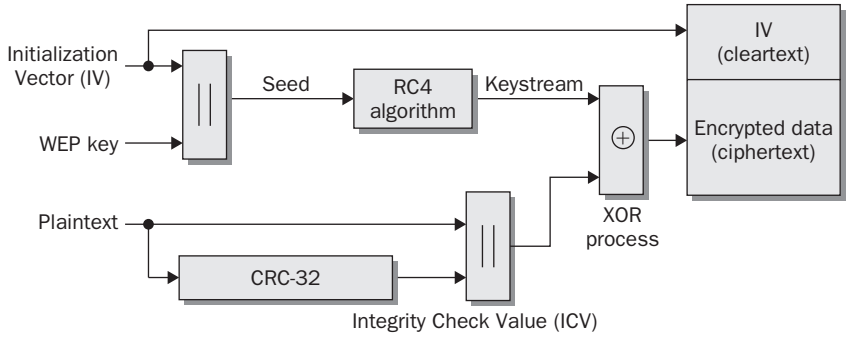
As you have already learned, WEP uses a preconfigured static key. Static keys are always susceptible to social engineering attacks; therefore, TKIP and CCMP use encryption keys that are dynamically generated by the *4-Way Handshake*. How TKIP and CCMP keys are created using the 4-Way Handshake is discussed in great detail in Chapter 5.

WEP

Wired Equivalent Privacy (WEP) is a Layer 2 security protocol that uses the RC4 streaming cipher. The original 802.11 standard defined both 64-bit WEP and 128-bit WEP as supported encryption methods. The current 802.11-2007 standard still defines WEP as a legacy encryption method for pre-RSNA security. The Wi-Fi Alliance has been certifying 802.11 radios using WEP encryption since 2000. You learned about WEP encryption in Chapter 2, "Legacy 802.11 Security."

For a brief review of the WEP encryption process, recall that a 24-bit cleartext *Initialization Vector (IV)* is randomly generated and combined with the static secret key. As shown in Figure 3.4, the static key and the IV are used as WEP seeding material through the pseudorandom RC4 algorithm that generates the keystream. The pseudorandom bits in the keystream are then combined with the plaintext data bits by using a Boolean XOR process. The end result is the WEP ciphertext, which is the encrypted data. WEP also runs a *cyclic redundancy check (CRC)* on the plaintext data that is to be encrypted and then appends the *Integrity Check Value (ICV)* to the end of the plaintext data. The ICV is used for data integrity and should not be confused with the Initialization Vector (IV), which is a part of the seeding material for the RC4 cipher.

FIGURE 3.4 WEP encryption process



WEP encryption is covered extensively in Chapter 2. Therefore, rather than exploring the topic again in great detail, we will direct you back to Chapter 2.

WEP MPDU

The encryption and decryption process for WEP is the same whether you are using WEP-40 or WEP-104. Figure 3.5 shows the WEP frame body, which contains an encrypted MSDU. To create the WEP-encrypted MSDU, WEP runs a cyclic redundancy check (CRC) on the plaintext data that is to be encrypted and then appends the Integrity Check Value (ICV) to the end of the plaintext data. The ICV adds 32 bits (4 octets) of overhead to an 802.11 data frame. The data and ICV are then encrypted. WEP can be configured with up to four different keys. A Key ID identifies which WEP key was combined with the system-generated 24-bit Initialization Vector (IV) to perform the encryption. This 24-bit IV is combined with the KEY ID and 6 bits of padding to create a 32-bit IV. The IV adds 32 bits (4 octets) of overhead to the frame body of an 802.11 data frame. The IV is not encrypted and is appended to the front of the encrypted MSDU payload.

Bits, Bytes, Octets

A *bit* is a binary digit, taking a value of either 0 or 1. Binary digits are a basic unit of communication in digital computing. A byte of information comprises 8 bits. An *octet* is another name for one byte of data. The CWSP exam uses the terminology of octet and byte interchangeably.

Remember that WEP encrypts the MSDU upper-layer payload that is encapsulated in the frame body of an MPDU. The MSDU payload has a maximum size of 2,304 bytes. Because the IV adds 4 octets and the ICV also adds 4 octets, when WEP is enabled, the entire size of the body inside an 802.11 data frame is expanded by 8 bytes to a maximum of 2312 bytes. In other words, WEP encryption adds 8 bytes of overhead to an 802.11 MPDU.

TKIP

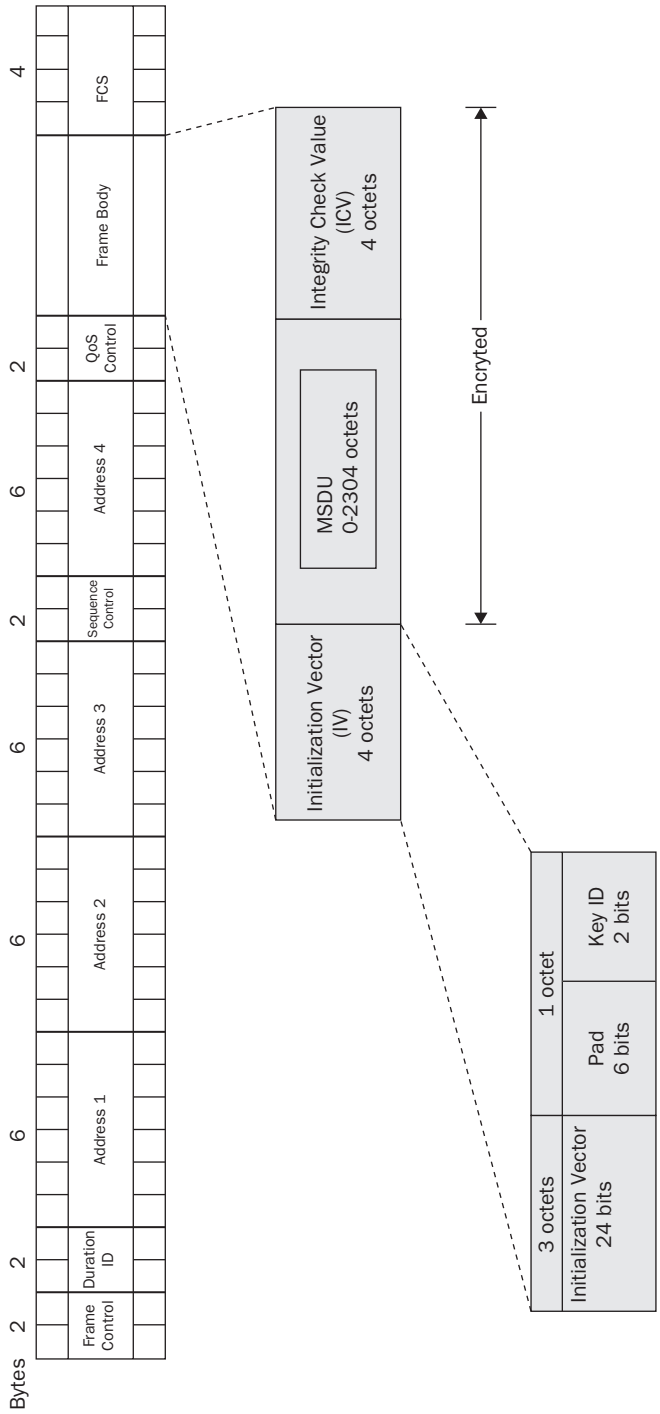
Temporal Key Integrity Protocol (TKIP) is a security protocol that was created to replace WEP. After WEP encryption was broken, 802.11 networks were left without a reliable security solution. The IEEE 802.11i security task group first defined TKIP to provide a stronger security solution without requiring users to replace their legacy equipment. Most legacy 802.11 radios could implement TKIP with a firmware upgrade, but not all legacy APs and STAs were upgradeable. The intent of TKIP was to provide a better temporary security solution until WLAN vendors could provide hardware that supported CCMP/AES encryption. The IEEE 802.11-2007 standard defines two RSNA data confidentiality and integrity protocols: TKIP and CCMP, with TKIP support optional. In April 2003, the Wi-Fi Alliance introduced the *Wi-Fi Protected Access (WPA)* certification, which requires the use of TKIP encryption.

TKIP is actually an enhancement of WEP. Like WEP, TKIP uses the ARC4 algorithm for performing its encryption and decryption processes. The TKIP enhancements were also intended to address the many known weaknesses of WEP. TKIP modifies WEP as follows:

Temporal Keys TKIP uses dynamically created encryption keys as opposed to the static keys. Any two radios use a 4-Way Handshake process to create dynamic unicast keys that are unique to those two radios. Static keys are susceptible to social engineering attacks. Dynamic encryption key generation is designed to defeat social engineering attacks.

Sequencing TKIP uses a per-MPDU *TKIP sequence counter (TSC)* to sequence the MPDUs it sends. An 802.11 station drops all MPDUs that are received out of order. Sequencing is designed to defeat replay and reinjection attacks that are used against WEP.

FIGURE 3.5 WEP MPDU format



Key Mixing TKIP uses a complex two-phase cryptographic mixing process to create stronger seeding material for the RC4 cipher. The key mixing process is designed to defeat the known IV collisions and weak-key attacks used against WEP.

Enhanced Data Integrity TKIP uses a stronger data integrity check known as the *Message Integrity Code (MIC)*. The MIC is sometimes also referred to as the Message Integrity Check. The MIC is designed to defeat bit-flipping and forgery attacks that are used against WEP.

TKIP Countermeasures Because of the design constraints of the TKIP MIC, it is still possible for an adversary to compromise message integrity; therefore, TKIP also implements countermeasures. The countermeasures bound the probability of a successful forgery and the amount of information an attacker can learn about a key.

Figure 3.6 shows the TKIP encryption and data integrity process. It will be helpful to refer to this figure as you read about the steps TKIP performs.

TKIP starts with a 128-bit temporal key. An often-asked question is "Where does the 128-bit temporal key come from?" The answer is that the 128-bit temporal key is a dynamically generated key that comes from a 4-Way Handshake creation process. The 128-bit temporal key can either be a *pairwise transient key (PTK)* used to encrypt unicast traffic or a *group temporal key (GTK)* used to encrypt broadcast and multicast traffic. The creation of these dynamic temporal keys is discussed in great detail in Chapter 5.

After the appropriate 128-bit temporal key (pairwise or group) is created, the two-phase key-mixing process begins. A 48-bit TKIP sequence counter (TSC) is generated and broken into 6 octets labeled TSC0 (least significant octet) through TSC5 (most significant octet). Phase 1 key mixing combines the 128-bit temporal key (TK) with the TSC2 through TSC5 octets of the TKIP sequence counter (TSC) as well as the *transmit address (TA)*. The TA is the MAC address of the transmitting 802.11 radio. The output of the Phase 1 key mixing is the creation of the *TKIP-mixed transmit address and key (TTAK)*.

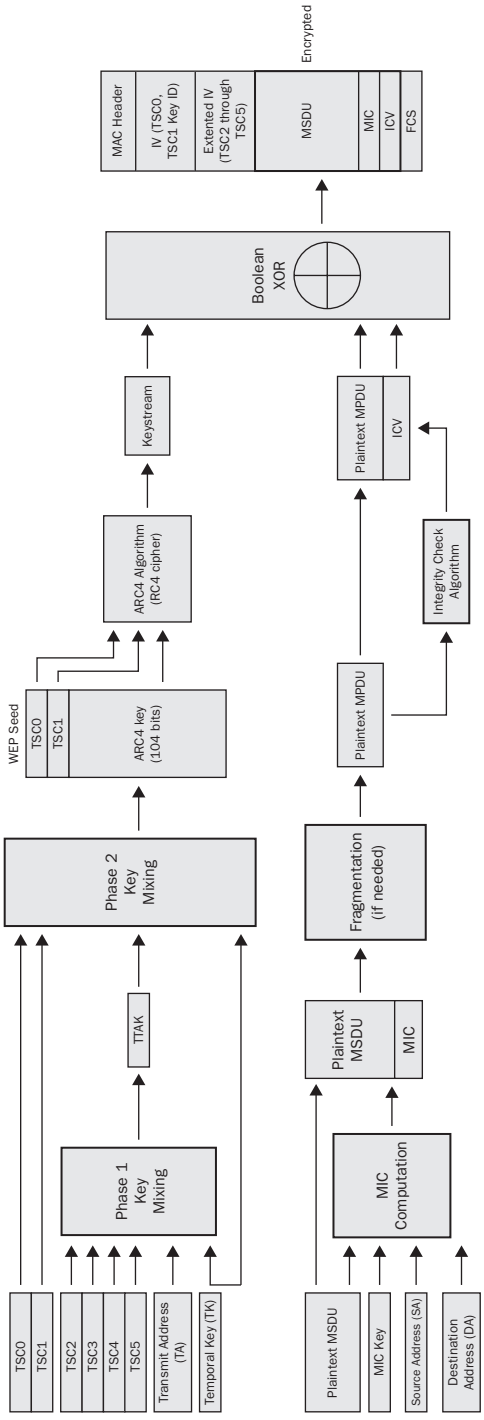
After the TTAK is generated, the Phase 2 key mixing can begin. Phase 2 key mixing combines the TTAK with the TSC0 and TSC1 octets of the TKIP sequence counter (TSC) with the 128-bit temporal key (TK). The output of the Phase 2 key mixing is referred to as the WEP seed. This WEP seed is then run through the ARC4 algorithm, and the keystream is created. The WEP seed is represented as a WEP Initialization Vector (IV) and 104-bit WEP key when fed into the ARC4 algorithm. You may often hear TKIP referenced as using a 48-bit IV. During the Phase 2 key mixing process, TKIP encodes the TSC value from the sender as a WEP IV and an extended IV. The encoding of the 48 bit TKIP sequence counter (TSC) effectively creates a 48-bit IV.

The two-phase key-mixing process can be summarized as follows:

- TTAK = Phase 1 (TK, TA, TSC)
- WEP seed = Phase 2 (TTAK, TK, TSC)

TKIP uses a stronger data integrity check known as the Message Integrity Code (MIC) to mitigate known forgery attacks against WEP. The MIC is often referred to by its nickname of Michael. The MIC can be used to defeat bit-flipping attacks, fragmentation

FIGURE 3.6 TKIP encryption and data integrity process



attacks, redirection, and impersonation attacks. The MIC is computed using the destination address (DA), source address (SA), MSDU priority, and the entire unencrypted MSDU plaintext data. After the MIC is generated, it is appended the end of the MSDU payload. The MIC is 8 octets in size and is labeled individually as M0 through M7. The MIC contains only 20 bits of effective security strength, making it somewhat vulnerable to brute-force attacks. Because the MIC only provides weak protection against active attacks, the 802.11-2007 standard defines *TKIP countermeasures* procedures. The TKIP countermeasures include the following:

Logging MIC failure would indicate an active attack that should be logged. MIC failure events can then be followed up by a system administrator.

60 Second Shutdown If two MIC failures occur within 60 seconds of each other, the STA or AP must disable all reception of TKIP frames for 60 seconds. This shutdown method theoretically provides a risk of a denial-of-service (DoS) attack. In reality, there are much easier ways to perform DoS attacks.

New Temporal Keys As an additional security feature, the PTK and (in the case of the Authenticator) the GTK should be changed.

The TKIP MIC augments, but does not replace, the WEP ICV. Because the TKIP MIC is still considered weak, TKIP protects the MIC with encryption, which makes TKIP MIC forgeries more difficult. The WEP ICV helps prevent false detection of MIC failures that would cause the countermeasures to be invoked.

After the MIC is created and appended to the plaintext MSDU, the 802.11 MAC performs its normal processing on this MSDU. If fragmentation is enabled, it is possible that this could be broken up into one or more MPDUs. It is even possible for the MIC to wind up split between two MPDUs. To keep things simple, we will assume that only one MPDU is created. An integrity check is performed on the plaintext MPDU, and the WEP integrity check value (ICV) is then appended to the MPDU. A Boolean XOR is then performed on the keystream and the MPDU/ICV to generate the encrypted payload. A *frame check sequence (FCS)* is calculated over all the fields of the header and entire frame body. The resulting 32-bit CRC is then placed in the FCS field.

Before verifying the MIC, a receiving 802.11 STA will check the FCS, ICV, and TSC of all MPDUs. Any MPDU that has an invalid FCS, an incorrect ICV, or a TSC value that is less than or equal to the TSC replay counter is dropped before checking the MIC. This avoids unnecessary MIC failure events. Checking the TSC before the MIC makes countermeasure-based DoS attacks harder to perform. Checking the TSC also protects against replay/injection attacks. Although considered weak for data integrity protection, the ICV also offers some error detection. If the MPDU is corrupted by multipath interference or collisions, the FCS fails and the entire MPDU must be retransmitted. After the FCS, ICV, and TSC are checked, the MIC is used for verification of data integrity.

Real World Scenario

What is the Difference Between TKIP and CKIP?

Prior to the ratification of the 802.11i security amendment in 2004, WLAN vendor Cisco Systems offered a prestandard proprietary version of TKIP called the *Cisco Key Integrity Protocol (CKIP)*. Cisco's proprietary enhancement of WEP also used temporal keys and a key-mixing process. A *Cisco Message Integrity Check (CMIC)* used for data integrity was designed to detect forgery attacks. Because of the extra overhead created, the CMIC was optional when CKIP was used as the encryption method. It should be noted that CKIP and CMIC only worked within a Cisco WLAN infrastructure due to the proprietary nature of the protocols. It should also be noted that the MIC is required when using the standard version of TKIP. In either case, whenever possible, a full upgrade to hardware that supports the stronger CCMP/AES encryption is highly recommended.

TKIP MPDU

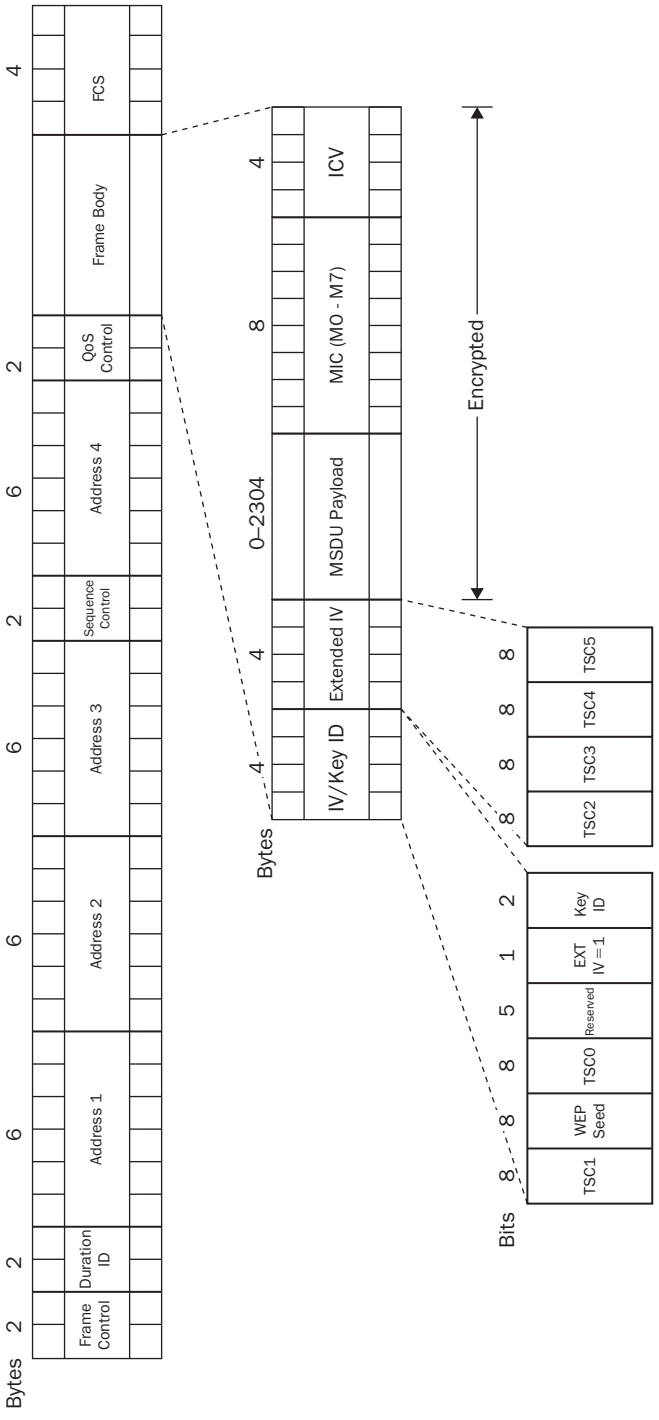
Figure 3.7 shows the TKIP MPDU. The first 32 bytes are the 802.11 MAC header, which does not change. The encrypted frame body is made up of five key pieces:

- IV/Key ID
- Extended IV
- MSDU payload
- MIC
- ICV

It begins with the IV/Key ID combination. This is 4 octets in size and is similar to the IV/KEY ID that is found in WEP. TSC0 and TSC1, the first two octets of the 48-bit TKIP sequence counter (TSC0 and TSC1), make up part of the IV/Key ID. If TKIP is being used, which is the case in this example, the Extended IV field is set to 1, indicating that an extended IV of 4 octets will follow the original IV. The Extended IV is 4 octets and is made up of the other 4 octets of the 48-bit TKIP sequence counter (TSC2 through TSC5). Both the original IV and the Extended IV are not encrypted. The 8 bytes that comprise the IV/Key ID and Extended IV could be considered a TKIP header.

After the original IV and the Extended IV comes the MSDU payload, followed by the 8 MIC octets, which is then followed by the 32-bit Integrity Check Value (ICV) that was calculated on the MPDU. The MSDU upper-layer payload as well as the MIC and ICV are all encrypted. The frame is then completed by adding the 32-bit frame check sequence (FCS) that is calculated over all the fields of the header and frame body.

FIGURE 3.7 TKIP MPDU



Because of the extra overhead from the IV (4 bytes), Extended IV (4 bytes), MIC (8 bytes), and ICV (4 bytes), a total of 20 bytes of overhead is added to the frame body of a TKIP encrypted 802.11 data frame. When TKIP is enabled, the entire size of the frame body inside an MPDU is expanded by 20 bytes to a maximum of 2,324 bytes. In other words, TKIP encryption adds 20 bytes of overhead to an 802.11 MPDU.

EXERCISE 3.1

TKIP Encrypted Frames

In this exercise, you will use a protocol analyzer to view 802.11 data frames encrypted with TKIP. The following directions should assist you with the installation and use of WildPackets' OmniPeek protocol analyzer demo software. If you have already installed OmniPeek, you can skip steps 1–5.

1. In your web browser, enter the following URL: `www.wildpackets.com/support/downloads`.
2. Under Product Evals, choose OmniPeek Professional. Fill out the OmniPeek evaluation request. A WildPackets representative will send an email message with a private download URL.
3. Proceed to the private download URL. Download the OmniPeek Professional demo software to your desktop using FTP. This evaluation copy of OmniPeek will be licensed to work for 30 days. Write down the evaluation copy license serial number.
4. Double-click the installation file `omnp602.exe`, and follow the installation prompts. You will need to be connected to the Internet to activate the license. You will be asked to enter the evaluation copy serial number.
5. This exercise will use frame captures that are on the CD that comes with this book. If you would like to use OmniPeek for live captures, you will need to install the proper drivers for your Wi-Fi radio card. Verify that you have a supported Wi-Fi card. Information about the supported drivers can be found at `www.wildpackets.com/support/downloads/drivers`. Review the system requirements and supported operating systems.
6. In Windows, choose Start ➢ Programs ➢ WildPackets OmniPeek, and then click the OmniPeek icon. The OmniPeek application should appear.
7. Click the Open Capture File icon and browse the book's CD. Open the packet capture file called `TKIP_FRAMES.PCAP`.
8. If you double-click on one of the 802.11 TKIP data packets (listed in the Protocol column), OmniPeek will open the packet in a new tabbed window. Scroll down to look at the different section of the frame and the different fields.
9. If you double-click on one of the beacons with the source address of 00:1A:1E:94:4C:31, OmniPeek will open the beacon frame in a new tabbed window. Scroll down to the WPA section, and you will see the cipher TKIP listed.

CCMP

Counter Mode with Cipher-Block Chaining Message Authentication Code Protocol (CCMP) is the security protocol that was created as part of the 802.11i security amendment and was designed to replace TKIP and WEP. CCMP uses the AES block cipher instead of the RC4 streaming cipher used by WEP and TKIP. As mentioned earlier, the IEEE 802.11-2007 standard defines two RSNA data confidentiality and integrity protocols: TKIP and CCMP, with CCMP support mandatory. CCMP is mandatory for robust security network (RSN) compliance. In September 2004, the Wi-Fi Alliance introduced version 2 of the Wi-Fi Protected Access certification, called *WPA2,* which requires the use of CCMP/AES encryption. Because the AES cipher is processor-intensive, older legacy 802.11 devices that only supported WEP and TKIP in most cases had to be replaced with newer hardware to support CCMP/AES encryption processing.

CCMP is made up of many components that provide different functions. Before going any further in this section, there are numerous acronyms and abbreviations relating to CCMP to which you need to be introduced. These acronyms and abbreviations are commonly used in the wireless industry and in the IEEE 802.11-2007 standard. Since CCMP is made up of many different components, it is common to reference the components individually. *CounterMode* is often represented as *CTR*. The CTR is used to provide data confidentiality. The acronym for *Cipher-Block Chaining* is *CBC*. You should also be familiar with *CBC-MAC,* which is the acronym for *Cipher-Block Chaining Message Authentication Code*. The CBC-MAC is used for authentication and integrity.

The full phrase of Counter Mode with Cipher-Block Chaining Message Authentication Code Protocol is represented by the acronym of CCMP. However, the shorter phrase of CTR with CBC-MAC is also sometimes represented by the CCMP acronym.

Some references to CCMP leave off the letter P and use the term, *CCM*, when referencing the block cipher and not the actual protocol. CCMP is based on the CCM of the AES encryption algorithm. CCM combines CTR to provide data confidentiality and CBC-MAC for authentication and integrity. In much simpler words, the CCM process uses the same key for encrypting the MSDU payload and provides for a cryptographic integrity check. The integrity check is used to provide data integrity for both the MSDU data and portions of the MAC header of the MPDU.

CCM is used with the AES block cipher. Although it is capable of using different key sizes, when implemented as part of the CCMP encryption method, AES uses a 128-bit key and encrypts the data in 128-bit blocks.

The inputs used by the CCMP encryption/data integrity process include:

Temporal Keys Just like TKIP, CCMP starts with a 128-bit temporal key. The 128-bit temporal key can either be a pairwise transient key (PTK) used to encrypt unicast traffic or a group temporal key (GTK) used to encrypt broadcast and multicast traffic.

Packet Number The 48-bit packet number (PN) is much like a TKIP sequence number. The PN uniquely identifies the frame and is incremented with each frame transmission. This protects CCMP from replay and injection attacks.

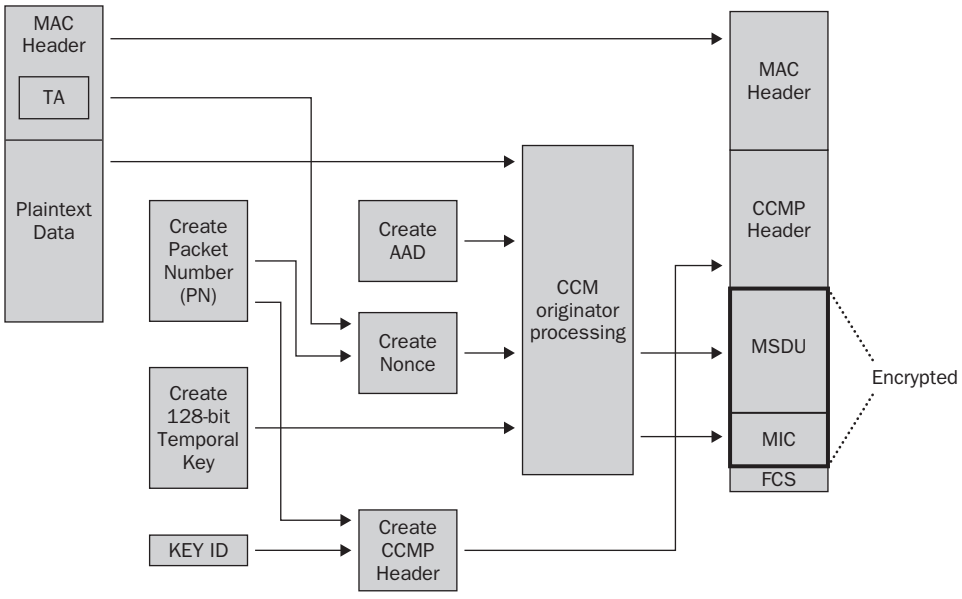
Nonce A *nonce* is a random numerical value that is generated one time only. A 104-bit unique nonce is constructed from the packet number (PN), priority data used in QoS, and the transmitter address (TA). Do not confuse this nonce with the nonces used during the 4-Way Handshake process described in Chapter 5.

802.11 data frame (MPDU) The frame body encapsulates the MSDU upper-layer payload that will be encrypted and protected by a Message Integrity Code (MIC). The MPDU header, also known as the MAC header, will not be encrypted but is partially protected by the MIC.

AAD *Additional authentication data (AAD)* is constructed from portions of the MPDU header. This information is used for data integrity of portions of the MAC header. Receiving stations can then validate the integrity of these MAC header fields.

Figure 3.8 shows the CCMP encryption and data integrity process. It will be helpful to refer to this figure as you read about the steps CCMP performs.

FIGURE 3.8 CCMP encryption and data integrity process



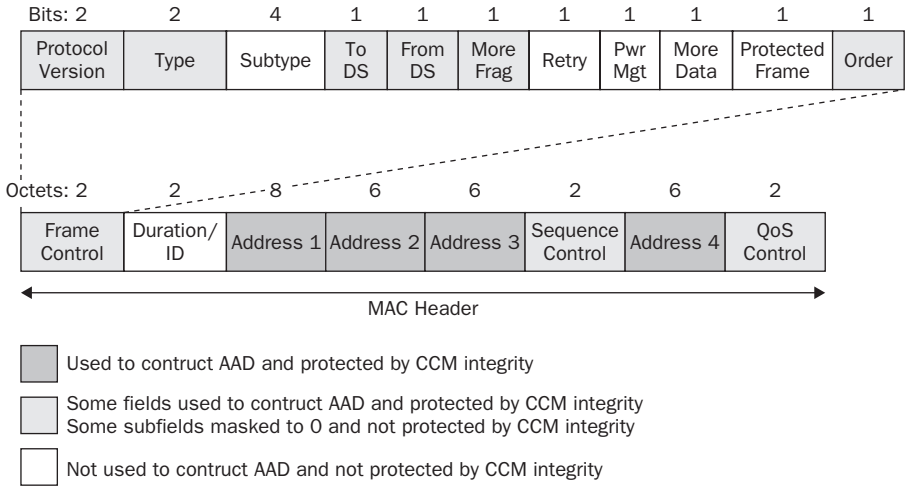
CCMP encrypts the payload of a plaintext MPDU using the following steps:

1. A 48-bit packet number (PN) is created. Packet numbers increment with each individual MPDU, although they remain the same for retransmissions.
2. As shown in Figure 3.9, certain fields in the MPDU header are used to construct the additional authentication data (AAD). The MIC provides integrity protection for these fields in the MAC header as well as for the frame body. All of the MAC addresses, including the BSSID, are protected. Portions of the other fields of the MAC header are also protected. Receiving stations will validate the integrity of these protected portions of the MAC header. For example, the frame type and the distribution bits that are subfields of the Frame Control field are protected. Receiving stations will validate the

integrity of these protected portions of the MAC header. The AAD does not include the header Duration field, because the Duration field value can change due to normal IEEE 802.11 operation. For similar reasons, several subfields in the Frame Control field, the Sequence Control field, and the QoS Control field are masked to 0 and therefore are not protected. For example, the Retry bit and Power Management bits are also masked and are not protected by CCM integrity.

3. A nonce is created from the packet number (PN), the transmitter address (TA), and priority data used in QoS.
4. The 8-octet CCMP header is constructed. The CCMP header includes the Key ID and the packet (PN), which is divided into 6 octets. You will notice that the construction of the CCMP header is basically identical to the 8-octet TKIP header.
5. The CCM module, which uses the AES clock cipher, will now be used to create a data integrity check and encrypt the upper-layer data. The 128-bit temporal key, the nonce, the AAD, and the plaintext data are then processed to create an 8-byte MIC. The MSDU payload of the frame body and the MIC are then encrypted in 128-bit blocks. This process is known as CCM originator processing.
6. The original MAC header is appended to the CCMP header, the encrypted MSDU, and the encrypted MIC. A frame check sequence (FCS) is calculated over all of the fields of the header and entire frame body. The resulting 32-bit CRC is then placed in the FCS field.

FIGURE 3.9 Additional authentication data (AAD)



CCMP MPDU

Figure 3.10 shows the CCMP MPDU. The first 32 bytes are the 802.11 MAC header, which does not change. The frame body consists of the CCMP header, the MSDU upper-layer payload, and the MIC. The CCMP header includes the Key ID and the packet (PN), which is divided into 6 octets. You will notice that the format of the CCMP

header is basically identical to the format of the 8-octet TKIP header (IV/Extended IV). The CCMP header is not encrypted. The MSDU payload and the 8-byte MIC are encrypted.

The overhead that results from CCMP encryption includes CCMP header (8 bytes) and the MIC (8 bytes). When CCMP is enabled, the entire size of the frame body inside an MPDU is expanded by 16 bytes to a maximum of 2,320 bytes. In other words, CCMP encryption adds 16 bytes of overhead to an 802.11 MPDU.

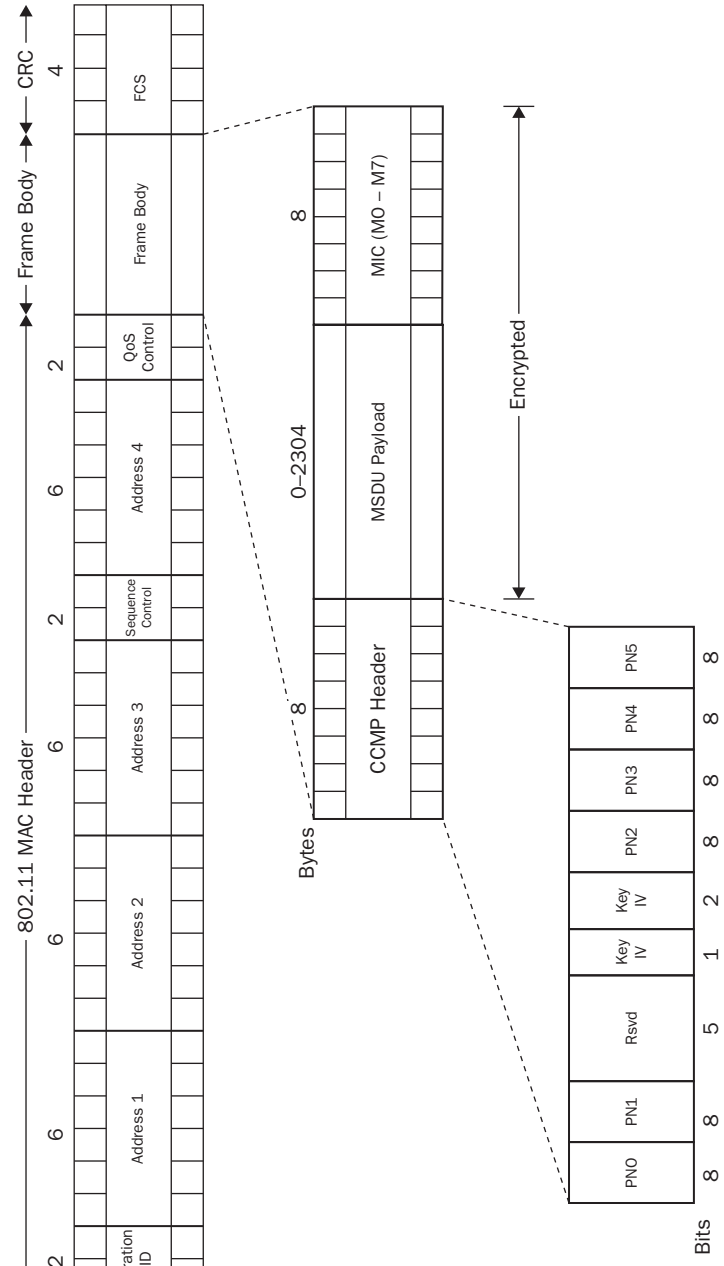
EXERCISE 3.2

CCMP Encrypted Frames

In this exercise, you will use a protocol analyzer to view 802.11 data frames encrypted with CCMP. The following directions should assist you with the installation and use of WildPackets' OmniPeek protocol analyzer demo software. If you have already installed OmniPeek, you can skip steps 1–5.

1. In your web browser, enter the following URL: `www.wildpackets.com/support/downloads`.
2. Under Product Evals, choose OmniPeek Professional. Fill out the OmniPeek evaluation request. A WildPackets representative will send an email message with a private download URL.
3. Proceed to the private download URL. Download the OmniPeek Professional demo software to your desktop using FTP. This evaluation copy of OmniPeek will be licensed to work for 30 days. Write down the evaluation copy license serial number.
4. Double-click the installation file `omnp602.exe`, and follow the installation prompts. You will need to be connected to the Internet to activate the license. You will be asked to enter the evaluation copy serial number.
5. This exercise will use frame captures that are on the CD that comes with this book. If you would like to use OmniPeek for live captures, you will need to install the proper drivers for your Wi-Fi radio card. Verify that you have a supported Wi-Fi card. Information about the supported drivers can be found at `www.wildpackets.com/support/downloads/drivers`. Review the system requirements and supported operating systems.
6. From Windows, choose Start ➢ Programs ➢ WildPackets OmniPeek, and then click the OmniPeek icon. The OmniPeek application should appear.
7. Click the Open Capture File icon and browse the book's CD. Open the packet capture file called `CCMP_FRAMES.PCAP`.
8. If you double-click on one of the beacons with the source address of 00:1A:1E:94:4C:32, OmniPeek will open the beacon frame in a new tabbed window. Scroll down to the RSN section, and you will see the cipher CCMP listed.
9. If you double-click on one of the 802.11 TKIP Data packets (listed in the Protocol column), OmniPeek will open the packet in a new tabbed window. Scroll down to look at the different sections of the frame and the different fields. Even though the frames are actually encrypted using CCMP, due to the similar frame structure OmniPeek displays them as TKIP data packets.

FIGURE 3.10 CCMP MPDU



Real World Scenario

Why Does the WLAN Protocol Analyzer Display CCMP Encrypted Data Frames as TKIP Encrypted Data Packets?

As you have already learned, the format of the 8-byte CCMP header is basically identical to the format of the 8-byte TKIP header (IV/Extended IV) used by TKIP. Therefore, most protocol analyzers cannot distinguish between TKIP-encrypted data frames and CCMP-encrypted data frames. However, you can always determine which cipher is being used by looking at a field called the *RSN information element*. The RSN information element is found in four different 802.11 management frames: beacon management frames, probe response frames, association request frames, and reassociation request frames. More information about the RSN information element can be found in Chapters 5 and 7.

WPA/WPA2

Prior to the ratification of the 802.11i amendment, the Wi-Fi Alliance introduced the Wi-Fi Protected Access (WPA) certification. WPA was a snapshot of the not-yet-released 802.11i amendment, but only supporting TKIP/RC4 dynamic encryption key generation. 802.1X/EAP authentication was required in the enterprise, and passphrase authentication was required in a SOHO environment. TKIP was designed as a stopgap measure, with a limited lifespan (5 years), until 802.11i was finalized. Recently, numerous publicly announced attacks have shown that there are flaws in TKIP and that it is able to be exploited. The Beck-Tews attack can recover plaintext from an encrypted short packet, recover the MIC key, and inject forged frames. However, the attack has a limitation in that the targets are restricted to WPA implementations that support WMM QoS features. The Ohiagi/Morii attack further enhances the Beck-Tews attack with a man-in-the-middle-approach. It should be noted that these attacks do not recover the encryption key but instead are used to recover the MIC checksum used for packet integrity.

These exploits can usually be prevented by changing TKIP settings as keying intervals on a WLAN controller or AP. The better solution is to stop using TKIP and upgrade to CCMP with AES. TKIP has begun to show its flaws, and more will certainly be exposed in the future. TKIP has provided WLAN data privacy for more than the five years for which it was intended. WLANs should now be protected with CCMP to provide the necessary data privacy and data integrity.

The further migration from TKIP to CCMP can be seen in the IEEE 802.11n amendment, which states that *High Throughput (HT)* stations should not use WEP or TKIP when communicating with other stations that support stronger ciphers. The IEEE states that an HT station should not use pre-RSNA security methods to protect unicast frames if the receiver address (RA) or address 1 of the frame corresponds to another HT

station. The Wi-Fi Alliance also began requiring that all HT radios not use TKIP when using HT data rates. Starting on September 1, 2009, the Wi-Fi Alliance began testing 802.11n APs and client STAs for compliance with this requirement. Most likely, the WLAN vendors will still offer support for TKIP and WEP with HT rates, but the use of TKIP and WEP will not be a default setting.

WPA2 is a Wi-Fi Alliance certification that is a mirror of the IEEE 802.11i security amendment. Testing of WPA2 interoperability certification began in September 2004. WPA2 incorporates the AES algorithm in CCMP, providing government-grade security based on the NIST FIPS 140-2 compliant AES encryption algorithm. WPA2 supports 802.1X/EAP authentication or pre-shared keys, and is backward-compatible with WPA.

Proprietary Layer 2 Implementations

In addition to the security and encryption standards, it is important to mention that there are also vendor-specific products that provide authentication and encryption for WLANs. Since these vendor-specific products are based on industry standard security and authentication technologies, they are better referred to as proprietary implementations rather than as proprietary solutions. These proprietary implementations require the installation of custom supplicant software on the client, which then utilizes authentication and encryption standards to communicate with the authenticator and authentication server on the network. The proprietary implementations historically provide higher levels of security than is found on a typical 802.11 network. These products are typically designed and marketed to organizations that need extremely high levels of security, usually government and military agencies. Most proprietary products are FIPS 140-2 compliant and incorporate standards such as AES 128, 192, and 256.

xSec is a Layer 2 protocol that provides a unified framework for securing both wired and wireless connections. xSec was jointly developed by Aruba Networks and Funk Software, a division of Juniper Networks. xSec implements a FIPS-compliant mechanism for providing identity-based security. xSec uses the AES-CBC-256 with HMAC-SHA1 algorithim, which provides for a 256-bit encryption key and even stronger data integrity. It is based on the IEEE 802.1X framework and supports many versions of EAP. xSec provides an extremely secure connection from the client, through the access point, all the way to an Aruba Networks WLAN controller.

Fortress Technologies also uses proprietary client software to enable secure communications between the wireless device and the Fortress Technologies controller or bridge, which is either connected to the wired network or providing wireless backhaul. The Fortress Technologies solution also uses proprietary Fortress encryption that can use a 256-bit encryption key and stronger data integrity.

You can find more information about xSec at `www.arubanetworks.com`. Learn more about Fortress encryption at `www.fortresstech.com`.

Summary

In this chapter, you learned about five different encryption ciphers: RC4, RC5, DES, 3DES, and AES. We discussed how symmetric and asymmetric algorithms function, as well as how stream and block ciphers are used to process plaintext data into ciphertext. We also covered the three different encryption technologies that are used in the 802.11 standard:

- WEP uses a 24-bit IV and a static key as the seed that is fed through the ARC4 algorithm to generate a keystream. The keystream is combined with the plaintext data bits to create the ciphertext. The ICV is calculated and appended as the data integrity check.
- TKIP uses a 128 bit temporal key + 48-bit TSC + TA address as the seeding material mixed together in the two-phase key-mixing process. The seed is then fed through the ARC4 algorithm to generate the keystream that is combined with the plaintext data bits to create the ciphertext. The MIC is also calculated and added as the data integrity check.
- CCMP uses a 128-bit temporal key + the AAD + a nonce as the seed for the AES block cipher. No key mixing is needed due to the strength of the AES algorithm. Data is encrypted in 128-bit blocks. A MIC is also calculated and added for integrity. The CCMP MIC is stronger than the TKIP MIC.

The frame formats of each of these encryption technologies were reviewed. The relationship between the Wi-Fi Alliance certifications (WPA/WPA2) and the 802.11 encryption technologies was also discussed.

Exam Essentials

Know the two categories of algorithms. Understand the differences between symmetric and asymmetric algorithms, and how they are used when encrypting and decrypting data.

Know the process of how public key and private key encryption works. Understand that the public key is available to anyone and is used to encrypt the data, whereas the private key is kept secret and is used to decrypt the data.

Describe stream and block ciphers. Explain the process used by stream and block ciphers to encrypt the plaintext, along with how a Boolean XOR is incorporated in the process.

Define RC4, RC5, DES, 3DES, and AES. Be able to explain the differences and similarities of all five of these algorithms.

Define WEP, TKIP, and CCMP. Be able to explain the differences and similarities between these three security protocols. Understand the individual encryption and data integrity processes associated with each security protocol.

Describe the frame MPDU format. Explain the differences and similarities between the MPDU frame formats of the three 802.11 security protocols. Explain why the frame sizes vary and which portions of the frame are actually encrypted.

Explain the relationship between WPA/WPA2 and 802.11. Understand how the 802.11 standard relates to the Wi-Fi Alliance certification. Know which 802.11 security protocols are required for the Wi-Fi Alliance certifications.

Key Terms

Before you take the exam, be certain you are familiar with the following terms:

4-Way Handshake

additional authentication data (AAD)

Advanced Encryption Standard (AES)

ARC4

Arcfour

asymmetric algorithm

Bit

block cipher

blocks

brute force attacks

CBC

CBC-MAC

CCM

cipher

Cipher-Block Chaining

Cipher-Block Chaining Message Authentication Code

ciphertext

Cisco Key Integrity Protocol (CKIP)

Cisco Message Integrity Check (CMIC)

Counter Mode with Cipher-Block Chaining Message Authentication Code Protocol (CCMP)

CounterMode

CTR

cyclic redundancy check (CRC)

Data Encryption Standard (DES)

Exclusive-OR (XOR)

Federal Information Processing Standards (FIPS)

frame check sequence (FCS)

group temporal key (GTK)

High Throughput (HT)

Initialization Vector (IV)

Integrity Check Value (ICV)

keystream

MAC Protocol Data Unit (MPDU)

MAC Service Data Unit (MSDU)

Message Integrity Code (MIC)

National Institute of Standards and Technologies (NIST)

nonce

octet

pairwise transient key (PTK)

plaintext

private key

public key

public key infrastructure (PKI)

RC4

RC5

Rijndael

robust security network (RSN)

round function

RSN information element

state

stream cipher

symmetric algorithm

Temporal Key Integrity Protocol (TKIP)

TKIP countermeasures

TKIP sequence counter (TSC)

TKIP-mixed transmit address and key (TTAK)

transmit address (TA)

Triple Data Encryption Algorithm (TDEA)

Triple DES (3DES)

Wi-Fi Protected Access (WPA)

Wired Equivalent Privacy (WEP)

WPA2

xSec

Review Questions

1. CCMP/AES encryption adds an extra _____ of overhead to the body of an 802.11 data frame.
   - **A.** 16 bytes
   - **B.** 12 bytes
   - **C.** 20 bytes
   - **D.** 10 bytes
   - **E.** None of the above

2. TKIP/RC4 encryption adds an extra _____ of overhead to the body of an 802.11 MPDU.
   - **A.** 16 bytes
   - **B.** 12 bytes
   - **C.** 20 bytes
   - **D.** 10 bytes
   - **E.** None of the above

3. An HT client STA is transmitting to an HT AP using modulation and coding scheme (MCS) #12 that defines 16-QAM modulation, two spatial streams, a 40-MHz bonded channel and an 800 ns guard interval to achieve a data rate of 162 Mbps. According to the IEEE, which types of encryption should be used by the HT client STA? (Choose all that apply.)
   - **A.** Static WEP
   - **B.** Dynamic WEP
   - **C.** TKIP/RC4
   - **D.** CCMP/AES
   - **E.** All of the above

4. CCMP/AES uses a _____ temporal key and encrypts data in _____ blocks.
   - **A.** 128-bit, 128-bit
   - **B.** 128-bit, 192-bit
   - **C.** 192-bit, 192-bit
   - **D.** 192-bit, 256-bit
   - **E.** 256-bit, 256-bit

5. Which of these temporal keys are used by TKIP/RC4 encryption? (Choose all that apply.)
   - **A.** PMK
   - **B.** PTK
   - **C.** GTK
   - **D.** GMK
   - **E.** 256-bit, 256-bit

6. Andy calls the help desk for assistance with sending an encrypted message to Chris. Without knowing what type of security protocol and encryption Andy and Chris are using, which of the answers here could make the following scenario true?

   In order for Andy to send an encrypted message successfully to Chris, Andy is told to enter _____ on his computer; Chris needs to enter _____ on his computer. (Choose all that apply.)
   - **A.** a public key, the companion private key
   - **B.** a private key, the companion public key
   - **C.** an asymmetric key, the same asymmetric key
   - **D.** a symmetric key, the same symmetric key

7. The TKIP MIC is used for data integrity. Which portions of an 802.11 MPDU does the TKIP MIC protect from being altered? (Choose all that apply.)
   - **A.** MSDU
   - **B.** SA
   - **C.** DA
   - **D.** TA
   - **E.** Frame Control field
   - **F.** MSDU priority bit

8. Given that CCMP uses a MIC for data integrity to protect the frame body and portions of the MAC header, what information needs to be constructed to protect certain fields in the MAC header?
   - **A.** Nonce
   - **B.** Extended IV
   - **C.** ICV
   - **D.** AAD
   - **E.** PN
   - **F.** IV

9. Which of the following is a FIPS encryption standard that uses a single 56-bit symmetric key? (Choose all that apply.)

A. RC4

B. RC5

C. DES

D. 3DES

E. AES

10. To protect against replay/injection attacks, TKIP uses _____. To protect against IV collisions and weak-key attacks, TKIP uses _____.

A. MIC, TSC

B. TSC, MIC

C. TSC, Key Mixing

D. RC4, Key Mixing

E. MIC, Key Mixing

11. When using TKIP encryption, the 48-bit TSC is generated and broken into TSC0 through TSC5. Which of the following are run through Phase 1 of the key-mixing process to generate the TTAK? (Choose all that apply.)

A. TSC0 and TSC1

B. TSC2 through TSC5

C. TSC0 through TSC5

D. Temporal key

E. Transmit address

12. Because the TKIP Message Integrity Check (MIC) is susceptible to brute-force attacks, which countermeasures does the 802.11-2007 standard define for further protection against active attacks against the MIC? (Choose all that apply.)

A. 60-second shutdown

B. CBC

C. CBC-MAC

D. Logging

E. Key refresh

13. Which of the following encryption methods use symmetric algorithms? (Choose all that apply.)

A. WEP

B. TKIP

C. Public-key cryptography

D. CCMP

14. The Rijndael algorithm was the foundation for which of the following ciphers?

A. TKIP

B. DES

C. AES

D. CCMP

E. 3DES

15. A data integrity check known as Message Integrity Code (MIC) is used by which of the following? (Choose all that apply.)

A. WEP

B. TKIP

C. CCMP

D. AES

E. DES

16. Given that additional authentication data (AAD) is constructed from portions of the MPDU header and that the information is used for data integrity, which fields of the MAC header comprise the AAD? (Choose all that apply.)

A. Frame Control field

B. Transmitter address

C. Sequence Control field

D. Receiver address

E. Destination address

F. BSSID

17. Which inputs are needed by Phase 2 of the TKIP mixing process? (Choose all that apply.)

A. SA

B. TTAK

C. Temporal key

D. MIC

E. TSC

F. TA

18. The CCMP header is made up of which of the following pieces? (Choose all that apply.)

A. PN

B. TTAK

C. TSC

D. Key ID

E. MIC

19. 3DES has effective key sizes of how many bits? (Choose all that apply.)

A. 56

B. 64

C. 112

D. 128

E. 168

F. 192

20. AES supports three key lengths of 128, 192, and 256. The number of rounds performed for AES-128 is _____, for AES-192 is _____, and for AES-256 is _____. (Choose all that apply.)

A. 8

B. 10

C. 12

D. 14

E. 16

Answers to Review Questions

1. A. CCMP/AES encryption will add an extra 16 bytes of overhead to the body of an 802.11 data frame. Eight bytes are added by the CCMP header and 8 bytes are added by the MIC. WEP encryption will add an extra 8 bytes of overhead to the body of an 802.11 data frame. When TKIP is implemented, because of the extra overhead from the extended IV and the MIC, a total of 20 bytes of overhead is added to the body of an 802.11 data frame.

2. C. When TKIP is implemented, because of the extra overhead from the extended IV and the MIC, a total of 20 bytes of overhead is added to the body of an 802.11 MPDU. CCMP/AES encryption will add an extra 16 bytes of overhead to the body of an 802.11 MPDU. WEP encryption will add an extra 8 bytes of overhead to the body of an 802.11 MPDU.

3. D. The IEEE 802.11n amendment states that an HT station should not use WEP or TKIP when communicating with other STAs that support stronger ciphers. HT STAs should not use pre-RSNA security methods to protect unicast frames if the RA or address 1 of the frame corresponds to an HT STA. On September 1, 2009, the Wi-Fi Alliance also began requiring that all HT radios not use TKIP when using HT data rates.

4. A. The AES algorithm is defined in FIPS PUB 197-2001. All AES processing used within CCMP uses AES with a 128-bit key and a 128-bit block size. Proprietary Layer 2 encryption methods, such as Fortress and xSec, can use stronger 192-bit and 256-bit encryption keys.

5. B, C. TKIP uses a two-phase mixing function to combine a 128-bit temporal key, the transmitter address (TA), and the TKIP sequence counter (TSC) as seeding material for the RC4 algorithm. The 128-bit temporal key is generated by the 4-Way Handshake process. Therefore, the temporal keys used by TKIP/RC4 are either a pairwise transient key (PTK) or a group temporal key (GTK).

6. A, D. When using asymmetric encryption, the message is encrypted with the public key and decrypted with the private key. An asymmetric encryption protocol uses different keys to encrypt the data and decrypt the data. A symmetric encryption protocol uses the same key to encrypt the data and decrypt the data.

7. A, B, C. TKIP uses a stronger data integrity check known as the Message Integrity Code (MIC) to mitigate known forgery attacks against WEP. The MIC is often referred to by its nickname of Michael. The MIC can be used to defeat bit-flipping attacks, fragmentation attacks, redirection, and impersonation attacks. The MIC is computed using the destination address (DA), source address (SA), MSDU Priority, and the entire unencrypted MSDU plaintext data. After the MIC is generated, it is appended to the end of the MSDU payload.

8. D. Additional Authentication Data (AAD) is constructed from portions of the MPDU header. This information is used for data integrity of portions of the MAC header. Receiving stations can then validate the integrity of these MAC header fields. The MIC protects the AAD information and the frame body for data integrity.

9. C. RC4 and RC5 were never FIPS encryption standards. 3DES is a FIPS encryption standard, but uses three keys with an effective key size of 168 bits. AES is a FIPS encryption standard with key sizes of 128, 192, and 256 bits.

10. C. TKIP uses a per-MPDU TKIP sequence counter (TSC) to sequence the MPDUs it sends. Sequencing is designed to defeat replay and reinjection attacks. TKIP also uses a complex two-phase cryptographic mixing process to create stronger seeding material for the RC4 cipher. The key-mixing process is designed to defeat the known IV collisions and weak-key attacks. TKIP uses a stronger data integrity check known as the Message Integrity Code (MIC). The MIC is designed to defeat bit-flipping and forgery attacks that are used against WEP.

11. B, D, E. The TKIP-mixed transmit address and key (TTAK) is generated by Phase 1 key mixing. It uses the 32 bits from the TKIP sequence counter (TSC) 2 through 5, the temporal key, and the transmit address.

12. A, D, E. A MIC failure would indicate an active attack that should be logged. MIC failure events can then be followed up by a system administrator. If two MIC failures occur within 60 seconds of each other, the STA or AP must disable all reception of TKIP frames for 60 seconds. As an additional security feature, new dynamic keys will be generated. The PTK and the GTK will be recreated.

13. A, B, D. WEP, TKIP, and CCMP use symmetric algorithms. WEP and TKIP use the RC4 algorithm. CCMP uses the AES cipher. Public-key cryptography is based on asymmetric communications.

14. C. AES is based on the Rijndael algorithm. CCMP is an encryption protocol that uses the AES cipher. TKIP uses the RC4. DES and 3DES are both block ciphers unrelated to Rijndael.

15. B, C. A stronger data integrity check known as a Message Integrity Code (MIC), or by its common name, Michael, was introduced with TKIP to correct some of the weaknesses in WEP. CCMP also uses a MIC. AES and DES are encryption algorithms and are not concerned with message integrity.

16. B, D, E, F. Certain fields in the MPDU header are used to construct the additional authentication data (AAD). The MIC provides integrity protection for these fields in the MAC header as well as in the frame body. All of the MAC addresses, including the BSSID, are protected. Portions of the other fields of the MAC header are also protected. Receiving stations will validate the integrity of these protected portions of the MAC header. For example, the frame type and the distribution bits, which are subfields of the Frame Control field, are protected. The AAD does not include the header Duration field, because the Duration field value can change due to normal IEEE 802.11 operation. For similar reasons, several subfields in the Frame Control field, the Sequence Control field, and the QoS Control field are masked to 0 and therefore not protected. For example, the Retry bit and Power Management bits are also masked and not protected by CCM integrity.

17. B, C, E. Phase 1 key mixing combines the appropriate temporal key (pairwise or group) with the TSC2 through TSC5 octets of the TKIP sequence counter as well as the transmit address (TA). The TA is the MAC address of the transmitting 802.11 radio. The output of the Phase 1 key mixing is the creation of the TKIP-mixed transmit address and key (TTAK). After the TTAK is generated, the Phase 2 key mixing can begin. Phase 2 key mixing combines the TTAK with the TSC0 and TSC1 octets of the TKIP sequence counter (TSC) with the 128-bit temporal key (TK). The output of the Phase 2 key mixing is referred to as the WEP seed. This WEP seed is then run through the ARC4 algorithm and the keystream is created.

18. A, D. The CCMP header includes the Key ID and the packet (PN), which is divided into 6 octets. The format of the CCMP header is basically identical to the format of the 8-octet TKIP header (IV/Extended IV). The CCMP header is not encrypted.

19. A, C, E. 3DES defines three keying options:

Keying Option 1 All three keys are unique.

Keying Option 2 K1 and K2 are unique, but K3 = K1.

Keying Option 3 All three keys are identical: K1 = K2 = K3.

Keying option 1 is the strongest, because all three keys are unique, giving it an effective key size of 168 bits. Keying option 3 is the weakest, and is essentially equal to very slow DES. Remember that with a symmetric algorithm, the same key that encrypts the data also decrypts the data. With 3DES, after the first pass with K1 encrypts the data, the second pass with K2 actually decrypts the data, and the third pass with K3 encrypts the data again. Keying option 2 provides an effective key size of 112 bits.

20. B, C, D. AES uses a block size of 128 bits, which is actually a 4 × 4 array of bytes, called a state. The number of rounds performed on the block varies depending on the key sizes. AES-128 performs 10 rounds, AES-192 performs 12 rounds, and AES-256 performs 14 rounds.

Chapter 4

Enterprise 802.11 Layer 2 Authentication Methods

IN THIS CHAPTER, YOU WILL LEARN ABOUT THE FOLLOWING:

- ✓ **WLAN authentication overview**
- ✓ **AAA**
  - Authentication
  - Authorization
  - Accounting
- ✓ **802.1X**
  - Supplicant
  - Authenticator
  - Authentication server
- ✓ **Supplicant credentials**
  - Usernames and passwords
  - Digital certificates and PACs
  - One-time passwords
  - Smart cards and USB tokens
  - Machine authentication
  - Preshared keys
  - Proximity badges and RFID tags
  - Biometrics

- ✓ **Authentication server credentials**
- ✓ **Shared secret**
- ✓ **Legacy authentication protocols**
  - PAP
  - CHAP
  - MSCHAP
  - MSCHAPv2
- ✓ **EAP**
  - Weak EAP protocols
  - EAP-MD5
  - EAP-LEAP
  - Strong EAP protocols
  - EAP-PEAP
  - EAP-TTLS
  - EAP-TLS
  - EAP-FAST
  - Miscellaneous EAP protocols
  - EAP-SIM
  - EAP-AKA

This chapter discusses the key concepts, components, and methods involved in WLAN authentication. You will learn about Authentication, Authorization, and Accounting (AAA), what roles are played in the authentication process, 802.1X, and all of the EAP methods you will encounter in the real world that will assist you in securing your enterprise WLAN. 802.1X/EAP authentication, in particular, can be a difficult topic to grasp. This chapter will describe how EAP authentication works within an 802.1X network access control framework when used in enterprise WLANs. As we introduce each topic, we will provide real-world examples and design principles to help solidify each major concept.

WLAN Authentication Overview

WLAN authentication, in all of its many flavors, is what needs to occur before an individual or a device is allowed to access network resources. Authentication is the verification of users' identity and credentials. Users must identify themselves and present credentials, such as usernames and passwords or digital certificates. Systems with higher levels of authentication use multifactor authentication, which requires at least two sets of different credentials to be presented. In a nutshell, authentication is based on *who* you are. Furthermore, *who* you are may indeed require more than one identifying element, but more on that later. After you successfully authenticate (via whatever method), encryption can then take place, but an important distinction must be made; authentication should be considered mutually exclusive from encryption. In Chapter 5, "802.11 Layer 2 Dynamic Encryption Key Generation," you will learn that the authentication process provides the seeding material to create the necessary encryption keys, but conceptually it is still a separate concept and process. While the encryption process is a by-product of the authentication process, understand that the goals of authentication and encryption are very different. Authentication provides mechanisms for validating user identity; encryption provides mechanisms for data privacy or confidentiality.

Since authentication requires proving who you are, you must present *credentials* that fall into three categories:

- Something you know
- Something you have
- Something you are

If multiple credentials are provided for validating identity, greater trust can be assigned to the identity of the party requesting access to the WLAN. Requiring multiple credentials to be presented for user validation is known as *multifactor authentication*. Requiring two sets of credentials to be presented for user validation is often called *two-factor authentication*. Some of the EAP authentication methods you will learn about in this chapter are capable of two-factor authentication.

For example, consider your bank debit card. When you insert your physical card (something you have) into the ATM machine, it then requests your PIN (something you know). Some banks even have a picture of the card owner imprinted on the card. The ATM machine can't verify that, but what about the cashier clerk at your local supermarket? It immediately tells the clerk that when you present the card that it is indeed yours (and not someone else's). The picture on the debit card immediately ties together for the clerk both something you *are* and something you *have*. If the debit card was used along with the PIN to complete a debit transaction and the clerk verifies your face with the picture identity on your card, three forms of credentials will have been used for authentication.

Biometrics, such as fingerprint, retina, and other biological verification methods, can also be used as *something you are* to prove your identity. Although biometrics are not usually employed in WLAN security authentication, it may indeed become common one day as biometric devices become more commonplace as built-in components of laptop computers. Even facial recognition, using the built-in video cameras in laptop displays, is being discussed as an additional form of authentication.

As these technologies develop, you can rest assured that yet another new authentication standard will emerge. The important thing to remember is that it will be just another authentication method using the principles presented in this chapter.

AAA

While we have already addressed authentication at a conceptual level, who or what is the one performing the authorization? Can we also have a record of this activity? In fact, how about having a record of when this authorization activity occurred, how long the user was on the network, where the user went, and if the user is either still online or has ended their session? *Authentication, authorization, and accounting (AAA)* is a common computer security concept that defines the protection of network resources.

As we have already discussed, *authentication* is the verification of user identity and credentials. Users must identify themselves and present credentials, such as usernames and passwords or digital certificates. More secure authentication systems use multifactor authentication, which requires at least two sets of different credentials to be presented.

Authorization involves granting access to network resources and services. Before authorization to network resources can be granted, proper authentication must occur.

Accounting is tracking the use of network resources by users. It is an important aspect of network security, used to keep a paper trail of who used what resource, when, and where. A record is kept of user identity, which resource was accessed, and at what time. Keeping an accounting trail is often a requirement of many industry regulations, such as the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Authentication

Let's discuss authentication in a more technical manner now. What can we take advantage of in order to prove the identity of someone wanting to gain access to your precious WLAN and, therefore, potentially all the data you consider secure? Answers to that question will vary depending on the level of concern over the access to that network and thus the data that resides on it. Understanding this concept is critical from a design perspective when you are being consulted to help an enterprise decide on how to best perform authentication.

The following are some common examples of authentication credentials used in enterprise WLANs today:

- Usernames and passwords
- Digital certificates
- Dynamic/One Time Passwords (for example, RSA SecurID)
- Smart cards or credentials stored on USB devices
- Machine authentication (based on an embedded machine identity)
- Preshared keys (PSK)

A bank system processing billions of dollars every second would have very different security concerns than a small company that sells, say, car tires. Both may consider their data secure, but there is additional cost and/or complexity in both deploying and operating stronger authentication types such as two- and three-factor authentication.

Two-factor authentication would function just as in our previous example where we are using the bank ATM with a debit card (first factor = something you have) and having to enter our PIN (second factor = something you know). A specific WLAN security example of two-factor authentication would be using a computer (a computer object) that is part of a Microsoft *Active Directory (AD)* and then having to use a Windows AD user account to log in from that computer. The purpose is to ensure access is only granted to your WLAN by being both from a valid and current AD computer and AD user account. For example, if you brought in your laptop from home that isn't known by AD, the entity performing the authorization will not let you on the network regardless of your valid AD user credentials because you are not accessing the network from a valid "enterprise asset."

Real World Scenario

Cost vs. Security

A warehouse company that requires a barcode system (which is only sending quantities and item numbers electronically) to operate over the WLAN has requested your expertise. The network the system will reside on already has access control mechanisms (firewalls and/or ACLs) that prevent access to any other network or device beyond where the barcode devices can communicate.

In your consultation with the IT director of the warehouse company, she has asked for the most secure method possible to be employed for the company's WLAN. She claims to have a large budget if necessary but has limited support staff. You also learn that the operators of the barcode devices have limited computer skills and will likely require a lot of training. Therefore, simplicity of security is a major requirement.

Every salesperson with a quota would cringe hearing this, but this is when it's time to balance cost and complexity. A two-factor authentication system would not be a good choice in this case because of the extra burden and cost involved in a high-end security infrastructure. Two-factor authentication systems would provide an unnecessary operational burden to the end users of the system and the technical staff as well.

People will typically opt to have their network secure as long as it does not become overly burdensome. However, at some level, the concern for security takes a front seat over the amount of burden an end user will have to endure to use the WLAN. In one of our previous examples, not only does the bank processing billions of dollars per second have concerns over the direct financial impact to the viability of its core business should somebody have access to manipulate this data, but there are also regulatory requirements such as PCI that dictate the minimum requirements to which the bank must adhere. Furthermore, there may also be trade secrets that could be gleaned from this data that competitors would want to access. Quite literally, a security breach of this network might mean the end of the bank's business. The bank scenario is an example of when multifactor authentication may be required regardless of the additional burden placed on the end users. Later in this chapter, all of the commonly used and available enterprise EAP authentication methods will be discussed in detail.

Authorization

When you log into your email account, you will likely enter a username and a password. Who is authorizing your username and password? This is conceptually the email

application server itself. The difference with WLAN security is that there are multiple applications being used via the WLAN portal, so some sort of overlay authorization solution is needed to validate user identity. An 802.11 WLAN normally serves as a portal to preexisting wired network resources, such as a corporate server farm. Authorization is about properly protecting network resources. Authorization allows authenticated users access to network resources, but users who cannot provide the proper authentication credentials will not be authorized. Authorization should be considered as a framework in which proper authentication can occur. Enterprise WLANs should use an 802.1X authorization framework.

In WLANs, a RADIUS server is typically the entity performing the authorization from the WLAN hardware's perspective. *Remote Authentication Dial-in User Service (RADIUS)* is a networking protocol that provides AAA capabilities for computers to connect to and use network services. RADIUS authentication and authorization is defined in IETF RFC 2865. Accounting is defined in IETF RFC 2866. RADIUS servers are sometimes referred to as AAA servers. While a RADIUS server may actually communicate with other systems like Windows Active Directory or an LDAP server, from the WLAN's perspective it is convenient to think of the RADIUS server as the single authorization entity. You will, in fact, find that many WLAN vendors are building RADIUS servers directly into their autonomous access points and WLAN controllers. This kind of feature is often useful in small networks desiring minimal infrastructure yet requiring strong WLAN security.

The IEEE 802.11-2007 standard does not dictate the use of a RADIUS server. However, the IEEE 802.11-2007 WLAN standard does dictate the use of the IEEE 802.1X-2004 standard for authentication and port control within an enterprise *robust security network (RSN)*. 802.1X is a *port-based access control* standard that defines the mechanisms necessary to authenticate and authorize devices to network resources. This was a clever and logical way for IEEE 802.11 designers to leverage the use of a preexisting and popular standards-based authorization method and inherit all its strengths and benefits. RADIUS servers are usually one of the main components of an 802.1X authorization framework.

The IEEE 802.1X-2004 Port-Based Network Access Control standard can be downloaded from this URL: `http://standards.ieee.org/getieee802/802.1.html`. Clause 8.45 of the IEEE 802.11-2007 WLAN standard defines how 802.1X mechanisms are used for authentication and port control within an 802.11 WLAN. These mechanisms will be described in detail in this chapter. Clause 8.48 of the IEEE 802.11-2007 WLAN standard defines how 802.11 and 802.1X mechanisms are used together to provide for robust secure key management. Key management and creation is discussed in great detail in Chapter 5.

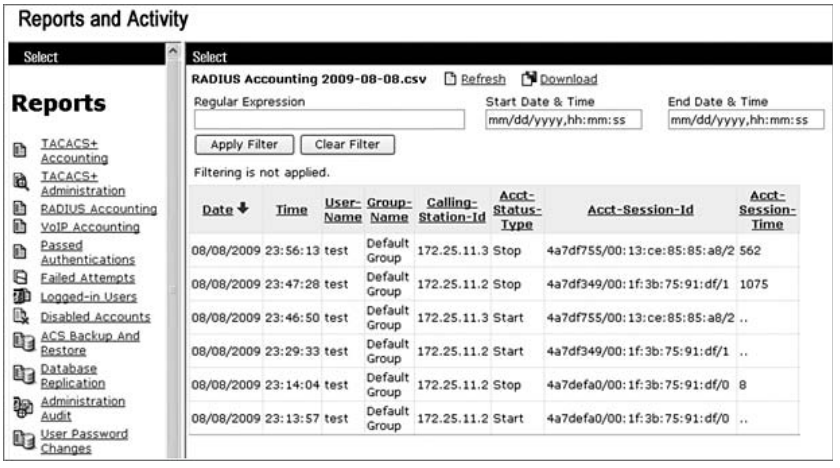
Accounting

When you purchase a gallon of milk from the supermarket with a check, there are many accounting records that are generated from this transaction. For example, if you wrote the check, it is always wise to write down the check number in your check ledger, as well as the date, merchant, and the amount of the check you just wrote. Better yet, much of the manual effort can be eliminated by using a checkbook with carbon copies. Next, the merchant will make their own accounting records and then the bank and so on. We can refer to this as the *accounting trail*.

An accounting trail is considered to be the Holy Grail if you are ever audited by the Internal Revenue Service (IRS), the United States government agency that ensures proper tax contributions. An IRS agent can follow the entire transaction from beginning to end with a proper accounting trail.

In the case of WLANs, an accounting record is also quite useful in security forensics in attempting to analyze a security breach or even when evaluating normal network activities. An accounting server will typically contain information such as the user account logged in, where it was logged in from (the actual AP or the controller), the time the transaction started, the amount of traffic sent and received by the user, when the user logged off, and so forth. Figure 4.1 shows an example of an accounting record from an accounting server.

FIGURE 4.1 Accounting trail



RADIUS accounting records typically contain the following elements at a minimum:

- Date
- Time

- Username
- RADIUS group
- Accounting status type
- Accounting session ID
- Accounting session time
- Service type
- Framed protocol
- Input octets
- Output octets
- Input packets
- Output packets
- Framed IP address
- NAS port
- NAS IP address
- Attribute value pairs

Vendors make use of their own *attribute value pairs (AVPs)* that can be captured by a RADIUS accounting service. Consult the manual for your particular RADIUS accounting system if there is other information not included in the standard reporting that you may want to have included.

Together, authentication, authorization, and accounting are commonly referred to as AAA. You will also find RADIUS servers typically referred to as AAA servers as most RADIUS servers perform the role of all three services. RADIUS accounting is defined in RFC 2866.

From a WLAN hardware device's perspective, the authentication and authorization is typically broken off separately in the device configuration from the accounting server.

802.1X

The IEEE 802.1X-2004 standard is not specifically a wireless standard and is often mistakenly referred to as 802.11x. As mentioned earlier, the 802.1X standard is a port-based access control standard. 802.1X provides an authorization framework that allows or disallows traffic to pass through a port and thereby access network resources. An 802.1X framework may be implemented in either a wireless or wired environment. The 802.1X authorization framework consists of three main components, each with a specific role. These three 802.1X components work together to make sure only properly validated users

and devices are authorized to access network resources. A Layer 2 authentication protocol called *Extensible Authentication Protocol (EAP)* is used within the 802.1X framework to validate users at Layer 2. EAP will be discussed in detail later in this chapter. The three major components of an 802.1X framework are as follows:

Supplicant A host with software that is requesting authentication and access to network resources. Each supplicant has unique authentication credentials that are verified by the authentication server. In a WLAN, the supplicant is often the laptop or wireless handheld device trying to access the network.

Authenticator A device that blocks or allows traffic to pass through its port entity. Authentication traffic is normally allowed to pass through the authenticator, while all other traffic is blocked until the identity of the supplicant has been verified. The authenticator maintains two virtual ports: an *uncontrolled port* and a *controlled port*. The uncontrolled port allows EAP authentication traffic to pass through, while the controlled port blocks all other traffic until the supplicant has been authenticated. In a WLAN, the authenticator is usually either an AP or a WLAN controller.

Authentication Server A server that validates the credentials of the supplicant that is requesting access and notifies the authenticator that the supplicant has been authorized. The authentication server will maintain a user database or may proxy with one or more external user databases to authenticate supplicant credentials.

You will see this terminology repeatedly over the course of your reading and hands-on work in WLAN security both inside this study guide and throughout industry publications. Each of these 802.1X components will now be discussed in further detail in the sections that follow.

Supplicant

The *supplicant* is the device that will need to be validated by the authentication server before being allowed access to network resources. The supplicant will use an EAP protocol to communicate with the authentication server at Layer 2. The supplicant will not be allowed to communicate at the upper layers of 3–7 until the supplicant's identity has been validated at Layer 2 by the authentication server. Once again, this EAP authentication process will be described in great detail later in this chapter.

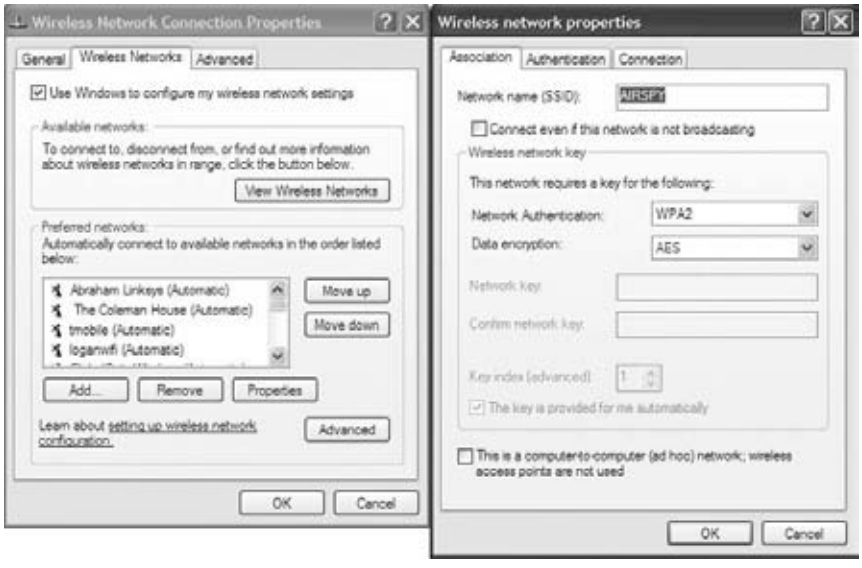
Think of the supplicant as the client software on a Wi-Fi device where the WLAN client security is configured. This isn't to be confused with the *driver* for the 802.11 radio of the device. The supplicant is a software application that performs the 802.1X endpoint services on a client device such as a laptop. Fully featured enterprise supplicants can offer support for the wired Ethernet adapter and perhaps multiple 802.11 network adapters if necessary. A good supplicant is just as important to the strength of your WLAN security as the authenticator and the authentication server. Make no mistake—this is an absolutely

true statement (as you will learn by continuing with this book) and must not be overlooked. Different types of supplicant client utility software exist, including:

- Integrated OS client supplicant
- Chipset vendor supplicant
- WLAN vendor supplicant
- Third-party supplicant

The most common supplicant software is integrated into the operating system, such as Windows XP *Wireless Zero Configuration (WZC),* as shown in Figure 4.2. A similar integrated client utility also exists in Windows Vista. Unfortunately, the WZC supplicant is limited in which flavors of EAP protocols it supports, and there are multiple known security risks with the WZC client. Several Wi-Fi hacking tools such as HotSpotter specifically target the Microsoft supplicant. The authors of this book recommend that the built-in Microsoft Windows XP Wi-Fi client utilities, known as the WZC, be disabled at all times because of numerous documented security risks. We recommend using one single vendor's software client or using third-party client utilities if multiple vendor cards must be supported.

FIGURE 4.2 Wireless zero configuration (WZC) supplicant



As shown in Figure 4.3, the Windows 7 OS offers an enhanced supplicant which has replaced the WZC. However, it is not yet known if the same security vulnerabilities exist as with earlier Microsoft supplicants. Another example of an integrated OS supplicant is Apple's AirPort client. The main advantage of the integrated OS supplicants is that they will work with any 802.11 radio and the software is free.

FIGURE 4.3 Windows 7 supplicant

Sometimes 802.11 radio chipset manufacturers such as Atheros, Broadcom, and Intel have their own supplicant software that often comes preinstalled on laptops. An Atheros supplicant will work on any laptop using an Atheros radio chipset but will not work with any laptop using a Broadcom chipset. Figure 4.4 shows the Intel PROSet client utilities.

FIGURE 4.4 802.11 radio chipset supplicant

When you purchase a third-party WLAN vendor card, it usually comes with specific software utility that can be installed onto your computer and provide the supplicant services for that specific card. An enterprise example of this is the Cisco Aironet Desktop Utility (ADU). Software applications are also bundled with a variety of SOHO consumer adapters from D-Link, Linksys, Netgear, SMC, and others. Figure 4.5 shows the Netgear supplicant that is used with Netgear WLAN radios. The main disadvantage of WLAN vendor supplicant solutions is that they only work with that one vendor card. It is always important to match specific versions of WLAN vendor drivers with specific versions of the vendor-supplied supplicant.

FIGURE 4.5 WLAN vendor supplicant

The final option is third-party supplicant software that works with multiple WLAN vendor radios. Commercial third-party client utilities offer a more robust set of configuration parameters and supported security features than either integrated utilities or bundled utilities. Third-party software supplicants often can operate on multiple OS platforms and device platforms. For example, a third-party supplicant might be used on a laptop as well as a handheld device, such as a WLAN barcode scanner. The main disadvantage of a third-party supplicant is the per-user cost. Some open source third-party client utilities do exist, however. Most enterprises look to commercial third-party supplicants and one of the best known third-party client utilities is Juniper Networks' Odyssey Access Client (OAC), which is shown in Figure 4.6. Cisco's Secure Services Client (SSC) is another well-known commercial supplicant.

FIGURE 4.6 Third-party supplicant

Courtesy of RSA

Which one do you use? Wow, that is a tough question to answer. Not all supplicants are created equal, and in order to keep up with the rapid pace of WLAN security, many older supplicants have limited EAP authentication method support and also may have severe performance problems. Some software supplicants are easier to configure than others. New features and capabilities are enabled in supplicant software as the standards progress. The best approach is to decide which EAP protocol(s) your organization will support, as well as thoroughly test your supplicant for performance and compatibility. Cost considerations may also be an issue.

Case in point: consider the evolution of WPA/WPA2-based security mechanisms. From the time it came out, every WLAN infrastructure vendor began offering support for WPA/WPA2, but the supplicant software and drivers also needed to be upgraded for WPA/WPA2 support.

Real World Scenario

Third-Party or OS Supplicant

The topic of which supplicant software to use is often debated. Consider a healthcare scenario such as a large hospital. Doctors, nurses, and other personnel will be using many different types of laptops with different WLAN vendor radio cards. Additionally, mobile patient monitoring solutions known as *computers on wheels (COWs)* also require WLAN access. Security must be maximized to protect patient medical information, and costs are always a concern. The WLAN administrator could support multiple WLAN vendor supplicant solutions; however, there is no guarantee that each solution will support the same type of EAP. Supporting multiple supplicant solutions will also put a strain on the IT help desk. The easiest and cheapest solution is to use the free Microsoft WZC supplicant. However, the WZC is limited to the number of EAP types that it supports, and there are numerous published security risks associated with the WZC. The best option is a third-party supplicant that will work with just about any WLAN vendor device. The third-party solution will cost more per user, but should support almost any type of EAP protocol. Furthermore, the help desk will have to support only one type of supplicant and the troubleshooting process should be nearly identical from device to device.

You will find that there is a substantial amount of overhead in WLAN security authentication, and the industry recognizes that it is a problem for certain types of applications, such as VoWiFi, and perhaps the devices themselves. Therefore, new amendments, such as IEEE 802.11k-2008 and 802.11r-2008, aim to improve the roaming performance while still maintaining the same or a higher level of security. WLAN infrastructure vendors have begun to implement 802.11k and 802.11r mechanisms in their enterprise solutions. Most supplicants currently do not support 802.11k and 802.11r mechanisms. Remember, the Ford Motor Company didn't go from the Model T to the Mustang overnight.

When Will 802.11k and 802.11r Mechanisms Find Their Way to the Client Side?

As 802.11 technologies evolve, new Wi-Fi CERTIFIED programs will be introduced by the Wi-Fi Alliance. Voice Enterprise is a certification scheduled to debut in 2010. Voice Enterprise will define enhanced support for voice applications in the enterprise environment. Some aspects of the 802.11r-2008 (fast secure roaming) and 802.11k-2008 (radio resource management) amendments will probably be tested in Voice Enterprise. A more detailed discussion of 802.11r and 802.11k mechanisms can be found in Chapter 7, "802.11 Fast Secure Roaming."

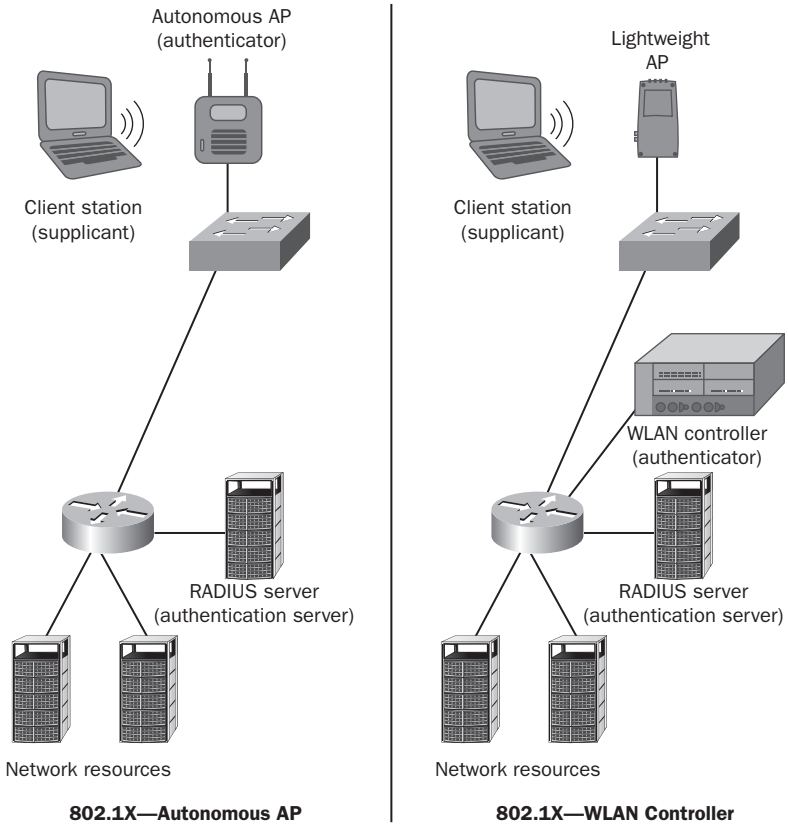
Authenticator

From the context of EAP authentication, the role of the authenticator is quite simple. The authenticator plays the role of the intermediary, passing messages between the supplicant

and the authentication server. These messages travel via an EAP authentication protocol. Remember that authenticator is an 802.1X term. Also remember that 802.1X was described as a port-based access control standard. 802.1X essentially blocks traffic until a successful Layer 2 EAP authentication occurs. As mentioned earlier, the authenticator maintains two virtual ports: an uncontrolled port and a controlled port. The uncontrolled port allows EAP authentication traffic to pass through, while the controlled port blocks all other traffic until the supplicant has been authenticated. EAP will be discussed later in this chapter, so don't worry how it works at this point.

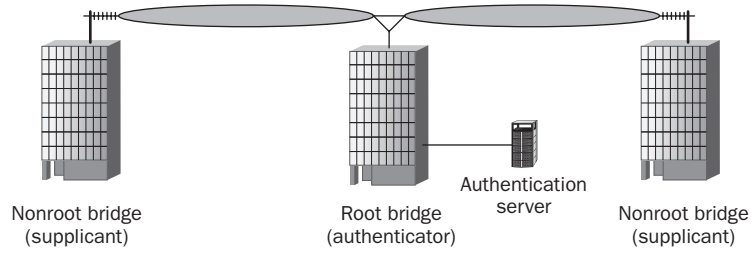
As shown in Figure 4.7, the authenticator is the AP when an autonomous access point solution is deployed and the authentication server is typically a RADIUS server. Figure 4.7 also shows that when an 802.1X security solution is used with a WLAN controller solution, the WLAN controller is the authenticator—and not the controller-based access points.

FIGURE 4.7 802.1X comparison-autonomous access point and WLAN controller



What about using an 802.1X framework with a WLAN bridging solution? As you can see in Figure 4.8, the root bridge would be the authenticator and the nonroot bridge would be the supplicant if 802.1X security is used in a WLAN bridged network.

FIGURE 4.8 WLAN bridging and 802.1X



Point-to-multipoint WLAN bridging

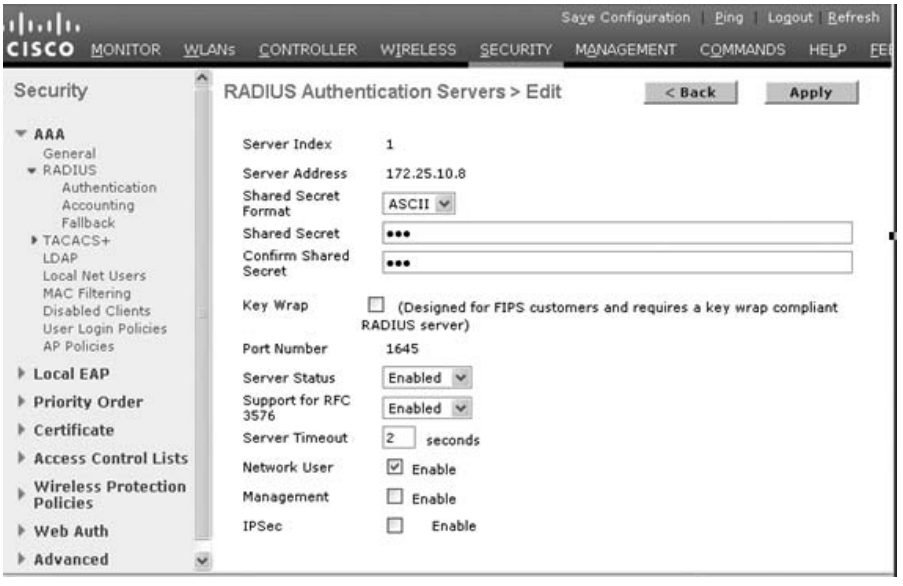
The term *authenticator* is a misnomer because the authenticator does not validate the supplicant's credentials. The authenticator's job is simply to either let traffic pass through or not pass through. As shown in Figure 4.9, a common analogy used to describe the authenticator is a bouncer at an exclusive nightclub that everybody is trying to get into. Picture some big, buff dude with a dark suit and an earpiece to communicate with the person holding the "guest list." The bouncer serves the role of the authenticator. He holds out his hand in a blocking fashion as would-be party-goers request entrance to the club. The would-be party guest (supplicant) shows their ID and the bouncer passes the identity to the guest list holder on the other end of his communication link. The guest list holder or nightclub owner (authentication server) looks up the identity on the list and simply responds with a verbal thumbs up or thumbs down.

FIGURE 4.9 Authenticator bouncer analogy

If the bouncer got a thumbs up, he would unblock the entrance for the authorized party guest to enter. Once the guest entered the nightclub, the bouncer would then block the entrance again for all new attempts to enter the nightclub. If the bouncer received a thumbs down from the nightclub owner, he would kick the posing party guest out of line and send them away.

As mentioned previously, the authenticator is either an AP or WLAN controller in your enterprise WLAN. What the authenticator needs to know is essentially who is going to provide the guest list services—which is the role of the authentication server. Therefore, when configuring a WLAN controller or AP as an authenticator, you would need to be able to point the authenticator in the direction of an authentication server. Typically, the authentication server is a RADIUS server. As shown in Figure 4.10, the authenticator would need to be configured with the RADIUS server's IP address and UDP port along with a shared secret in order to communicate with the server. A shared secret is only used to validate and encrypt the communication link between the authenticator and the authentication server. The shared secret configured on both the authenticator and authentication server is not used for any past of supplicant validation. The shared secret is only for the authenticator-to-authentication server communication link. It should also be noted that the authenticator will be configured to "require" EAP authentication, but a specific EAP type is not chosen. Remember that the authenticator is essentially a pass-through device that either allows or disallows traffic to flow through the authenticator's virtual ports.

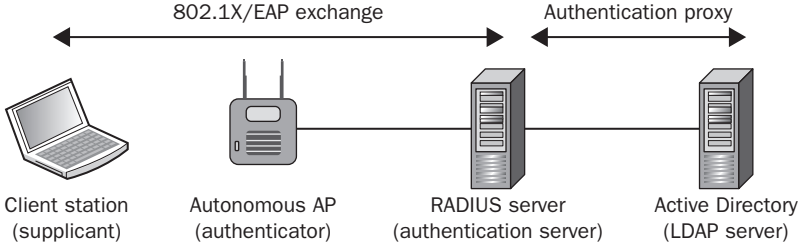
FIGURE 4.10 Authenticator configuration



Authentication Server

As mentioned earlier, the *authentication server (AS)* validates the credentials of a supplicant that is requesting access and notifies the authenticator that the supplicant has been authorized. The authentication server will maintain a user database or may proxy with an external user database to authenticate user credentials. The authentication server and the supplicant communicate using a Layer 2 EAP authentication protocol. While it has been mentioned many times that a RADIUS server is a commonly used AS, others may be used. Any *Lightweight Directory Access Protocol (LDAP)*-compliant database can be used as the authentication server. LDAP is an application protocol for querying and modifying directory services running over TCP/IP networks. Basically, any type of protocol used to communicate with the holder of the master "guest list" (referring to the bouncer analogy) is fair game. Authentication servers (such as RADIUS) may indeed hold the master native user database, but may need to communicate with other user databases in other systems. In fact, it is usually possible to use a combination of databases, such as built-in RADIUS user accounts, for simple devices like VoWiFi phones and also to integrate with a network operating system containing user accounts for employees and external networking databases can be UNIX, Microsoft Active Directory, and Novell. SQL databases can also be used. As shown in Figure 4.11, typically a RADIUS server performs authentication server duties; however, the RADIUS server also does a proxy query to a pre-established LDAP-compliant database, such as Microsoft Active Directory (AD). This is referred to as *proxy authentication*.

FIGURE 4.11 Proxy authentication



Some WLAN controller vendors allow for direct queries from the authenticator (WLAN controller) to an LDAP database. In fact, there is a growing trend to incorporate Microsoft Active Directory (AD) authentication directly from the authenticator in lieu of going first through a RADIUS server. This method may have design constraints for some situations, but may be desirable for some enterprises wanting to increase authentication performance where RADIUS servers aren't adding special features or additional user databases.

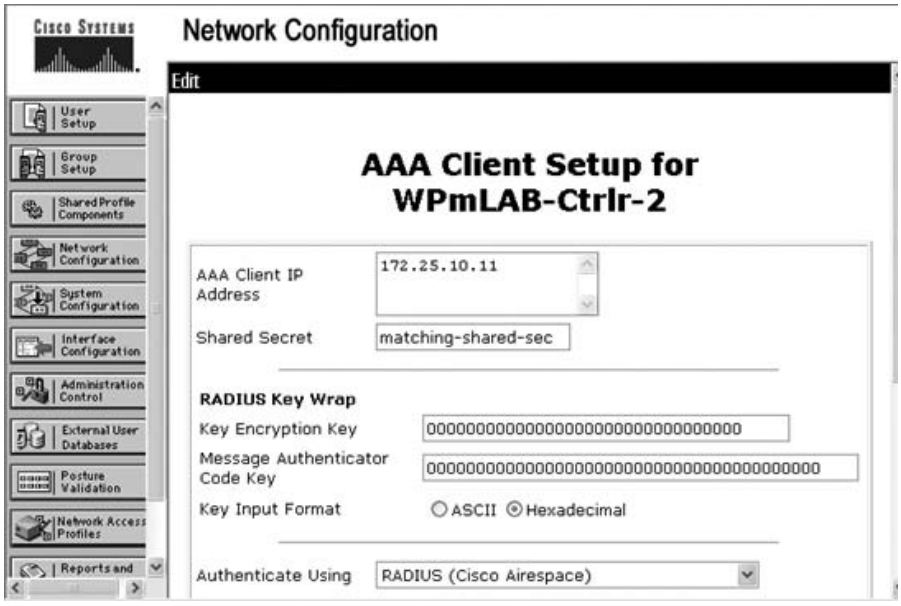
While LDAP and direct AD integration is growing, RADIUS has been around for a very long time in WLAN security and is by far the most common method used for authentication servers. Table 4.1 contains examples of authentication servers.

TABLE 4.1 Examples of Authentication Servers

Product Name	Protocol
Cisco ACS	RADIUS
Juniper Steel Belted RADIUS	RADIUS
Microsoft IAS (Windows Server 2003)	RADIUS
Microsoft NAP (Windows Server 2008)	RADIUS
Microsoft AD 2003 and higher	Kerberos and LDAP
FreeRADIUS (open source)	RADIUS

When configuring a RADIUS server, you need to be able to point the authentication server back in the direction the authenticator. Typically the authenticator is a WLAN controller or autonomous AP. As shown in Figure 4.12, the AS would need to be configured with the authenticator's IP address and shared secret in order to communicate with the authenticator.

FIGURE 4.12 Authentication server configuration



Configuration Gotchas

When configuring authenticators (APs or WLAN controllers) and RADIUS servers, there are usually two configuration problems that people regularly encounter: nonmatching shared secrets and wrong UDP ports. Ensure these values are correct before attempting any supplicant authentication attempts. RADIUS uses UDP ports 1812 for RADIUS authentication and 1813 for RADIUS accounting. These ports were officially assigned by the Internet Assigned Number Authority (IANA). However, prior to IANA allocation of UDP ports 1812 and 1813, the UDP ports of 1645 and 1646 (authentication and accounting, respectively) were used as the default ports by many RADIUS server vendors.

From years of experience, most RADIUS servers used in enterprise WLAN security implementations are implemented quite simply. As mentioned earlier, RADIUS servers usually are only used to proxy a user authentication to some master list of users, which is typically Microsoft Active Directory. While there are several features that can be used to enhance security and operational features, most enterprises do not take advantage of them. One example of this is a feature called dynamic VLAN assignment. If a user who is requesting authentication is part of the Accounting group, that user will be assigned to a specific VLAN by passing down a VLAN identifier RADIUS attribute in the RADIUS response message when a user authentication is accepted. If the user requesting authentication is part of the Marketing group or General Staff group, those users can be placed in a different VLAN based on RADIUS attributes. RADIUS attributes carry the specific authentication, authorization information, and configuration details for requests and replies including VLAN identifiers. RADIUS servers are also often used for dynamic role assignment.

Additional information such as user roles can be sent using *vendor-specific attributes (VSAs)*. Without digressing too much, this capability would allow the WLAN designer to inherit any currently implemented *role-based access control (RBAC)* mechanisms already implemented on the wired network, dynamically assigning them to the proper VLAN. For example, we generally want to keep the hands of non-accounting employees from accessing accounting applications like paycheck and expense approval systems, so typically most networks already employ some level of segmentation and access control to accomplish this for the wired network.

More information about RADIUS-based VLAN assignment and RADIUS-based role assignment can be found in Chapter 12, "Wireless Security Infrastructure."

That being said, there is another server that can, in a way, be referred to as a new type of authentication server—NAC. *Network Access Control (NAC)* is a computer network security methodology that integrates endpoint security technology with user authentication. NAC can allow for access decisions to be based on a client's antivirus state and OS patch version. NAC is an upcoming security enhancement gaining a lot of industry attention, and is typically designed to work with RADIUS servers. NAC servers are often being tied into an 802.1X framework design.

The NAC server could interrogate the user's machine when attempting to authenticate, and it could additionally make sure the computer being used has the most recent antivirus definitions update installed. Therefore, not only is the 802.1X framework validating that the user is valid, but also other factors important to controlling virus outbreaks and patching operating system and software security vulnerabilities. You can see how, if a NAC server determined a computer did not meet certain minimum criteria, it would then dynamically assign a VLAN that would be a "quarantine network" whereby the user only has access to update the virus definitions, download the necessary software patch, or whatever didn't meet the minimum requirements to join the network.

Authentication servers provide the following key features:

Client/Server Model RADIUS servers receive user connection requests, authenticate the user, and provide any other information required to support the user network connection.

Network Security Transactions between the authenticator and the RADIUS server contain sensitive user identity information and are encrypted by the RADIUS protocol.

Flexible Authentication Mechanisms RADIUS can support a variety of authentication methods that can, in turn, support a wide variety of applications and systems.

Extensible Authentication Protocol This protocol was designed to be flexible and to accommodate new attributes or enhancements easily.

Some vendors may supply features in addition to the ones listed here, but you will only be tested on your understanding of these topics.

Supplicant Credentials

As you have learned, the supplicant is the device that will need to be validated by the authentication server before being allowed access to network resources. The supplicant will use an EAP protocol to present credentials to the authentication server to prove identity. Depending on which type of EAP protocol is used, the supplicant identity credentials can be in many different forms, including:

- Usernames and passwords
- Digital certificates
- Protected Access Credentials (PACs)
- Dynamic security token devices
- Smart cards
- USB device
- Machine authentication
- Preshared keys (PSK)
- Proximity badges
- RFID tags
- Biometrics

How these supplicant user credentials are used with EAP will be discussed later in this chapter. The following sections will offer a broad overview of the various types of supplicant identity credentials.

Usernames and Passwords

Simple usernames and their respective passwords are the most common form of identity information that is supplied by a supplicant to an authentication server. Many EAP methods use usernames and passwords. What may also be used is a domain name or realm that might tell the RADIUS server what master database to use. This is a clever way to use a single RADIUS infrastructure that proxies the correct user database based on the domain or realm. For example, if you are using Windows Active Directory and have more than one domain where user accounts exist, the supplicant can pass its credentials in a DOMAIN-NAME/USERNAME format. Here's an example:

```
CWNP/ShawnJackman
```

Most RADIUS servers accept multiple formats of the domain or realm identifier. It can, in some cases, also be accepted in the form of

```
ShawnJackman@CWNP
```

Basically, the RADIUS server will dictate what forms are acceptable for this identity to be formatted. Be careful, though—some supplicants try to tinker with this format, making the assumption that the RADIUS server might always want to see it in the first form (*DOMAIN-NAME/USERNAME*) even if a user entered it using the second method.

Real World Scenario

Supplicant Configuration

Remember, supplicants are software. Software designers make certain assumptions when they write their code. Some supplicants will ask you for username, password, and domain. Some will just ask you for username and password, assuming you will actually type `DOMAIN/USERNAME` in the Username box.

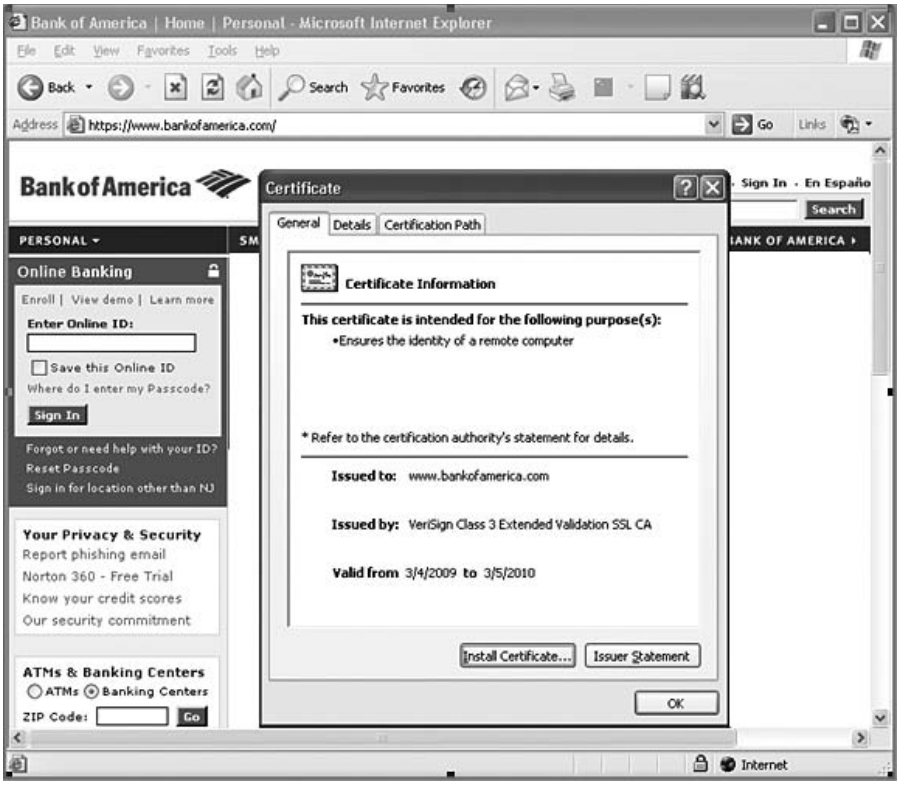
Furthermore, some supplicants will check to make sure the end-user did not perform a configuration error and type the domain name twice. For example, say the desktop engineers embedded the domain name into all suppliants installed on all mobile devices so the user didn't have to type it. What if the user actually typed `DOMAIN/USERNAME`? You might find that the EAP method actually presents `DOMAIN/DOMAIN/USERNAME` to the authentication server. There are other cases where login scripts might be configured to precede the username with a domain as well. The bottom line is that you should assume nothing and should always check for proper configurations. Check your authentication server log files for failed authentications if you are having failures, and issues like this will usually quickly reveal themselves.

Digital Certificates and PACs

Any Internet user who browses to a website with the `https://` prefix encounters digital certificates. Likewise, every time an Internet user logs into a website or uses online banking, they are using digital certificates.

Most of us know that the web server's certificate is used for encryption—a technology called *Secure Socket Layer (SSL)*. SSL is a cryptographic protocol normally used to provide secure communications over the Internet. SSL uses end-to-end encryption at the Transport layer of the OSI model. What may not be self-evident is that your computer is also authenticating the web server based on the contents of the SSL certificate, as shown in Figure 4.13. In this example, we used the Bank of America website. The bank uses a *Public Key Infrastructure (PKI)* digital certificate. Notice that the URL matches exactly the "Issued to" statement in the certificate. You can also see the certificate was issued by VeriSign, who provides the PKI management service for the bank's website.

FIGURE 4.13 SSL certificate

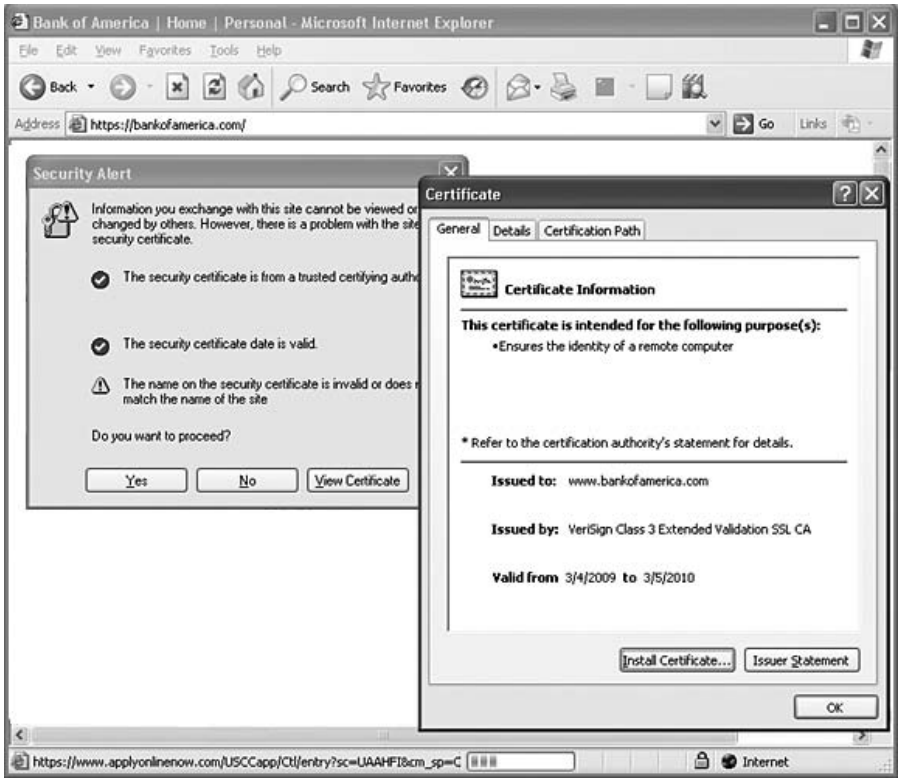


Then by utilizing the X.509 PKI certificate, we were able to verify the identity of the remote computer. In this case, it is the web server for the bank. If you have ever viewed a certificate, you will see that it contains information about the holder, such as

- Common name
- Subject
- Issuer
- Valid dates

Figure 4.14 shows what happens when we change the URL to a DNS alias for the same website. Pay special attention to the browser URL address shown in both figures and notice the slight difference. The error shown in the Figure 4.14 is warning us that the name in the certificate does not match the URL in the browser. We have all seen certificate error alert screens like this pop up, but most people never pay the proper attention the alert.

FIGURE 4.14 SSL certificate alert



EAP authentication protocols can use both server-side and client-side certificates. Later in this chapter, we will discuss how some EAP protocols use server-side certificates to create an encrypted tunnel during the authentication process. If the EAP protocol supports client-side certificates, the implementation of a PKI will be necessary. Unique client certificates will have to be created, issued, and managed for every WLAN user or device. Upon expiration, certificates will also require updating. Because the client-side certificates are being used as credentials to validate the supplicant, the 802.1X authentication server validates the client-side certificate issued by a PKI.

Public Key Infrastructure (PKI)

A PKI is a framework used for creating a secure method for exchanging information based on public key cryptography. A PKI uses hardware, software, people, policies, and procedures to create, manage, store, distribute, and revoke digital certificates. Certificates require a common format and are largely based on the ITU-T X.509 standard. A more detailed explanation of digital certificates and how they work within a PKI can be found in Chapter 12.

Another certificate-like credential that can be used by supplicants is called a Protected Access Credential (PAC). EAP-FAST uses PACs as credentials instead of the more standards-based X.509 certificates. EAP-FAST is an EAP protocol that was originally developed by Cisco as a replacement for EAP-LEAP and was designed for ease of deployment and renewal.

Because using client-side certificates requires the implementation of a PKI, the installation, administration, and cost of the PKI is often considered to be undesirable to maintain just for WLAN devices. Cisco knew this when they designed EAP-FAST and designed a PAC file. A PAC file is a close cousin of a digital certificate, but the RADIUS server is the issuing party. We already know the RADIUS server is also the authenticating party that validates the supplicant. While it is not quite the same, as a mental model you can think of an EAP-FAST PAC/RADIUS infrastructure as a mini-PKI. The RADIUS server issues and validates the correct PAC that is used by the supplicant. Each PAC is tied to an individual user identity. EAP-FAST will be discussed in greater detail later in this chapter.

One-time Passwords

A *security token* is any physical device that is issued to an authorized user of computer services to enhance authentication strength. Some security tokens also incorporate one-time password capabilities. A *one-time password (OTP)* is a password that is only valid for a single login session or transaction. RSA Security is largely considered the inventor of the one-time password and is the dominant market leader in this space at the time of this writing. RSA developed a technology called SecurID that uses a dynamically updated one-time password at fixed intervals—usually 30 or 60 seconds. OTP security

tokens can exist in either a hardware or software form factor. A hardware OTP security token device is shown in Figure 4.15.

FIGURE 4.15 OTP token device

Courtesy of RSA

Each token device is unique and is assigned to an individual user ID. The OTP generated from the token device is designed to be different from other token devices at any given time. When that user requests an authentication, the token device OTP must be supplied with the user's normal password. If the user's password is correct, but the one-time password is wrong, the authentication fails. Therefore, this protects against stolen user identities.

The OTP token devices and the OTP authentication server verifying the passwords work off a precise time clock. A mathematical calculation is performed using the token device clock value as well as other token information. The OTP authentication server's clock runs a similar calculation because it is synchronized with the token device. The OTP server already knows the other token device identity for each unique user in order to construct the same calculated result the token device uses.

OTP achieves a two-factor authentication for the user requesting access based on their user identity *and* something that user has in their possession.

Most of the vendors in the market segment use other form factors for security token devices, which is an admonition that a single type of hardware device doesn't fit all situations. These include USB tokens, smart cards, and software-based OTP applications. Some of the vendors in this space include RSA (as mentioned earlier), VASCO, Aladdin, and ActivIdentity.

All security token devices have a mandatory cost per user (for the device), including the additional infrastructure components and operational overhead of maintaining the infrastructure. Vendors of each solution have their own software mechanisms to keep track of to whom each device is issued and to revoke them should the device be lost.

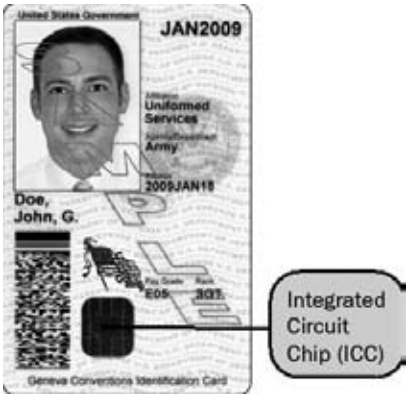
Just as you would your car key, you typically realize it is gone quite quickly. The same usually goes for these types of products, which is partly what makes them more secure than simply using usernames and passwords. Compromised user credentials can literally go unnoticed for months or even years if the user doesn't change their password.

If a smart card slot is available on your end-user devices, it can be a more convenient way to accomplish two-factor authentication compared with entering in a numeric token at each login. It can be quite convenient to insert it into the slot and simply log in normally with a username and a password. When the smart card is removed, the system can be designed to log the user out automatically. This can assist with your enterprise security policy even further if those devices are tethered to the end users so that, when the workstation is left unattended, it is not also left logged in.

Smart Cards and USB Tokens

Smart cards and USB tokens can also be used for a single-factor authentication. They really haven't gained the mass popularity that was once anticipated, but they do have their niche. As shown in Figure 4.16, a *smart card* is any pocket-sized card with embedded integrated circuits that can process data. A smart card is also often referred to as an *integrated circuit card (ICC)*. The key concept around a smart card or a USB token is to store unique user identity information securely on the integrated circuit chip. Typically, this data cannot be modified or copied. The contents can be nearly any type of information, but it is usually similar to or quite literally a client-side digital certificate. Most smart card technology is based on X.509 certificates. The core problem behind this identity method falls into the same PKI cost and management issues that are needed for client-side certificates on a per-user and perhaps even a per-machine basis. Effectively, a smart card or USB token functions as a client-side certificate.

FIGURE 4.16 Smart card



The United States Department of Defense (DoD) uses a Common Access Card (CAC) for identification of active-duty military personnel, reserve personnel, civilian employees, and contractor personnel. The CAC is based on X.509 certificates, with software middleware enabling an operating system to interface with the card via a hardware smart card reader. As shown in Figure 4.17, most smart card readers are external devices; however, internal smart card readers are now being built into laptops, handheld scanners, and even phones. As shown in Figure 4.18, USB security tokens can also function as client-side credentials. However, it should be noted that most government agencies and many corporations do not allow the use of any kind of USB device due to the security risks associated with the USB interface.

FIGURE 4.17 Smart card reader

FIGURE 4.18 USB security token

Courtesy of Aladdin

Machine Authentication

Machine authentication is the concept of ensuring the *device* requesting access to the network is authorized. User authentication usually ultimately follows the machine authentication, although it is not required. Machine authentication is primarily used to provide a "wired-like" experience to wireless users.

When you are plugged into a wired network and your machine turns on from scratch, the machine itself is already on the network and is awaiting your credentials to communicate with your network operating system to validate your identity. When the machine is completely wireless, how does this happen when the supplicant is not launched until a user has logged in? Machine authentication is a way for a network device to join the WLAN before a user is logged into it in order to communicate with a network operating system such as Windows Active Directory.

In the case of Windows, the machine credentials are based on a *System Identifier (SID)* value that is stored on a Windows domain computer after being joined to a Windows domain with Active Directory. The information stored in this SID is unique for each AD machine. We have the option to use this unique computer information in order to authenticate the machine to the network when no user information exists.

It doesn't mean that the machine will be logged into the Desktop. Rather, it will provide a "wire-like" experience and have an active network connection in order to authenticate a user's login without using cached credentials. Other important benefits are also provided, such as enabling remote access, pushing software patches, monitoring applications, and other remote administrative tasks.

Real World Scenario

Machine Authentication

There are several supplicants that can be configured for machine authentication. The computer will associate to the wireless network using 802.1X and, instead of passing user credentials, it will use a system identifier that Active Directory stores on all Active Directory computer objects. When machine authentication is configured, after a machine boots up—even for the first time—and the user is asked for their user credentials, the machine can be already on the WLAN via these machine credentials. This will allow a never-before-seen user to log into that computer because it already has communication with Active Directory.

Requirements for using machine credentials are that you must use a supplicant capable of machine authentication and 802.1X must be employed. Most enterprise supplicants support machine authentication, including the Microsoft's integrated WZC supplicant. Furthermore, your RADIUS server needs to be integrated with Active Directory and machine authentication must be enabled.

Preshared Keys

Preshared keys are only mentioned here because of their supported use in WLAN security. PSKs are not recommended for use in enterprise WLAN deployments. A *preshared key (PSK)* is a common password or passphrase that is shared between the authenticator and the supplicant. The PSK is used for authenticating the wireless client and is the derivative for the encryption keys generated to encrypt the data traffic. The Wi-Fi Alliance defines the use of PSKs in the WPA/WPA2-Personal certifications. Preshared keys are usually used in SOHO environments. A more detailed discussion of how preshared keys are used can be found in Chapter 6, "SOHO 802.11 Security."

Proximity Badges and RFID Tags

Several types of proximity badges and RFID tags are available for a variety of uses. As shown in Figure 4.19, a proximity badge is usually incorporated into a corporate nametag where a photo sticker with the employee's name is worn on their body. When the person walks up to the computer, a badge reader or RFID tag interrogator recognizes the user's exact location. Then the user is typically prompted for a password or PIN to gain

access to the computer. Hospitals are a common environment where proximity badges are used because the caregivers are highly mobile.

FIGURE 4.19 Proximity badge

Courtesy of Ensure Technologies

Biometrics

Biometrics involves the use of uniquely identifiable elements of the human body that are scanned and stored on a central authentication server and later validated against for each login. When biometrics is used in conjunction with passwords or PINs, it can be an extremely effective way of validating identity.

Enterprises employing biometrics usually are extremely sensitive to security because of the high overall system and management cost. However, many enterprise laptop manufacturers are building in fingerprint sensors, so the per-device cost is becoming less of an issue. Biometrics has even been integrated into mobile phones in some countries. As companies typically standardize on a single manufacturer's hardware, it is becoming more and more feasible to deploy biometrics as a multifactor authentication mechanism that can also be incorporated into WLAN authentication.

Authentication Server Credentials

You have already learned that within any 802.1X framework the authentication server validates the supplicant's credentials. The most secure EAP authentication methods incorporate the concept of *mutual authentication*. We already know that the supplicant's

identity gets validated, but how about validating the authentication server's identity? In other words, the EAP-protocol allows the supplicant to also validate the authentication server. Mutual authentication validates both the supplicant and the AS and, if implemented properly, will prevent man-in-the-middle attacks. If the authentication server is to be validated by the supplicant, the AS must present credentials to the supplicant. Most EAP protocols use a server-side certificate for the authentication server credentials.

A server-side certificate must be created and installed on the authentication server. Copies of the server-side public certificate or the issuing root authority must also be installed on the supplicant. The authentication server certificate serves two major purposes:

Validates the Authentication Server The AS certificate is first used to validate the identity of the server to the WLAN supplicant. This process is akin to the supplicant saying, "Oh, I know who you are," before the supplicant submits its own sensitive identity information.

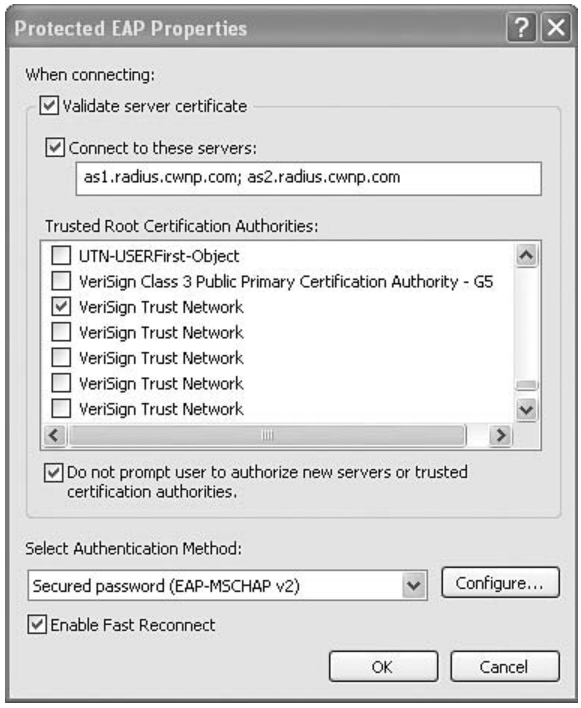
Creates an Encrypted TLS Tunnel EAP protocols that require a server-side certificate for the authentication server are used to create *Transport Layer Security (TLS)* encryption tunnels. TLS is a cryptographic protocol normally used to provide secure communications at the Transport layer of the OSI model. However, in the case of 802.1X/EAP TLS technology is leveraged at Layer 2. Similar to a browser-based SSL session, the TLS protocol uses end-to-end encryption. Once the supplicant is sure of the identity of the authentication server, the supplicant then uses the certificate to establish an encrypted TLS tunnel. The supplicant identity credentials are then exchanged within the encrypted TLS tunnel. The supplicant identity, we have already learned, can come in many forms. Whatever form of identity that is passed by supplicant, it will be passed within the encrypted TLS tunnel. The TLS tunnel protects the supplicant credentials from offline dictionary attacks and from eavesdropping. This is just like the method employed with e-commerce websites using SSL where credit card and personal information is passed securely through an SSL tunnel.

When the client supplicant authenticates the AS, it is usually done in one of two ways. The first method is via a certificate issued from a "trusted root authority." The second, and more common, method is to use a self-signed server certificate that is installed onto each WLAN supplicant when a PKI is not available. A common mistake is that people confuse the installation of a self-signed server certificate on the supplicant with a client-side certificate. Remember, the server-side certificate is used to validate the server. Client-side certificates were discussed earlier, and they are sometimes used to validate supplicants.

More advanced supplicants will also allow the ability to pattern match against the contents contained in the server certificate. Because a digital certificate contains certain values about the host, the issuing identity, and other information, a client supplicant can make good use of this information.

Let's examine a common configuration scenario. Consider an enterprise that purchased a server-side certificate from a well-known and established trusted root authority and installed it on the AS. Security best practices mandates that clients be configured for mutual authentication by validating the server certificate, as shown in Figure 4.20.

FIGURE 4.20 Server certificate validation



Trusted root certificate authorities are being updated all of the time and distributed with regular OS service patches, or if you're using Windows Active Directory, can be passed via a domain Group Policy automatically. The list of trust root authorities, sometimes referred to as a Certified Trust List (CTL), keeps on growing.

Put simply, a client should be configured to be *skeptical* of the AS identity. Most supplicants allow this in the simple form of a *Validate Server Identity* checkbox, just as with Windows WZC.

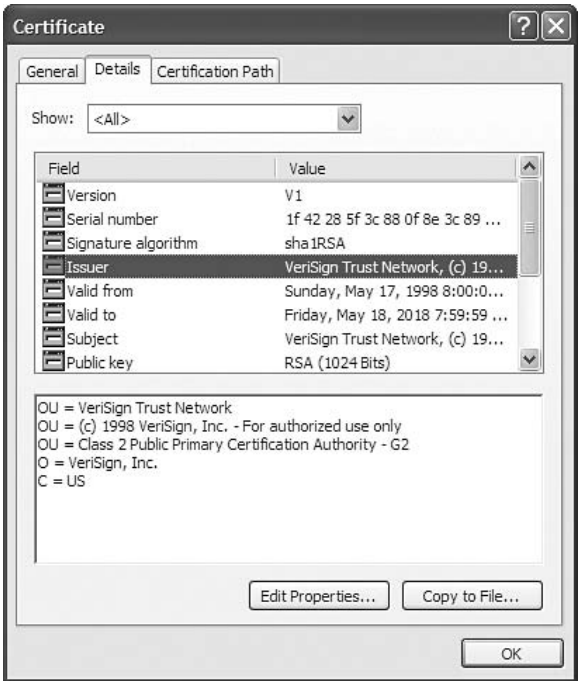
Once this is checked, a list of known trusted root authorities and imported computer certificates is listed. In some supplicants, when clicking this checkbox with default options, it is essentially saying that *any* server with a certificate issued from *any* one of these trusted root authorities is fine with you. This leaves a potentially large security hole for a hacker to perform a man-in-the-middle attack. All an attacker would have to do is purchase a valid, current certificate from any one of those sources, and it would pass the supplicant's acceptance criteria.

To configure a WLAN supplicant to be as skeptical as possible, we can *discriminate* on information details contained in the server certificate. Thankfully, many enterprise supplicants have built-in mechanisms that we can use. Deploying 802.1X/EAP solutions without discriminating, based on server validation criteria, is a poor security design and

will leave your network vulnerable to man-in-the-middle attacks. We will explore examples of those later.

As shown in Figure 4.21, every digital certificate contains publicly advertised information, such as the *common name (CN)* of the server or host and typically a string that is used to identify the *organizational unit (OU)* for which the certificate is used. Even the DNS name of the server is an option to which the supplicant can make a comparison. Of course, during a Layer 2 authentication, no IP connectivity is available during the initial authentication for a DNS query verification to be performed, but this is nonetheless a technique that can be used for digital certificate pattern matching verification in general.

FIGURE 4.21 Certificate information details



If a server-side certificate was presented to a WLAN supplicant during a TLS-tunnel establishment, the client could first validate this information against some information we are expecting to see from the server's certificate, such as `*.radius.cwnp.com`. The asterisk is a wildcard mask whereby a RADIUS server cluster using the `radius.cwnp.com` subdomain would match. These criteria would ensure any certificate with a domain suffix of `radius.cwnp.com` would be valid. Some supplicants may require wildcard characters at the end of the validation string. Refer to your supplicant documentation for syntax and options. While not all supplicants are created equal, the previous examples allow a WLAN security professional to design and deploy a highly secure WLAN.

There are options when it comes to using digital certificates. You can purchase a certificate from an issuing authority, such as VeriSign, Equifax, and other issuing authorities, for several hundred dollars per year—prices vary by options. A private PKI can be configured for your enterprise and published to each of your client endpoints. Microsoft AD Group Policies make this easy to do when using a domain. Another option is to create a self-signed certificate. A variety of free tools are available to create self-signed certificates. A simple web search will yield a variety of results.

Which one is better? Assuming your clients' Certified Trust List (CTL) is up to date; you can purchase a certificate from an issuing authority and install the certificate in a single day. This approach, however, can be costly. If several hundred dollars per year for each RADIUS server is too costly you must consider the staff time involved to manually deploy a self-signed certificate to each supplicant.

If you roll your own PKI infrastructure, well, you are in for a little reading and experimenting. Not a great deal of educational/training information is available about managing your own PKI. Keep in mind, there are server hardware costs, licensing, maintenance, power consumption, and many hours of staff time involved in managing your own private PKI.

Real World Scenario

Distributing the Public Server-side Certificate to Supplicants

To deploy a self-signed certificate to wireless devices that have no convenient way to distribute it automatically, you have several options.

First, you can configure the supplicant *not* to validate the server certificate temporarily. The device will connect to your WLAN and be on your network. When you publish the public certificate(s) on an internal web server or network file share, the certificate can be manually downloaded and installed on each client in the Trusted Root Certificate store. Then you reconfigure the supplicant to validate the server certificate, select the new trusted root(s), and reconnect.

The other option is to use an enterprise supplicant like Juniper Odyssey Access Client (OAC) or Cisco Secure Services Client (SSC). Administrative tools within these supplicants allow you to create an MSI (executable installer file) with prebuilt profile(s) and even bundle in the certificates. That's all in a single MSI installer that can install the supplicant with preconfigured WLAN profiles and also have the certificate(s). That is just darn cool.

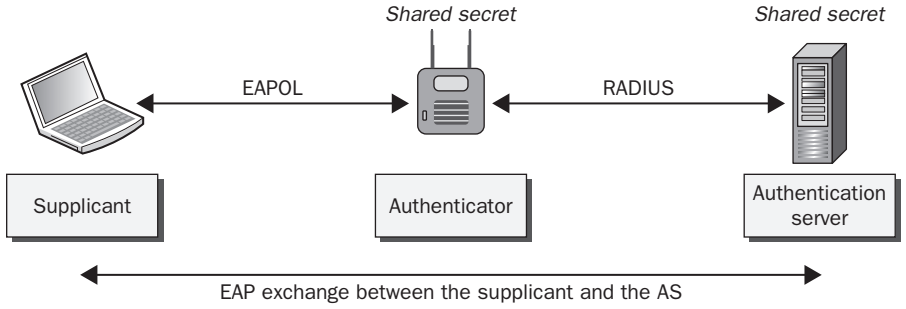
The second method can work just fine even for end-user devices that are (or aren't) part of a Windows domain. What's more, enterprise supplicants, like Cisco SSC and Juniper OAC, actually allow you to lock end users out of reconfiguring wireless options such as enabling Ad Hoc mode, misconfiguring the standard enterprise profiles, choosing weak EAP types, and more.

Self-signed server certificates can be a great choice and actually quite secure as well. The problem is distributing the public server certificate to each client endpoint. As stated earlier, if you are using Microsoft AD this is quite simple, and for devices that aren't part of the domain, the public certificate can be placed on a public website for clients to download and install. Remember, a certificate's public identity is something you want to distribute. Only the private key can decrypt information encrypted with the public key and only the AS (RADIUS server) will be able to do that. If distributing the public server certificate isn't an issue for your organization, then using a self-signed certificate can be a cheap (free!) option.

Shared Secret

A *shared secret* is used between the authenticator and the authentication server for the RADIUS protocol exchange. As shown in Figure 4.22, Layer 2 EAP protocol communications occur between the supplicant and the AS. The 802.11 frames use what is called *EAP over LAN (EAPOL)* encapsulation between the supplicant and the authenticator to carry the EAP data. On the wired side, the RADIUS protocol is used between the authenticator and the AS. The EAP data is encapsulated within a RADIUS packet. A shared secret exists between the authenticator and the AS, so that they can validate each other with the RADIUS protocol.

FIGURE 4.22 Shared secret



As mentioned earlier in this chapter, when configuring a RADIUS server, you need to configure each authenticator's identity within each authentication server. Typically, the authenticator is a WLAN controller or autonomous AP. The AS would need to be configured with each authenticator's IP address and the shared secret in order to communicate with each authenticator.

Conversely, the authenticator itself is configured to point to a prioritized list of authentication servers (RADIUS server in this example) with the following information:

- IP address of the RADIUS server
- UDP ports (1645 or 1812 for authentication; 1646 or 1813 for accounting)
- Shared secret

Usually, APs and WLAN controllers allow designation of up to three RADIUS servers for redundancy purposes.

Very often there will be only one WLAN controller, so there is only a need for one shared secret between the WLAN controller and the RADIUS server. However, what if there are multiple WLAN controllers or multiple autonomous APs acting as authenticators? Best security practices dictate that there should be a separate and unique shared secret for each authenticator communicating with the RADIUS server. If one of the shared secrets is somehow compromised, at least the other shared secrets are still protected.

Legacy Authentication Protocols

Before explaining EAP, it is important to discuss some legacy authentication protocols that have contributed to the history of network security. Some of these legacy protocols are still used within the stronger EAP authentication protocols. However, the legacy authentication protocols are used inside of a TLS tunnel. You will see that the TLS tunnel is used to encrypt and protect the legacy authentication encryption methods. Let's take a closer look at the legacy authentication protocols relevant to WLAN security.

PAP

Password Authentication Protocol (PAP) is defined in RFC 1334 and provides no protection to the peer identity. It was originally designed for use with Point-to-Point Protocol (PPP). Although rarely used, it would be logical to use PAP inside an encrypted TLS tunnel because of its nonsecure nature.

CHAP

Challenge Handshake Authentication Protocol (CHAP) is defined in RFC 1994 and is slightly more evolved than PAP. CHAP is used with PPP as well and differs in that the password of the user identity is encrypted with an MD5 hash. Because MD5 is not considered secure by today's standards, CHAP should never be used outside of a TLS tunnel.

MS-CHAP

Microsoft developed a proprietary version of CHAP and later defined it in RFC 2433. *Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)* also uses a hash

of the password in a transmitted user identity. Early versions of Microsoft Windows Active Directory (AD) stores an MS-CHAP compatible hash of a user's password in the AD database in lieu of the actual password. This hash can then be compared to the hash presented by the supplicant.

This initial version of MS-CHAP is considered weak and many freely available software packages exist that can recover the password from the MS-CHAP hash. Therefore, MS-CHAP should only be used inside a TLS tunnel.

MS-CHAPv2

Of course, whenever vulnerability is discovered, a new version is ushered along. *MS-CHAPv2* is defined in RFC 2759 and was first released with the Microsoft Windows 2000 family. MS-CHAPv2 uses a much stronger hashing algorithm and also supports mutual authentication during an MS-CHAPv2 exchange. EAP-PEAP, EAP-TTLS, and EAP-FAST all optionally use MS-CHAPv2, or in the case of EAP-LEAP, it is exclusively used. MS-CHAPv2 has also been found vulnerable and should also only be used inside a TLS tunnel.

EAP

The Extensible Authentication Protocol (EAP), as defined in IETF RFC 2284, provides support for many authentication methods. EAP was originally adopted for use with PPP. EAP has since been redefined in the IETF RFC 3748 for use with 802.1X port-based access control.

As noted earlier, EAP stands for Extensible Authentication Protocol. The key word in EAP is *extensible*. EAP is a Layer 2 protocol that is very flexible, and many different flavors of EAP exist. Some, such as Cisco's Lightweight Extensible Authentication Protocol (LEAP), are proprietary; while others, such as EAP-TLS, are considered standard based. Some may provide for only one-way authentication, while others provide two-way authentication more commonly called mutual authentication. Mutual authentication not only requires that the authentication server validate the client credentials, but also that the supplicant authenticate the validity of the authentication server. Most types of EAP that require mutual authentication use a server-side digital certificate to validate the authentication server. As stated earlier, a server-side certificate will also be used to create an encrypted TLS tunnel.

As you learned earlier in this chapter, 802.1X is an authorization framework with the three components of the supplicant, authenticator, and authentication server. The main purpose of an 802.1X solution is to authorize the supplicant to use network resources. The supplicant will not be allowed to communicate at the upper layers of 3–7 until the supplicant's identity has been validated at Layer 2. EAP is the Layer 2 protocol used within an 802.1X framework.

As mentioned earlier, the EAP messages are encapsulated in EAP over LAN (EAPOL) frames. There are five major types of EAPOL messages, as shown in Table 4.2.

TABLE 4.2 EAPOL Messages

Packet Type	Name	Description
0000 0000	EAP-Packet	This is an encapsulated EAP frame. The majority of EAP frames are EAP-Packet frames.
0000 0001	EAPOL-Start	This is an optional frame that the supplicant can use to start the EAP process.
0000 0010	EAPOL-Logoff	This frame terminates an EAP session and shuts down the virtual ports. Hackers sometimes use this frame for DoS attacks.
0000 0011	EAPOL-Key	This frame is used to exchange dynamic keying information. For example, it is used during the 4-Way Handshake.
0000 0100	EAPOL- Encapsulated - ASF-Alert.	This frame is used to send alerts, such as SNMP traps to the virtual ports.

Let's review a generic EAP exchange. The two workhorses are the supplicant and the authentication server because they both use the EAP protocol to communicate with each other at Layer 2. The authenticator is the bouncer that sits between the two devices. As you have already learned, the authenticator maintains two virtual ports: an uncontrolled port and a controlled port. When open, the uncontrolled port allows EAP authentication traffic to pass through. The controlled port blocks all other traffic until the supplicant has been authenticated. When the controlled port is open, upper layer 3–7 traffic can pass through. Dynamic IP addressing with DHCP is performed once the controlled port is opened.

As shown in Figure 4.23, 802.1X/EAP authentication works together with standard 802.11 Open System authentication and association. An 802.11 client station will actually establish a Layer 2 connection with the AP by associating and joining the basic service set (BSS). However, if 802.1X/EAP is implemented, Layer 2 is as far as the 802.11 station gets until the client also goes through the entire 802.1X/EAP process.

FIGURE 4.23 802.11 association and 802.1X/EAP

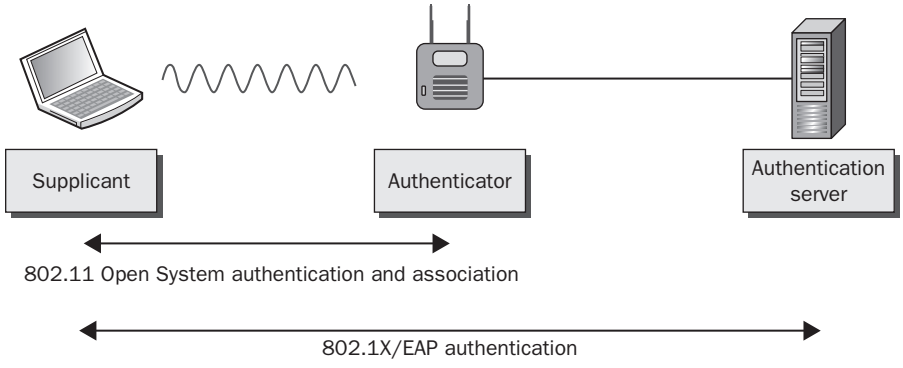
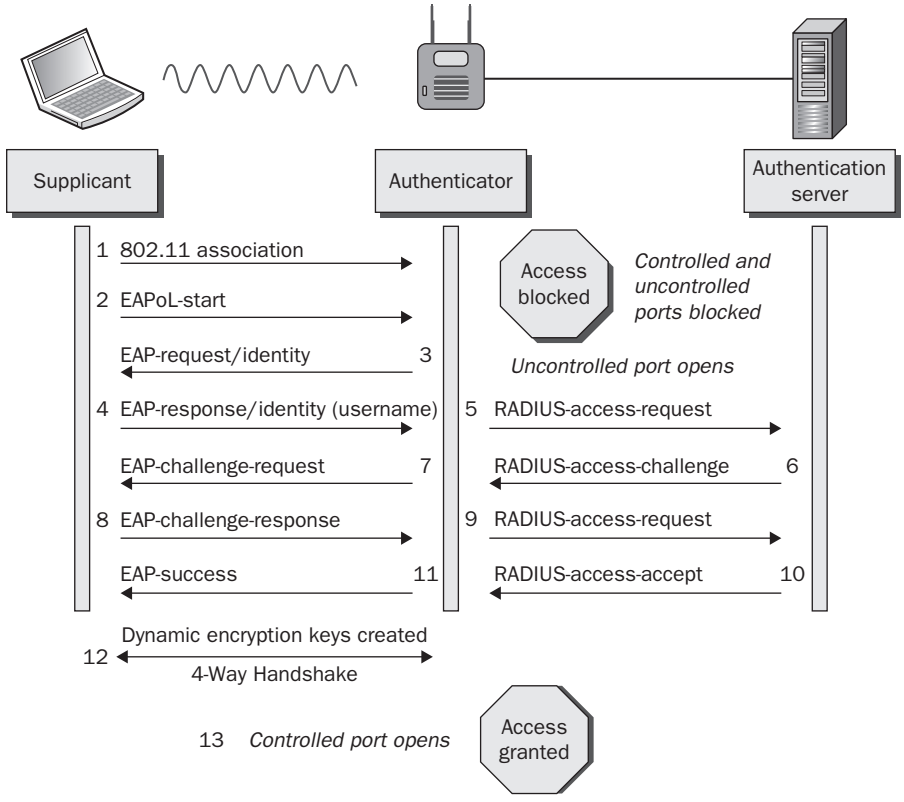


Figure 4.24 displays all the steps in a generic EAP exchange. The authenticator in this example is an autonomous AP. Please refer to the figure as we go over each of these steps.

FIGURE 4.24 Generic EAP exchange



1. The 802.11 client (supplicant) associates with the AP and joins the BSS. Both the controlled and uncontrolled ports are blocked on the authenticator.
2. The supplicant initiates the EAP authentication process by sending an 802.11 EAPOL-Start frame to the authenticator. This is an optional frame and may or may not be used by different types of EAP.
3. The authenticator sends an 802.11 EAP-Request frame requesting the identity of the supplicant. The EAP-Request Identity frame is always a required frame.
4. The supplicant sends an EAP response frame with the supplicant's identity in clear text. The username is always in clear text in the EAP-Response Identity frame. At this point, the uncontrolled port opens to allow EAP traffic through. All other traffic remains blocked by the controlled port.
5. The authenticator encapsulates the EAP response frame in a RADIUS packet and forwards it to the authentication server.

6. The AS looks at the supplicant's name and checks the database of users and passwords. The AS will then send a password challenge to the supplicant encapsulated in a RADIUS packet.
7. The authenticator forwards the password challenge to the supplicant in an 802.11 EAP frame.
8. The supplicant takes the password and hashes it with a hash algorithm such as MD-5 or MS-CHAPv2. The supplicant then sends the hash response in an EAP from back to the AS.
9. The authenticator forwards the challenge response in a RADIUS packet to the AS.
10. The AS runs an identical hash and checks to see if the response is correct. The AS will then send either a success or failure message back to the supplicant.
11. The authenticator forwards the AS message to the supplicant in an EAP-Success frame. The supplicant has now been authenticated.
12. The final step is the 4-Way Handshake negotiation between the authenticator and the supplicant. This is a complex process used to generate dynamic encryption keys. This process is discussed in great detail in Chapter 5.
13. Once the supplicant has completed Layer 2 EAP authentication and created dynamic encryption keys, the controlled port is unblocked. The supplicant is then authorized to use network resources. If using IP, the next step the supplicant will take is obtain an IP address using DHCP.

You should notice that in step 4, the supplicant's username is seen in clear text. You might say that is a security risk—and you would be correct. You should also notice that in steps 6–9, the supplicant's password credentials are validated using a weak challenge/hash response. This frame exchange can be captured using a WLAN protocol analyzer. This is a security risk because the hash algorithms have been cracked and they are susceptible to offline dictionary attacks. In other words, the presentation of supplicant identity and validation of supplicant credentials is a security risk. Wouldn't it be better if steps 4–9 were protected in an encrypted tunnel? Since its original adoption, a number of weaknesses were discovered with some EAP authentication methods. The most secure EAP methods used today employ *tunneled authentication* to pass identity credentials (usernames and passwords) similar to what you find with web-based e-commerce transactions. We will now discuss the major EAP protocols, including the ones that use tunneled authentication.

Weak EAP Protocols

Older legacy EAP protocols exist that are highly susceptible to a variety of attacks, including social engineering and offline dictionary attacks. These authentication protocols had their day in the sun, but they should be viewed as absolutely unacceptable solutions in enterprise WLANs now that more secure EAP protocols are available. We will now discuss two legacy protocols called EAP-MD5 and EAP-LEAP.

EAP-MD5

EAP-Message Digest5 (EAP-MD5) is a fairly simple EAP type and is conceptually similar to the generic EAP method described in the previous section. EAP-MD5 has for a long time been used for port authentication on wired networks and therefore was one of the very first EAP types used with WLANs. Many organizations were already using EAP-MD5, and it was a logical progression to leverage it for WLANs because RADIUS servers already supported it. However, EAP-MD5 has several major weaknesses:

One-Way Authentication Only the supplicant is validated; the server is not validated. Mutual authentication is needed to create dynamic encryption keys. If EAP-MD5 is the chosen authentication method, the encryption method is static WEP or no encryption at all.

Username in Clear Text The supplicant's username is always seen in clear text, as illustrated in Figure 4.24. If a hacker knows the identity of the user, the hacker can attempt to get the password using social engineering techniques. Therefore, EAP-MD5 is vulnerable to social engineering attacks.

Weak MD5 Hash The supplicant password is hashed using the MD5 hash function, which was once considered secure enough for its intended use in PPP networks. MD5 was never designed to be used over a wireless medium, and it is easily broken using a variety of hacker tools available today. Therefore, EAP-MD5 is highly susceptible to offline dictionary attacks.

Because of these three major weaknesses, EAP-MD5 should never be used in an enterprise WLAN environment now that stronger EAP protocols exist.

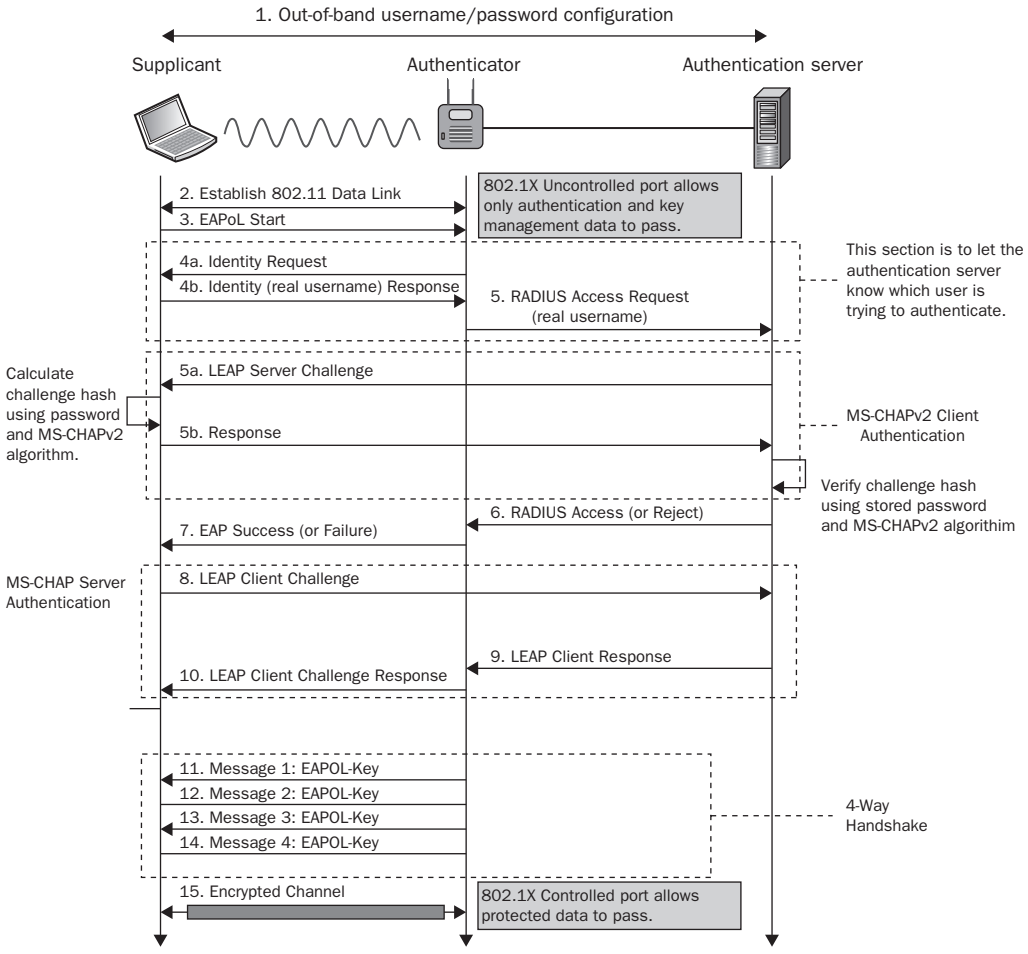
EAP-LEAP

EAP-Lightweight Extensible Authentication Protocol (EAP-LEAP), also known simply as LEAP, was a hugely successful EAP type used in the enterprise for many years. LEAP was easy to deploy using the same identity credentials to which end-users were already intimately accustomed; that is, usernames and passwords. Furthermore, it was introduced in 2000 when security weaknesses were discovered with static WEP encryption. LEAP was also used to generate dynamic WEP keys, as described in Chapter 5. Dynamic WEP was a predecessor to TKIP/RC4 and CCMP/AES dynamic encryption. LEAP was a big step forward in security at the time. However, as Bob Dylan once sang, "the times, they are a-changin."

Unlike EAP-MD5, LEAP does perform a type of pseudo-mutual authentication. Most documentation claims that LEAP supports mutual authentication. The password hash comparison algorithm used with MS-CHAP and MS-CHAPv2 validates that each side has the same password using a mutual authentication process. This is not the same mutual authentication that we've discussed where the supplicant validates the authentication server identity.

LEAP is not a TLS tunneled authentication method and is not an open standard; it must be licensed from Cisco. Figure 4.25 depicts the entire EAP-LEAP authentication process.

FIGURE 4.25 EAP-LEAP



LEAP has several major weaknesses:

Username in Clear Text The supplicant's username is always seen in clear text in the initial EAP-Response frame sent by the supplicant to the authentication server. If a hacker knows the identity of the user, the hacker can attempt to get the password using social engineering techniques. Therefore EAP- LEAP is vulnerable to social engineering attacks.

Weak MS-CHAPv2 Hash The supplicant password is hashed using the MS-CHAPv2 hash function. MS-CHAPv2 has also been found to be vulnerable. A widely available program called ASLEAP, developed by Joshua Wright, can perform an offline dictionary attack on the hash function and easily obtain the password. Therefore, EAP-LEAP is highly susceptible to offline dictionary attacks.

Pseudo-Mutual Authentication There has been some confusion with LEAP over the years with respect to mutual authentication. Since LEAP uses MS-CHAPv2, the MS-CHAPv2 protocol itself supports a *form* of mutual authentication. With respect to the grand scheme of WLAN security and what a WLAN security professional should look for in a security protocol, this form of mutual authentication buys very little.

The biggest problem with both EAP-MD5 and LEAP is that the prize is absolutely huge to a hacker—a username and password. The username and password is likely the same username and password used for Windows Active Directory or whatever network operating system might be installed. With a high-gain antenna sitting from quite far away, an attacker can pick up this exchange and gain full access credentials for WLAN users in mass. Combine this with a little knowledge of who the IT administrator is, and an attacker can have the keys to the kingdom in very short order. Or what about the CEO? That username and password just might give an attacker access to the CEO's email account. What's more, there is no way this attack can be detected because it can be performed completely passively and offline.

The success of an offline dictionary attack is only as strong as the size of the offline dictionary file. The use of strong and complex passwords might defeat this attack, but the bulk of the end-user population does not use passwords anywhere near strong enough to defeat the offline attack. Furthermore, enforcing strong password policies comes with significant end-user challenges.

A more detailed discussion about offline dictionary attacks can be found in Chapter 8, "Wireless Security Risks."

LEAP is a Cisco proprietary protocol, and despite claims of mutual authentication, the authentication server in reality is never authenticated. LEAP relies on the mutual authentication properties of MS-CHAPv2, which is simply the peer challenge and response.

When configuring a supplicant for LEAP, put simply, we only provide a username and password. There is no configuration for validating a server-side certificate or any information about the AS. An authentication server can easily be impersonated when a supplicant participates in a LEAP authentication. A rogue access point configured for a different authentication server—perhaps one that records usernames and passwords to a log file—would result in a supplicant merrily sending along its user credentials, unaware that the credentials are being intercepted.

As a WLAN security professional, you should never deploy LEAP in a new enterprise network given the options available to you today. If your organization is currently running LEAP, provide a quick migration path for your organization to a WPA/WPA2-based, TLS-tunneled EAP method.

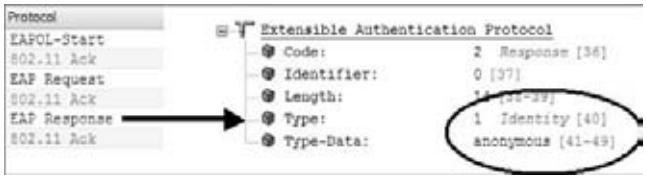
Strong EAP Protocols

It should be clear at this point that the key to enterprise wireless security is leveraging 802.1X. The service provided by 802.1X, as we have also already learned, blocks traffic until a successful authentication transaction occurs. 802.1X is simply a vehicle that enables port blocking and provides the framework for the authentication transaction to occur. The stronger methods of EAP use TLS-based authentication and/or TLS-tunneled authentication. We have already referenced tunneled EAP authentication types earlier in this chapter. In this section, we are going to explore the most common of these types and their inner workings in detail.

Unlike EAP-MD5 and EAP-LEAP, which only have one supplicant identity, EAP methods that use tunneled authentication have two supplicant identities. These two supplicant identities are often called the *outer identity* and *inner identity*. The outer identity is effectively a bogus username, and the inner identity is the true identity of the supplicant. The outer identity is seen in clear text outside the encrypted TLS tunnel, while the inner identity is protected within the TLS tunnel.

As you can see in Figure 4.26, the original EAP standard requires that there always be a clear-text value in the initial EAP-Response frame sent by the supplicant to the authentication server. This clear-text value is the outer identity that travels outside the TLS tunnel. The default value used by most supplicants is "anonymous."

FIGURE 4.26 Outer identity



Although the default value used by most supplicants for the outer identity is "anonymous," the outer identity is usually a configurable setting. Keep in mind that this is not the real username. Some WLAN administrators use funny names such as Donald Duck or Mickey Mouse. Other WLAN administrators use a facility code identifying a group of supplicants. The facility code could be used for troubleshooting efforts of 802.1X supplicant failures and can help you quickly narrow down the facility where the problem was occurring. Other WLAN administrators use the outer identity as a social engineering honeypot.

Do not confuse the encryption used by the TLS tunnel with Layer 2 encryption that is used to protect the payload of 802.11 data frames. The encrypted TLS tunnel is created and only exists for a few milliseconds. The whole purpose of tunneled authentication is to provide a secure channel to protect the user identity credentials. The user credentials are encrypted inside the TLS tunnel. The TLS tunnel is *not* used to encrypt 802.11 data frames. We will now discuss versions of EAP that support tunneled authentication.

Tunneled EAP and a Social Engineering Honeypot

In computer terminology, a *honeypot* is a trap set for potential hackers to detect and possibly counteract unauthorized access of a computer network. EAP methods, such as EAP-PEAP or EAP-TTLS that use tunneled authentication, will always have an outer identity that can be seen in clear text with a WLAN protocol analyzer. A common strategy is to set a social engineering honeypot using the outer identity. The WLAN administrator configures all of the company's supplicants with the same value for the outer identity. The value could be "Shawn Jackman" but there is no user by that name who works at the company. Employees at the company are trained to alert security if anyone ever inquires about an employee named Shawn Jackman. If someone inquires about the imaginary Shawn Jackman, a social engineering attack is occurring and can be further investigated.

EAP-PEAP

EAP-Protected Extensible Authentication Protocol (EAP-PEAP), also known simply as PEAP, creates an encrypted TLS tunnel within which the supplicant's inner identity is validated. Thus the term "protected" is used because the supplicant's identity and credentials are always encrypted inside the TLS tunnel that is established.

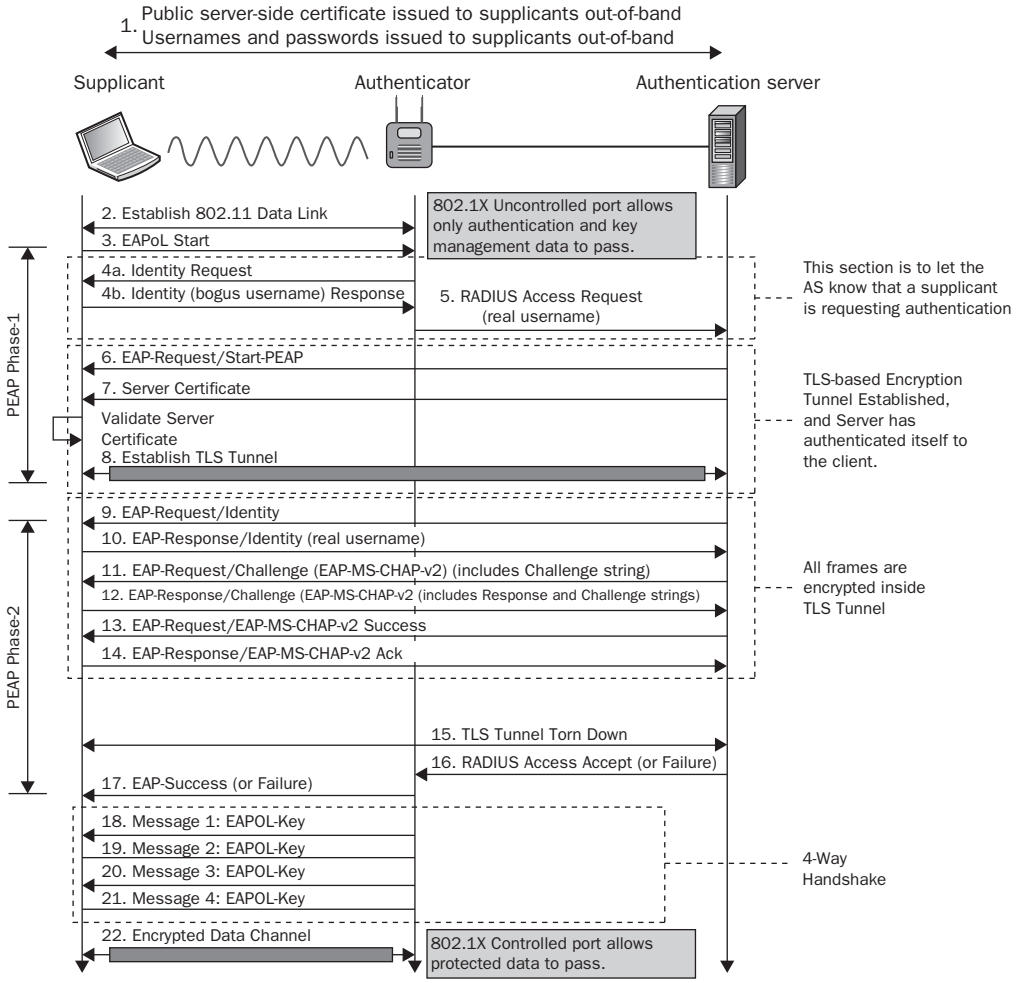
PEAP is probably the most common and most widely supported EAP method used in WLAN security. That is, it is the most popular EAP type that is considered highly secure. The confusion regarding PEAP usually revolves around the fact that there are multiple flavors of PEAP, including these three major versions:

- EAP-PEAPv0 (EAP-MSCHAPv2)
- EAP-PEAPv0 (EAP-TLS)
- EAP-PEAPv1 (EAP-GTC)

PEAP is often referred to as "EAP inside EAP" authentication because the inner authentication protocol used inside the TLS tunnel is also another type of EAP. PEAPv0 and PEAPv1 both refer to the outer authentication method and are the mechanisms that create the secure TLS tunnel to protect subsequent authentication transactions. The EAP protocol enclosed within parentheses is the inner EAP protocol used with each of these three flavors of EAP-PEAP. The main difference between these three major flavors of EAP is simply the inner EAP protocol that is used within the TLS tunnel.

We will discuss the differences between these three versions of PEAP later in this section. First, let's discuss how all flavors of PEAP operate. A key point is that in order to establish the TLS tunnel, a server-side certificate is required for all flavors of PEAP. As shown in Figure 4.27, the EAP-PEAP process involves two phases. Please refer to the figure as we discuss the two phases of EAP-PEAP. We will use EAP-PEAPv0 (EAP-MSCHAPv2), as shown in Figure 4.27.

FIGURE 4.27 EAP-PEAP process



Phase 1

1. The authenticator sends an EAP frame requesting the identity of the supplicant.
2. The supplicant responds with an EAP response frame with the clear-text outer identity that is not the real username and is a bogus username.
3. At this point, the uncontrolled port opens on the authenticator to allow EAP traffic through. All other traffic remains blocked by the controlled port. The authenticator forwards the outer identity response to the AS.

4. The outer identity response cannot inform the AS about the actual identity of the supplicant. It simply informs the AS that a supplicant wants to be validated.
5. The AS sends the server certificate down to the supplicant. The supplicant validates the server-side certificate and therefore authenticates the authentication server.
6. An encrypted point-to-point TLS tunnel is created between the supplicant and the authentication server. Once the TLS tunnel is established, Phase 2 can begin.

Phase 2

1. The AS requests the real identity of the supplicant.
2. The supplicant responds with the inner identity, which is the real username. The real username is now hidden because it is encrypted inside the TLS tunnel.
3. The remaining steps in Phase 2 involve a password challenge from the AS and a hashed response from the supplicant using an authentication protocol within the tunnel. The supplicant credentials are validated by the authentication server. The entire exchange is encrypted within the TLS tunnel.

The whole point of Phase 2 is to validate the supplicant credentials while encrypted within the TLS tunnel. The inner identity, or real username, is protected and therefore hidden. Whatever authentication method is used inside the tunnel is also protected; therefore, any offline dictionary attacks are ineffective in obtaining the password.

PEAP has an interesting history. It begun as a joint proposal by Cisco, Microsoft, and RSA Security. It is reported that Microsoft and Cisco didn't completely agree on every detail and subsequently Microsoft implemented PEAPv0 using MS-CHAPv2 as the inner authentication method. MS-CHAPv2 is Microsoft's own version of CHAP. As Microsoft is the dominant player in both client and server operating systems providing built-in support, this has led to the success of EAP-PEAPv0 (EAP-MS-CHAPv2). Cisco split from the original specification, PEAPv1, which predominantly uses EAP-GTC as the inner authentication method.

It is no secret that the Microsoft Windows operating system has dominated the client platforms that most of us use. Microsoft has been a big proponent of PEAP. Microsoft has included support for PEAP since Windows 2000, and has continued support ever since then. RADIUS server vendors quickly recognized this fact, and every major enterprise RADIUS platform has included support for Microsoft's version of PEAP for many years now. EAP-PEAPv0 (EAP-MS-CHAPv2) is supported in client operating systems such as Macintosh OS X, Windows CE, Windows Mobile, Windows 2000, Windows 2003, XP, Vista and, of course, the new Windows 7 OS. One might consider this list a fairly large chunk of the client population, no?

We will now discuss the differences between the various versions of PEAP. As mentioned earlier, PEAP is often referred to as "EAP inside EAP" authentication because the inner authentication protocol used inside the TLS tunnel is also another type of EAP. The only real difference is the inner EAP protocol that is used within the TLS tunnel. PEAPv0 and PEAPv1 both refer to the outer authentication method and are the mechanisms that create the secure TLS tunnel to protect subsequent authentication transactions. PEAPv0 supports

inner EAP methods of EAP-MSCHAPv2and EAP-TLS while PEAPv1 supports the inner EAP method of EAP-GTC. All versions of PEAP require a server-side certificate, and all versions of PEAP operate using the two phases described earlier.

EAP-PEAPv0 (EAP-MSCHAPv2)

As mentioned earlier, Microsoft's *EAP-PEAPv0 (EAP-MSCHAPv2)* is the most common form of PEAP. The protocol used for authentication inside the tunnel is EAP-MSCHAPv2. What is the difference between the normal MS-CHAPv2 protocol and the EAP-MSCHAPv2 protocol? For all practical purposes, they basically operate in the same manner and use the same hash algorithm. However, it should be noted that EAP-MSCHAPv2 is considered a separate protocol. The credentials used for this version of PEAP are usernames and passwords. Client-side certificates are not used and are not supported.

EAP-PEAPv0 (EAP-TLS)

This is another type PEAP from Microsoft. *EAP-PEAPv0 (EAP-TLS)* uses the EAP-TLS protocol for the inner-tunnel authentication method. EAP-TLS requires the use of a client-side certificate. The client-side certificate is validated inside the TLS tunnel. No username is required for validation because the client-side certificate serves as the user credentials. In a later section, you will also learn that EAP-TLS can be used as a standalone EAP authentication protocol.

EAP-PEAPv1 (EAP-GTC)

Cisco's version of PEAP uses yet another different type of EAP for the inner tunnel authentication. *EAP-PEAPv1 (EAP-GTC)* uses *EAP-Generic Token Card (EAP-GTC)* for the inner-tunnel authentication protocol. EAP-GTC is defined in the IETF RFC 3748 and was developed to provide interoperability with existing security token device systems that use one-time passwords (OTP) such as RSA's SecurID solution. The EAP-GTC method is intended for use with security token devices, but the credentials can also be a clear-text username and password. In other words, when EAP-GTC is used within a PEAPv1 tunnel, normally the credentials are a simple clear-text username and password.

Other versions of PEAP also exist. Other EAP protocols, such as EAP-POTP, can also be used for the inner-tunnel authentication method. EAP-POTP will be discussed later in this chapter.

Initially there were numerous compatibility issues because of the different types of PEAP. However, in practice you will be hard-pressed to find a case where you need to consider what PEAP version you are using anymore. Most RADIUS server vendors now support all versions of PEAP.

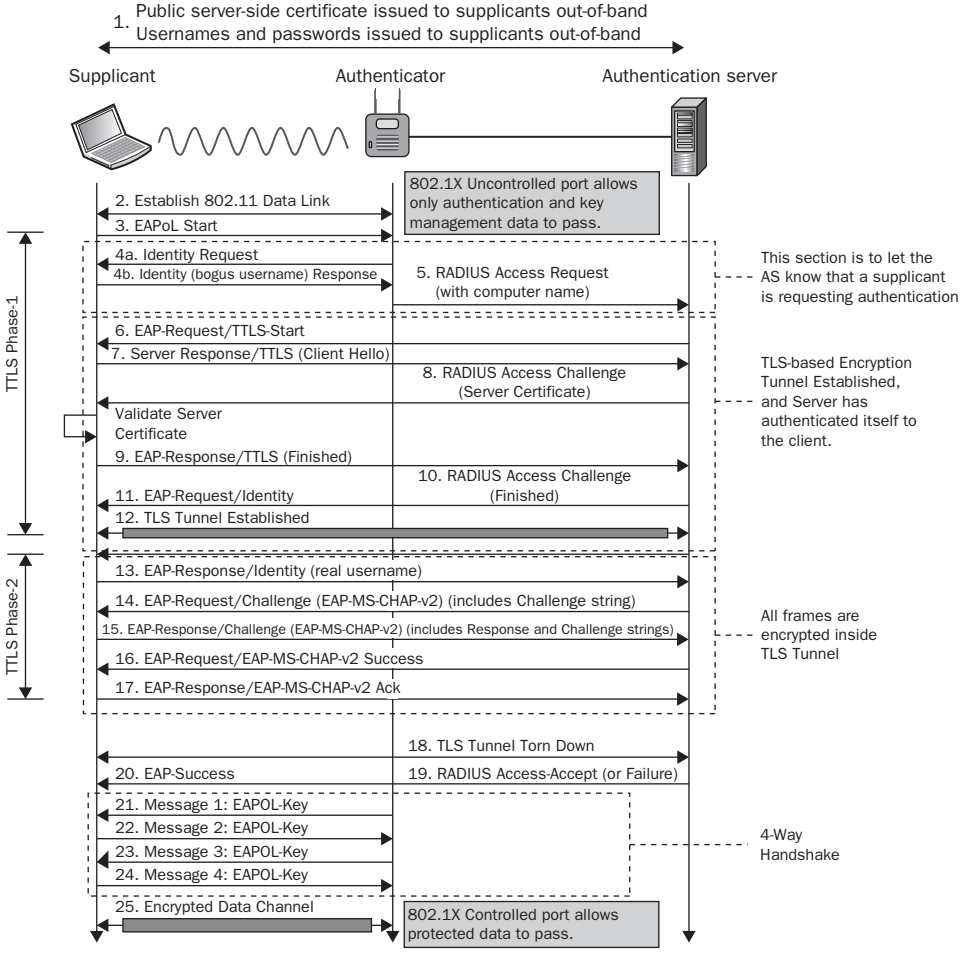
Likewise, most enterprise supplicant software solutions also support all versions of PEAP. However, the internal Microsoft WZC supplicant only supports the Microsoft versions of PEAP. There is another problem with the Microsoft WZC supplicant. As you have learned, PEAP uses an outer and inner identity. The inner identity is hidden within the TLS tunnel and the outer identity is seen in clear text. All supplicants have the ability to configure the outer identity with a bogus username except for the Microsoft WZC supplicant. The WZC uses the same username for both the inner and outer

identity. Therefore, the real username can always be seen when using the Microsoft WZC supplicant. This is a security risk and once again another reason the authors of this book recommend that the built-in Microsoft WZC supplicant be disabled at all times. Although more expensive, a third-party supplicant solution will always be the more secure answer.

EAP-TTLS

EAP-Tunneled Transport Layer Security (EAP-TTLS) was originally designed by Certicom and Funk Software (which is now owned by Juniper Networks) and is defined in RFC 5281. As with PEAP, it also uses a TLS-tunnel to protect less secure inner authentication methods. As shown in Figure 4.28, EAP-TTLS also uses two phases of operation very similar to EAP-PEAP.

FIGURE 4.28 EAP-TTLS process



The differences between EAP-TTLS and EAP-PEAP are fairly minor when analyzing them from a high level. The biggest difference is that EAP-TTLS supports more inner authentication methods, such as the legacy methods of PAP, CHAP, MS-CHAP, and MS-CHAPv2. EAP-TTLS also supports the use of EAP protocols as the inner authentication method. Figure 4.28 shows EAP-MSCHAPv2 being used for inner authentication; however, multiple authentication methods are supported within the TLS tunnel.

Remember that EAP-PEAP *only* supports EAP protocols for inner authentication while EAP-TTLS supports just about anything for inner authentication. Server-side certificates are required with EAP-TTLS to create the TLS tunnel, and client-side certificates are optional. Depending on the type of inner authentication method used, client-side certificates can be used as the protected supplicant credentials within the tunnel. Normally, however, the supplicant credentials are usernames and passwords because it is far easier to implement.

EAP-TTLS has been widely deployed, and it is likely to be encountered in many enterprise WLANs. While EAP-TTLS is almost identical to EAP-PEAP, it doesn't enjoy the native support with Windows operating systems. This has resulted in relatively much less market penetration than other protocols. If the integrated Microsoft WZC is not used as a supplicant, EAP-TTLS might be an option to consider. All major enterprise RADIUS servers seem to have built-in support for EAP-TTLS as well as most other supplicants.

EAP-TLS

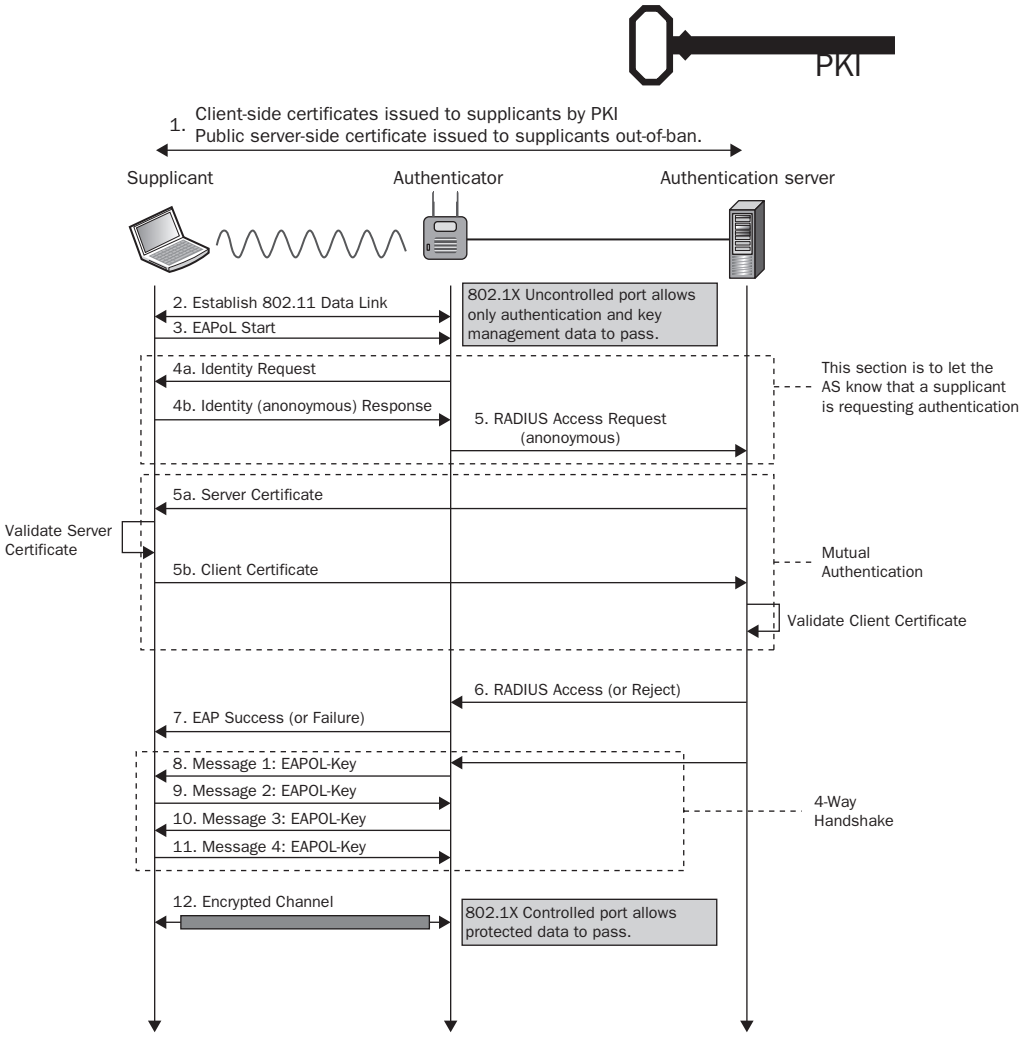
EAP Transport Layer Security (EAP-TLS) is defined in RFC 5216 and is a widely used security protocol. It is largely considered one of the most secure EAP methods used in WLANs today. This, however, comes at a cost.

EAP-TLS requires the use of client-side certificates in addition to a server certificate. Implementing a server-side certificate is not much of a burden, and EAP-TLS has the same server-side certificate requirement as EAP-PEAP and EAP-TTLS. The problem is that having a unique digital certificate for each client requires a great deal of planning, infrastructure, and staff time relative to all the other EAP methods.

The biggest factor when deciding to implement EAP-TLS is whether an enterprise PKI infrastructure is already in place. This would usually, and optimally, include separate servers in a high-availability server cluster. Furthermore, access to these servers is critically important and must be guarded just like a master password list. Quite literally, these servers will have the certificate store, which includes the private keys for the entire PKI infrastructure. Therefore, even though EAP-TLS is widely considered secure, it can only be as secure as the certificate store.

Most enterprises consider managing, securing, and maintaining a PKI to be an unwanted burden. Therefore, unless one was already in place, EAP-TLS would not likely be a WLAN security professional's first recommendation. Figure 4.29 depicts the EAP-TLS process.

FIGURE 4.29 EAP-TLS process



There are a few noteworthy points about the EAP-TLS protocol. From this process, you will notice that the AS presents its public server-side certificate to the client first. If this certificate is not from a source that the client trusts, the supplicant can end the conversation immediately. The same goes for the AS. If the AS does not like the identity of the client-side certificate, it will reject the authentication attempt after the client has been given the first right of refusal.

An AS configured for EAP-TLS will typically allow validation of the client-side certificate by comparing one or more of the following in the user certificate:

- Certificate Subject Alternative Name (SAN)
- Certificate Subject Common Name (CN)
- Certificate Binary—a binary comparison to what's included with the user object in LDAP or Active Directory database to what the supplicant presents

Also, there isn't necessarily a tunnel where an inner authentication takes place like the other TLS tunnel-based EAP types. However, there is an optional *privacy* mode where a TLS handshake can be established before the client identity is passed. When privacy mode is established, a typical TLS tunnel is also created as in PEAP and EAP-TTLS. However, the privacy method is generally not implemented by vendors.

Using client certificates is optional with EAP-TTLS and some flavors of EAP-PEAP. However, using a tunnel for a client certificate is not necessary. It is typically recommended to deploy EAP-TLS when using client-side certificates because of the wide support for the protocol.

An important point to mention is Microsoft's implementation of Certificate Auto-enrollment. Microsoft built a feature into their Active Directory solution when using their Certificate Authority (CA) product (free with Windows Server products) to auto-publish client certificates. This means that the biggest problem with EAP-TLS—deploying certificates to each end-user device—has been mostly automated with Microsoft end-user devices. Keep in mind that only Domain objects will be applicable for this feature and the client-side certificate will have to be installed manually with other non-Microsoft WLAN clients. A more detailed explanation about client-side certificates and how they work within a PKI can be found in Chapter 12.

EAP-FAST

Cisco initially developed the *EAP-Flexible Authentication via Secure Tunneling (EAP-FAST)* protocol, and it has been a proprietary protocol until fairly recently. No, "FAST" doesn't mean that it is necessarily faster than other EAP types, but WOW, what a brilliant marketing name. IETF RFC 4851 was filed in an attempt to standardized EAP-FAST, and it appears that the efforts have paid off. In a press release in May 2009, the Wi-Fi Alliance formally announced that EAP-FAST (along with EAP-AKA) will be added to the WPA2 interoperability certification.

Client support for EAP-FAST still pales in comparison to PEAP, but it is yet another growing option now that it has even been formally adopted by Juniper's Steel Belted RADIUS platform and other authentication server platforms. EAP-FAST is clearly stated in public documents by Cisco that it was designed to be a convenient, easy-to-implement replacement for LEAP. When it was discovered that LEAP can be easily cracked, something had to be done quickly.

EAP-FAST provides for both mutual authentication and tunneled authentication just like EAP-PEAP and EAP-TTLS. However, EAP-FAST does not use standards-based X.509 digital certificates to create the TLS tunnel. Instead, EAP-FAST uses PACs.

PACs

A *Protected Access Credential (PAC)* is a cousin of a digital certificate. Actually, it is a shared secret. Since EAP-FAST is the only EAP type that uses PACs, it is prudent to discuss a bit of the EAP-FAST process with respect to how it is used in authentication server identity validation for the supplicant.

A PAC can consist of three components:

Shared Secret—The PAC-Key A preshared key between the client and the authentication server.

Opaque Element—The PAC-Opaque A variable-length data element sent during tunnel establishment where the AS can decode the required information to validate the client's identity.

Other Information—PAC-Info A variable-length data element that minimally provides the authority identity of the PAC issuer (usually the master RADIUS server, which would be the PAC Authority). May also contain the PAC-Key lifetime.

As shown in Figure 4.30, EAP-FAST operates in three phases:

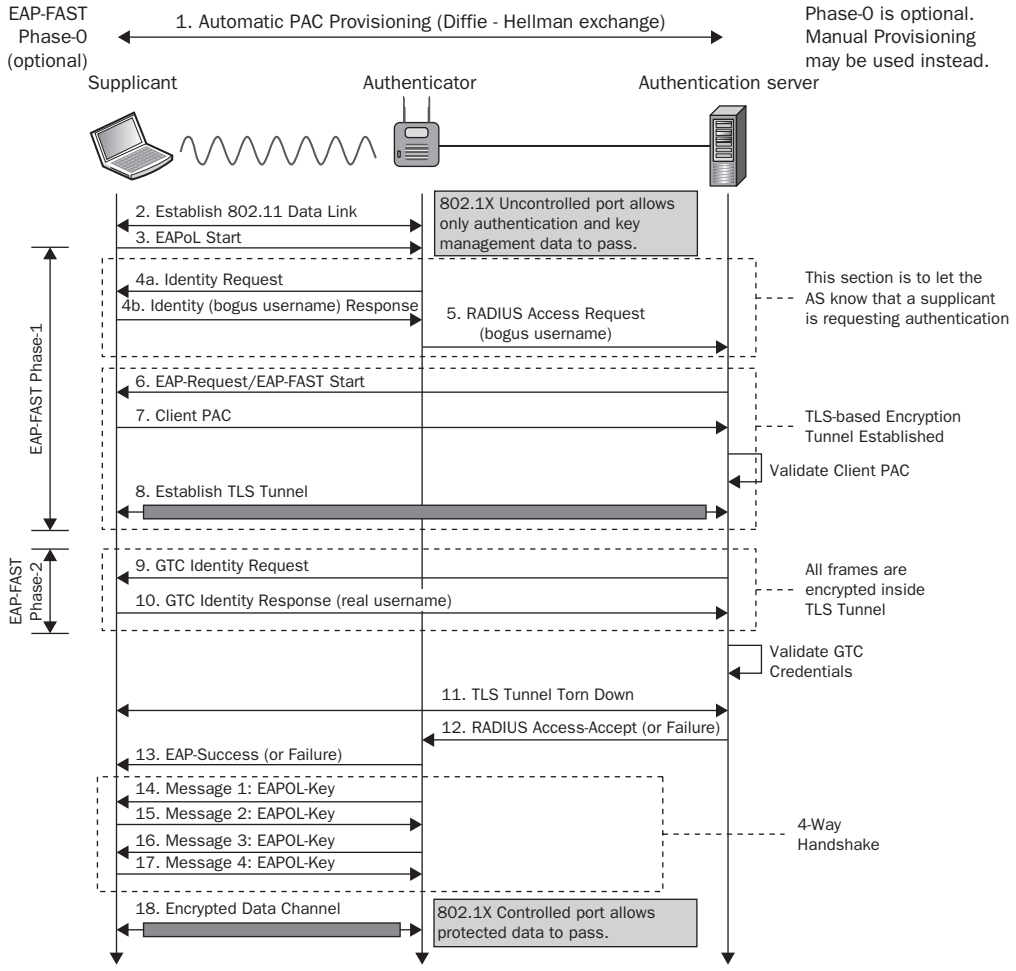
Phase 0 This phase is used for automatic PAC provisioning. Each supplicant is automatically sent a unique client PAC using an anonymous Diffie-Hellman exchange. After each client station initially receives a PAC, clients will skip Phase 0 in subsequent logins. Phase 0 is an optional phase, and all PACs can also be installed on the clients manually.

Phase 1 During this phase, the supplicant sends the outer bogus identity to let the AS know that a client seeks validation. The client and the AS negotiate using symmetric key encryption from the PAC shared secret (PAC-Opaque). The result of this negotiation is the establishment of an encrypted TLS tunnel.

Phase 2 The supplicant is then validated within the encrypted tunnel. EAP-FAST supports several inner authentication methods including client-side certificates just as EAP-TLS does. The authentication protocol normally used inside the tunnel is EAP-GTC when username and passwords serve as the client identity information. A token-based solution is also a possibility.

Let's discuss manual and automatic PAC provisioning in a little more detail. The client PACs referenced above are created on the RADIUS server using a server-side master key and are unique to each client identity. After they have been created, they must be *installed* on each supplicant much like a client-side certificate is done. The client PACs can be manually installed by the WLAN administrator on each separate machine, and there will be no need for the optional Phase 0. Clients that already have a PAC file would proceed directly to Phase 1. However, if the WLAN administrator enables *automatic PAC provisioning* in Phase 0, the client PACs are installed automatically.

FIGURE 4.30 EAP-FAST process



Wow, this sounds great, but the problem is how does the client know that it is talking to a valid RADIUS server? If you use EAP-FAST with auto-provisioned PAC files, you are allowing your clients to auto-provision from an unknown and perhaps untrusted server.

Automatic PAC provisioning is performed using an anonymous Diffie-Hellman exchange whereby the client simply has to trust the person providing the PAC. This subjects EAP-FAST to man-in-the middle attacks during Phase 0. Despite the risks of Phase 0, most organizations using EAP-FAST typically deploy using automatic PAC provisioning because they are seeking the convenience provided by EAP-FAST. Auto-provisioning is a configurable option on the RADIUS server. However, the problem is that most client supplicants do not have any administrative control over enforcing this, even if the RADIUS server did not allow automatic PAC provisioning.

As mentioned earlier, if EAP-FAST is deployed without the optional phase 0, the IT administrator will have to deploy PAC files manually to each machine. Doing this sacrifices the convenience of EAP-FAST. If you were to do all of that, why wouldn't you just use a more standardized and much more widely acceptable protocol like EAP-TLS or EAP-PEAP? The amount of effort and coordination involved to accomplish this is ridiculous. It would be far easier and logical to use EAP-PEAP, EAP-TTLS, or EAP-TLS. Even though EAP-FAST is not proprietary, it is normally deployed in enterprise environments that use a Cisco infrastructure.

Some organizations will use Phase 0 and automatic PAC provisioning during the initial installation of the WLAN and then disable automatic PAC provisioning. However, it should be noted that the only way EAP-FAST can be considered relatively secure is if, and only if, each PAC was deployed manually and automatic PAC provisioning was disabled.

There is another point to mention about EAP-FAST. A key component of this protocol revolves around PACs and distributing them to clients. What is truly unique about EAP-FAST is that the PAC file contains a shared secret *instead* of a certificate. When using a PKI, asymmetric encryption must be used to decrypt the client identity response. In other words, the AS will use its private key, that only it has, to decrypt the supplicant's response that is encrypted using the AS public certificate.

The computational overhead involved in this asymmetric encryption process is expensive. EAP-FAST uses a symmetric encryption algorithm based on the shared secret of each client's unique PAC. Therefore, there is technically some performance advantage to using EAP-FAST because the tunnel setup acts more like a TLS session resumption because a shared secret between the supplicant and AS is already known.

From experience, a client authentication without using Opportunistic Key Caching (OKC) or Cisco's CCKM may differ from approximately 250 ms using PEAP versus 225 ms using EAP-FAST under fairly ideal circumstances. As you will learn in other chapters, once a client has already authenticated and OKC or Cisco's CCKM is used, subsequent re-authentications are typically sub 50 ms.

Furthermore, EAP-FAST supplicants must use the appropriate PAC file from its PAC file storage for the appropriate user identity. Since PAC files are based on user identities, a different client identity cannot use the same PAC file or authentication will fail.

EAP-FAST has the potential to be very secure, but it can only be considered secure when not auto-provisioning PAC files.

The CWSP exam tests heavily on the differences of all the various EAP types, both strong and weak. Make sure you understand the processes and capabilities of each Layer 2 EAP protocol. Table 4.3 shows an in-depth comparison of most of the major EAP methods. Please use this chart when studying for the exam.

TABLE 4.3 EAP Comparison Chart

	EAP-MD5	EAP-LEAP	EAP-TLS	EAP-TTLS	PEAPv0 (EAP-MSCHAPv2)	PEAPv0 (EAP-TLS)	PEAPv1 (EAP-GTC)	EAP-FAST
Security Solution	RFC-2284	Cisco proprietary	RFC-2716	IETF draft	IETF draft	IETF draft	IETF draft	IETF draft
Digital Certificates—Client	No	No	Yes	Optional	No	Yes	Optional	No
Digital Certificates—Server	No	No	Yes	Yes	Yes	Yes	Yes	No
Client Password Authentication	Yes	Yes	N/A	Yes	Yes	No	Yes	Yes
PACs—Client	No	No	No	No	No	No	No	Yes
PACs—Server	No	No	No	No	No	No	No	Yes
Credential Security	Weak	Weak (depends on password strength)	Strong	Strong	Strong	Strong	Strong	Strong (if Phase 0 is secure)
Encryption Key Management	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Mutual Authentication	No	Debatable	Yes	Yes	Yes	Yes	Yes	Yes
Tunneled Authentication	No	No	Optional	Yes	Yes	Yes	Yes	Yes
Wi-Fi Alliance supported	No	No	Yes	Yes	Yes	No	Yes	Yes
Man-in-the-Middle Protection	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Dictionary Attack Resistance	No	No	Yes	Yes	Yes	N/A	Yes	Yes
Token support	No	No	Yes	Yes	No	Yes	Yes	Yes

Miscellaneous EAP Protocols

Many other flavors of EAP also exist. For example, there are proprietary protocols such as AirFortress EAP and Cogent Systems Biometrics Authentication EAP. We mentioned earlier that PEAPv1-EAP-GTC can be used with one-time password (OTP) token devices. IETF RFC 4793 defines *EAP-Protected One-Time Password Protocol (EAP-POTP),* which is another EAP method suitable for use with one-time password (OTP) token devices. EAP-POTP may be used as a better alternative for an internal authentication method inside the TLS tunnel of other protocols such as EAP-PEAP or EAP-TTLS.

Some EAP protocols are intended for use in the mobile phone industry. In the sections that follow, we will discuss two EAP methods that are intended for use with cellular networks.

EAP-SIM

EAP-Subscriber Identity Module (EAP-SIM) was primarily developed for the mobile phone industry and more specifically for second-generation (2G) mobile networks. Many of us who have mobile phones are familiar with the concept of a *Subscriber Identity Module (SIM)* card. A SIM card is an embedded identification and storage device very similar to a smart card. SIM cards are smaller and fit into small mobile devices like cellular or mobile phones with a 1:1 relationship to a device at any given time. The *Global System for Mobile Communications (GSM)* is a second-generation mobile network standard. EAP-SIM is outlined in the IETF RFC 4186, and it specifies an EAP mechanism that is based on 2G mobile network GSM authentication and key agreement primitives. For mobile phone carriers, this is a valuable piece of information that can be utilized for authentication. EAP-SIM does not offer mutual authentication, and key lengths are much shorter than the third-generation mechanisms used in third-generation (3G) mobile networks.

EAP-AKA

EAP-Authentication and Key Agreement (EAP-AKA) is an EAP type primarily developed for the mobile phone industry and more specifically for 3G mobile networks. EAP-AKA is outlined in the IETF RFC 4187, and it defines the use of the authentication and key agreement mechanisms already being used by the two types of 3G mobile networks. The 3G mobile networks include the *Universal Mobile Telecommunications System (UTMS)* and *CDMA2000*. AKA typically runs in a SIM module. The SIM module may also be referred to as a User Subscriber Identity Module (USIM) or Removable User Identity Module (R-UIM), which, as discussed earlier, is very similar to a smart card.

AKA is based on challenge-response mechanisms and symmetric cryptography and runs in the USIM or RUIM module. Key lengths can be substantially longer, and mutual authentication has now been included.

In mid-2009, the Wi-Fi Alliance announced the inclusion of EAP-AKA into the WPA2 interoperability suite.

As WLANs are used more and more for voice communications, a protocol that can extend from the mobile network carriers into an enterprise WLAN can provide some advantages. *Fixed Mobile Convergence (FMC)* is a growing market segment targeted at large enterprises whereby dual-mode mobile phones (Wi-Fi-enabled mobile phones) can roam from a mobile network carrier to a WLAN and maintain a call session state. It is still early for enterprise WLANs to support FMC, and it will be interesting to see how EAP-AKA will play a role with these devices. The promise is that with EAP-AKA being standardized in 802.11-based networks, a single user identifier would authenticate the device for both networks.

EXERCISE 4.1

802.1X/EAP Frame Exchanges

In this exercise, you will use a protocol analyzer to view the 802.11 frame exchanges used during an 802.1X/EAP authentication process. The following directions should assist you with the installation and use of WildPackets' OmniPeek protocol analyzer demo software. If you have already installed OmniPeek, you can skip steps 1–5.

1. In your web browser, go to the following URL: `www.wildpackets.com/support/downloads`.
2. Under Product Evals, choose OmniPeek Professional. Fill out the OmniPeek evaluation request. A WildPackets representative will send you an email message with a private download URL.
3. Proceed to the private download URL. Download the OmniPeek Professional demo software to your desktop using FTP. This evaluation copy of OmniPeek will be licensed to work for 30 days. Write down the evaluation copy license serial number.
4. Double-click the installation file `omnp602.exe`, and follow the installation prompts. You must be connected to the Internet to activate the license. You will be asked to enter the evaluation copy license serial number.
5. This exercise will use frame captures that are on the CD that comes with this book. If you would like to use OmniPeek for live captures, you will need to install the proper drivers for your Wi-Fi radio card. Verify that you have a supported Wi-Fi card. Information about the supported drivers can be found at `www.wildpackets.com/support/downloads/drivers`. Review the system requirements and supported operating systems.
6. In Windows, choose Start ➢ Programs ➢ WildPackets OmniPeek, and then click the OmniPeek icon. The OmniPeek application should appear.

EXERCISE 4.1 *(continued)*

7. Click the Open Capture File icon and browse the book's CD. Open the packet capture file called EAP_MD5.pcap.
8. In the left column, click Capture ➢ Packets. Drag the Protocol column so that it can be viewed within the window. Observe the EAP frame exchange in packets 15–25 using EAP-MD5. Notice the lack of EAPOL-key frames. This is because EAP-MD5 uses one-way authentication and dynamic encryption keys are not created. Notice in frames 7–13 that Open System authentication and association occurs prior to the EAP exchange.
9. Double-click on packet 15 to observe the frame details. Scroll down to the field called 802.1X Authentication. Observe that the packet type is an EAPOL-Start frame.
10. Double-click on packet 17 to observe the frame details. Scroll down to the field called 802.1X Authentication. Observe that the packet type is an EAP-Packet frame.
11. Close all open tabs. Click the Open Capture File icon and browse the book's CD. Open the packet capture file called EAP_LEAP.pcap.
12. Double-click on packet 7 to observe the frame details. Scroll down to the field called Extensible Authentication Protocol. Observe that the identity is this EAP-Response frame, which can be seen in clear text. The identity is "airspy." The real username is always seen in clear text when LEAP is used.
13. Close all open tabs. Click the Open Capture File icon and browse the book's CD. Open the packet capture file called EAP_PEAP.pcap.
14. Double-click on packet 13 to observe the frame details. Scroll down to the field called Extensible Authentication Protocol. Observe that the identity is this EAP-Response frame, which can be seen in clear text. The identity is "administrator." This is the outer identity that is always seen in clear text when PEAP is used. This is a bogus username. The real username is hidden inside the encrypted TLS tunnel.
15. Observe the EAPOL-key frames in packets 47–53. These are the frames used to create dynamic encryption keys following the authentication process. Once the supplicant gets validated and the keys are created, the controlled port becomes unblocked.
16. Close all open tabs. Click the Open Capture File icon and browse the book's CD. Open the packet capture file called EAP_TTLS.pcap, and observe the EAP-TTLS frame exchange. Notice the similarity to PEAP.
17. Close all open tabs. Click the Open Capture File icon, and browse the book's CD. Open the packet capture file called EAP_TLS.pcap and observe the EAP-TLS frame exchange.

Summary

WLAN security is still in its infancy relative to more mature mediums like Ethernet and wired networks. 802.1X/EAP enterprise methods currently exist that allow for secure WLAN communication. Hopefully, enough information was presented in this chapter to create more awareness regarding 802.1X framework and Layer 2 EAP authentication methods.

A great deal of maturity is still needed for WLAN supplicant development, including the methods of controlling configuration and management of each individual endpoint. While this is a complex problem to solve, there exists a significant management need for administrators of large numbers of WLAN client devices.

Still, as a WLAN security professional, your ability to understand the complexities of the many protocols involved in WLAN security is paramount. Each protocol has its advantages and drawbacks, which must be mapped to the requirements of each implementation. Furthermore, a proper deployment of each security type must be performed. Simply using a strong EAP type doesn't mean security is achieved.

The key thing to keep in mind is that you need to employ the most secure method possible for your organization based on the abilities of the client devices, end-users, and systems being deployed.

Exam Essentials

Explain the concept of credentials. Understand the differences between something you are, something you have, and something you know. Explain the importance of multifactor authentication.

Understand the concept of AAA. Explain the in detail how authentication is used to validate identity, authorization is used to grant access, and accounting is used for a paper trail.

Describe the 802.1X framework. Explain the roles of the 802.1X components of the supplicant, authenticator, and authentication server. Understand the concept of controlled and uncontrolled virtual ports.

Define the various types of supplicant identity credentials. Describe the many different types of credentials that can be used by a supplicant. This includes username/passwords, client certificates, security tokens, and many more.

Describe the role of server-side certificates. Understand how a server-side certificate is used to validate the authentication server. Understand that the other purpose of the server-side certificate is to create an encrypted TLS tunnel.

Explain all the Layer 2 EAP methods. Be able to explain all the capabilities of each EAP method as well as the differences. Understand why different EAP methods may be used in different situations.

Key Terms

Before you take the exam, be certain you are familiar with the following terms:

accounting

accounting trail

Active Directory (AD)

attribute value pairs (AVPs)

authentication

authentication server (AS)

authentication, authorization, and accounting (AAA)

Authorization

CDMA2000

Challenge Handshake Authentication Protocol (CHAP)

common name (CN)

controlled port

credentials

EAP-Authentication and Key Agreement (EAP-AKA)

EAP-Generic Token Card (EAP-GTC)

EAP-Protected Extensible Authentication Protocol (EAP-PEAP)

EAP-Protected One-Time Password Protocol (EAP-POTP)

EAP-Subscriber Identity Module (EAP-SIM)

EAP-Tunneled Transport Layer Security (EAP-TTLS)

EAP- Flexible Authentication via Secure Tunneling (EAP-FAST)

EAP over LAN (EAPOL)

EAP Transport Layer Security (EAP-TLS)

EAP-Lightweight Extensible Authentication Protocol (EAP-LEAP)

EAP-Message Digest5 (EAP-MD5)

EAP-PEAPv0 (EAP-MSCHAPv2)

EAP-PEAPv0 (EAP-TLS)

EAP-PEAPv1 (EAP-GTC)

Extensible Authentication Protocol (EAP)

Fixed Mobile Convergence (FMC)

Global System for Mobile communications (GSM)

Honeypot

inner identity

integrated circuit card (ICC)

Lightweight Directory Access Protocol (LDAP)

Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)

MS-CHAPv2

multifactor authentication

mutual authentication

Network Access Control (NAC)

one-time password (OTP)

organizational unit (OU)

outer identity

Password Authentication Protocol (PAP)

port-based access control

Protected Access Credential (PAC)

proxy authentication

Public Key Infrastructure (PKI)

Remote Authentication Dial In User Service (RADIUS)

role based access control (RBAC)

Secure Socket Layer (SSL)

security token

shared secret

smart card

Subscriber Identity Module (SIM)

supplicant

Transport Layer Security (TLS)

tunneled authentication

two-factor authentication

uncontrolled port

Universal Mobile Telecommunications System (UTMS)

vendor specific attributes (VSAs)

Wireless Zero Configuration (WZC)

Review Questions

1. Which of these types of EAP use tunneled authentication? (Choose all that apply.)
   - **A.** EAP-LEAP
   - **B.** EAP-PEAPv0 (EAP-MSCHAPv2)
   - **C.** EAP-PEAPv1 (EAP-GTC)
   - **D.** EAP-FAST
   - **E.** EAP-TLS (privacy mode)

2. Which of these types of EAP require a client-side X.509 digital certificate to be used as the supplicant credentials? (Choose all that apply.)
   - **A.** EAP-TTLS
   - **B.** EAP-PEAPv0 (EAP-MSCHAPv2)
   - **C.** EAP-PEAPv0 (EAP-TLS)
   - **D.** EAP-FAST
   - **E.** EAP-TLS (privacy mode)
   - **F.** EAP-TLS (nonprivacy mode)

3. Which of these types of EAP use three phases of operation? (Choose all that apply.)
   - **A.** EAP-TTLS
   - **B.** EAP-PEAPv0 (EAP-MSCHAPv2)
   - **C.** EAP-PEAPv0 (EAP-TLS)
   - **D.** EAP-FAST
   - **E.** EAP-TLS (privacy mode)
   - **F.** EAP-TLS (nonprivacy mode)

4. Which of these types of EAP require a server-side certificate to create an encrypted TLS tunnel?
   - **A.** EAP-TTLS
   - **B.** EAP-PEAPv0 (EAP-MSCHAPv2)
   - **C.** EAP-PEAPv0 (EAP-TLS)
   - **D.** EAP-FAST
   - **E.** EAP-PEAPv1 (EAP-GTC)
   - **F.** EAP-LEAP

5. Which of these types of EAP are susceptible to offline dictionary attacks? (Choose all that apply.)
   - **A.** EAP-SIM
   - **B.** EAP-MD5
   - **C.** EAP-PEAPv0 (EAP-TLS)
   - **D.** EAP-FAST
   - **E.** EAP-PEAPv1 (EAP-GTC)
   - **F.** EAP-LEAP

6. What is the difference between the inner and outer identity?
   - **A.** Only the authentication server provides its credentials in the outer identity response.
   - **B.** The inner identity is only for authentication server credentials provided to the supplicant.
   - **C.** The inner identity must correspond to the outer identity for realm-based authentications.
   - **D.** The outer identity is in plain text; the inner identity is securely transmitted inside a TLS tunnel.
   - **E.** The outer identity is only for authentication server credentials provided to the supplicant.

7. How does a RADIUS server communicate with an authenticator? (Choose all that apply.)
   - **A.** UDP ports 1812 and 1813
   - **B.** TCP ports 1645 and 1646
   - **C.** Encrypted TLS tunnel
   - **D.** Encrypted IPsec tunnel
   - **E.** RADIUS IP packets
   - **F.** EAPOL frames

8. In a point-to-point bridge environment where 802.1X/EAP is used for bridge authentication, what device in the network acts as the 802.1X supplicant?
   - **A.** Nonroot bridge
   - **B.** WLAN Controller
   - **C.** Root bridge
   - **D.** RADIUS server
   - **E.** Layer 3 core switch

9. Which Layer 2 protocol is used for authentication in an 802.1X framework?

A. PAP

B. MS-CHAPv2

C. EAP

D. CHAP

E. MS-CHAP

10. Which of these types of EAP offers support for legacy authentication protocols within the inner TLS tunnel to validate supplicant credentials?

A. EAP-TLS

B. EAP-TTLS

C. EAP-FAST

D. EAP-PEAPv0

E. EAP-PEAPv1

11. When using an 802.11 wireless controller solution, which device would be considered the authenticator?

A. Access point

B. RADIUS database

C. LDAP

D. WLAN controller

E. VLAN

12. For an 802.1X/EAP solution to work properly, which two components must both support the same type of EAP? (Choose two.)

A. Supplicant

B. Authorizer

C. Authenticator

D. Authentication server

13. What does 802.1X/EAP provide when implemented for WLAN security? (Choose all that apply.)

A. Access to network resources

B. Verification of access point credentials

C. Dynamic authentication

D. Dynamic encryption-key generation

E. Verification of user credentials

14. Joel has been hired as a consultant to secure the Barrett Corporation's WLAN infrastructure. Management has asked him to choose a WLAN authentication solution that will best protect the company's network resources from unauthorized users. The company is also looking for a strong dynamic encryption solution for data privacy reasons. Management is also looking for the cheapest solution as well as a solution that is easy to administer. Which of these WLAN security solutions meets all of the objectives required by management? (Choose the best answer.)
    A. EAP-TLS and TKIP/RC4 encryption
    B. EAP-TLS and CCMP/AES encryption
    C. EAP-PEAPv0 (MSCHAPv2) and CCMP/AES encryption
    D. EAP-PEAPv0 (EAP-TLS) and CCMP/AES encryption
    E. EAP-FAST/manual provisioning and CCMP/AES encryption
    F. EAP-MD5 and CCMP/AES encryption

15. What type of credential is used by the authenticator and authentication server to validate each other?
    A. Server-side X.509 digital certificate
    B. PAC
    C. Client-side X.509 digital certificate
    D. Username and password
    E. Security token
    F. Shared secret

16. Which of these types of EAP is designed for a Fixed Mobile Convergence (FMC) authentication solution over an 802.11 WLAN and a 3G cellular telephone network?
    A. EAP-SIM
    B. EAP-GTC
    C. EAP-PEAPv0 (EAP-TLS)
    D. EAP-AKA
    E. EAP-Fortress
    F. EAP-TTLS

17. What are some of the supplicant credentials that could be validated by an authentication server? (Choose all that apply.)
    A. Server-side X.509 digital certificate
    B. PAC
    C. Client-side X.509 digital certificate
    D. Username and password
    E. Security token
    F. Smart card

18. Which of these databases can be used as an authentication server within an 802.1X framework? (Choose all that apply.)

A. RADIUS

B. Supplicant

C. LDAP

D. Active Directory

19. Which of these inner authentication EAP types is intended to be used with an 802.1X framework that uses security token devices as the supplicant credentials? (Choose all that apply.)

A. EAP-GTC

B. EAP-MSCHAPv2

C. EAP-POTP

D. EAP-LEAP

E. EAP-PEAP

F. EAP-TTLS

20. Keith has been hired as a consultant to secure the Parsons Corporation's WLAN infrastructure. Management has asked him to choose a WLAN authentication solution that will best protect the company's network resources from unauthorized users. The end-users will be a variety of WLAN client devices, including barcode scanners and laptops, all using different chipsets. Both Windows and Macintosh operating systems will be supported on the client side. Management is also looking for the cheapest solution as well as a solution that is easy to administer. Which of these WLAN security solutions meets all of the objectives required by management? (Choose the best answer.)

A. EAP-TTLS (MSCHAPv2) and integrated OS supplicants

B. EAP-PEAPv0 (MSCHAPv2) and chipset vendor supplicants

C. EAP-PEAPv0 (MSCHAPv2) and WLAN vendor supplicants

D. EAP-PEAPv0 (MSCHAPv2) and commercial third party supplicants

E. EAP- PEAPv0 (MSCHAPv2) and integrated OS supplicants

Answers to Review Questions

1. B, C, D, E. Tunneled authentication is used to protect the exchange of client credentials between the supplicant and the authentication server within an encrypted TLS tunnel. All flavors of EAP-PEAP use tunneled authentication. EAP-TTLS and EAP-FAST also use tunneled authentication. While EAP-TLS is highly secure, it rarely uses tunneled authentication. Although rarely supported, an optional privacy mode does exist for EAP-TLS, which can be used to establish a TLS tunnel. EAP-MD5 and EAP-LEAP do not use tunneled authentication.

2. C, E, F. EAP-TLS and EAP-PEAPv0 (EAP-TLS) require client-side certificates to be used as the supplicant credentials. Client-side certificates are optional with EAP-TTLS. EAP-FAST does not use X.509 digital certificates. It is typically recommended that you deploy EAP-TLS when using client-side certificates because of the wide support for the protocol.

3. D. EAP-PEAP and EAP-TTLS both use two phases of operation. Phase 1 is used to create an encrypted TLS tunnel, and the supplicant credentials are exchanged during Phase 2. EAP-FAST also uses Phase 1 and 2 operations to accomplish the same goals. However, EAP-FAST also defines an optional Phase 0 that is sometimes used for automatic PAC provisioning.

4. A, B, C, E. All versions of EAP-PEAP and EAP-TTLS require a server-side certificate to create an encrypted TLS tunnel. EAP-FAST uses a Protected Access Credential (PAC) to create the encrypted tunnel as opposed to a server-side certificate. EAP-LEAP and EAP-MD5 do not use a TLS tunnel. EAP-TLS requires a server certificate; however, establishing a TLS tunnel is optional.

5. B, F. EAP-MD5 uses the MD5 hash algorithm to validate the supplicant credentials during a password challenge and response exchange. EAP-LEAP uses the MS-CHAPv2 hash algorithm to validate the supplicant credentials during a password challenge and response exchange. Both hash methods can be cracked with hacker tools. EAP-MD5 and EAP-LEAP do not protect the supplicant validation exchange within a TLS tunnel and are therefore susceptible to offline dictionary attacks.

6. D. Unlike EAP-MD5 and EAP-LEAP, which have only one supplicant identity, EAP methods that use tunneled authentication have two supplicant identities. These two supplicant identities are often called the outer identity and inner identity. The outer identity is a bogus username and the inner identity is the actual username of the supplicant. The outer identity is seen in clear text outside the encrypted TLS tunnel, while the inner identity is protected within the TLS tunnel.

7. A, E. The RADIUS protocol uses UDP ports 1812 for RADIUS authentication and 1813 for RADIUS accounting. These ports were officially assigned by the Internet Assigned Number Authority (IANA). However, prior to IANA allocation of UDP ports 1812 and 1813, the UDP ports of 1645 and 1646 (authentication and accounting, respectively) were used as the default ports by many RADIUS server vendors. TCP is not used. All Layer 2 EAP traffic sent between the RADIUS server and the authenticator is encapsulated in RADIUS IP packets. The encrypted TLS tunnel communications are between the supplicant and the authentication server. IPsec is not used.

8. A. The root bridge would be the authenticator, and the nonroot bridge would be the supplicant if 802.1X/EAP security is used in a WLAN bridged network.

9. C. The supplicant, authenticator, and authentication server work together to provide the framework for 802.1X port-based access control, and an authentication protocol is needed to assist in the authentication process. The Extensible Authentication Protocol (EAP) is used to provide user authentication. The other protocols are all legacy protocols.

10. B. All of these EAP protocols create a TLS tunnel to protect the supplicant credentials. However, only EAP-TTLS offers support for legacy authentication protocols within the TLS tunnel. EAP-TTLS supports the legacy methods of PAP, CHAP, MS-CHAP, and MS-CHAPv2. EAP-TTLS also supports the use of EAP protocols as the inner authentication method. EAP-PEAP *only* supports EAP protocols for inner authentication, while EAP-TTLS supports just about anything for inner authentication. EAP-FAST only supports the use of EAP-GTC within the TLS tunnel.

11. D. WLAN controllers use lightweight controller-based access points, which are like dumb terminals with radio cards and antennas. The WLAN controller is the authenticator. When an 802.1X/EAP solution is deployed in a wireless controller environment, the virtual controlled and uncontrolled ports exist on the WLAN controller.

12. A, D. An 802.1X/EAP solution requires that both the supplicant and the authentication server support the same type of EAP. The authenticator must be configured for 802.1X/EAP authentication, but does not care which EAP type passes through. The authenticator and the supplicant must support the same type of encryption.

13. A, D, E. The purpose of 802.1X/EAP is authentication of user credentials and authorization to access network resources. Although the 802.1X framework does not require encryption, it highly suggests the use of encryption. A by-product of 802.1X/EAP is the generation and distribution of dynamic encryption keys. While the encryption process is actually a byproduct of the authentication process, the goals of authentication and encryption are very different. Authentication provides mechanisms for validating user identity while encryption provides mechanisms for data privacy or confidentiality.

14. C. EAP-TLS and EAP-PEAPv0 (EAP-TLS) both require the use of client-side certificates and therefore would be considered costly and hard to manage. EAP-FAST with manual PAC provisioning would also be difficult to administer. EAP-MD5 is cheap and simple to set up; however, it will only work with static WEP encryption and therefore would not meet the data privacy needs. EAP-PEAPv0 (MSCHAPv2) only requires the use of a server-side certificate and is easy to administer. EAP-PEAPv0 (MSCHAPv2) is the most widely supported EAP protocol available and is therefore cost-effective. CCMP/AES dynamic encryption is now widely supported and meets the data privacy objectives.

15. F. A shared secret is used between the authenticator and the authentication server for the RADIUS protocol exchange. The shared secret exists between the authenticator and the AS so that they can validate each other with the RADIUS protocol. The shared secret is only used to validate and encrypt the communication link between the authenticator and the authentication server. The shared secret is not used at all for any validation of the supplicants.

16. D. EAP-Authentication and Key Agreement (EAP-AKA) is an EAP type primarily developed for the mobile phone industry and more specifically for third-generation (3G) mobile networks. EAP-AKA defines the use of the authentication and key agreement mechanisms already being used by the two types of 3G mobile networks. The 3G mobile networks include the Universal Mobile Telecommunications System (UMTS) and CDMA2000. EAP-SIM was primarily developed for the mobile phone industry and more specifically for second-generation (2G) mobile networks.

17. B, C, D, E, F. Depending on which type of EAP protocol is used, the supplicant identity credentials can be in many different forms, including usernames and passwords, client-side certificates, PACS, security token devices, smart cards, USB devices, proximity badge, and many more.

18. A, C, D. Any Lightweight Directory Access Protocol (LDAP)-compliant database can be used as the authentication server. RADIUS has been around for a very long time in WLAN security, and it is by far the most common method used for authentication servers. However, some WLAN controller vendors allow for direct queries from the authenticator (WLAN controller) to an LDAP database. In fact, there is a growing trend to incorporate Microsoft Active Directory (AD) authentication directly from the authenticator in lieu of going first through a RADIUS server. The supplicant is the client-side application that communicates with the database.

19. A, C. EAP-Generic Token Card (EAP-GTC) was developed to provide interoperability with existing security token device systems that use one-time passwords (OTP), such as RSA's SecurID solution. The EAP-GTC method is intended for use with security token devices, but the credentials can also be a clear-text username and password. EAP-Protected One-Time Password Protocol (EAP-POTP) is another EAP method suitable for use with one-time password (OTP) token devices. EAP-POTP and EAP-GTC are both intended to be used as an inner authentication protocol. EAP-MSCHAPv2 is an inner authentication protocol that only uses usernames and passwords. LEAP, PEAP, and TTLS are not inner authentication protocols.

20. D. EAP-PEAPv0 (MSCHAPv2) only requires the use of a server-side certificate and is very easy to administer. EAP-PEAPv0 (MSCHAPv2) is the most widely supported EAP protocol available and is therefore cost-effective. The main issue is the need for a secure supplicant solution that is easy to administer. Options A and E both suggest the use of an integrated OS supplicant. While that solution is cost-effective, the integrated OS supplicants have known security flaws and may not support all types of EAP. Options B and C would be hard to administer because of the fact that the WLAN clients will be using different chipsets, devices, and OS platforms. Commercial third-party client utilities offer a more robust set of configuration parameters and supported security features than either integrated utilities or bundled utilities. Third-party software supplicants very often can operate on multiple OS platforms and device platforms. For example, a third-party supplicant might be used on a laptop as well as a handheld device such as a barcode scanner. The main disadvantage of a third-party supplicant is the per-user cost.

Chapter 5

802.11 Layer 2 Dynamic Encryption Key Generation

IN THIS CHAPTER, YOU WILL LEARN ABOUT THE FOLLOWING:

- ✓ **Advantages of dynamic encryption**
  - Dynamic WEP
  - Robust security network (RSN)
  - RSN information element
  - Authentication and key management (AKM)
  - RSNA key hierarchy
  - 4-Way Handshake
  - Group Handshake
  - PeerKey Handshake
  - Passphrase-to-PSK mapping
  - Roaming and dynamic keys

The 802.11-2007 standard defines two classes of security methods using pre-RSNA and RSNA algorithms. Pre-RSNA methods use static WEP encryption and the legacy authentication methods that were discussed in Chapter 2, "Legacy 802.11 Security." RSNA security methods use either TKIP/RC4 or CCMP/AES encryption, dynamic key management procedures, and the 802.1X authentication methods that were discussed in Chapter 4, "Enterprise 802.11 Layer 2 Authentication Methods."

In this chapter, you will learn about dynamic WEP, which was a short-term, nonstandard method of dynamic encryption, as well as the standards-based dynamic encryption key management methods that are widely deployed in today's enterprise WLANs.

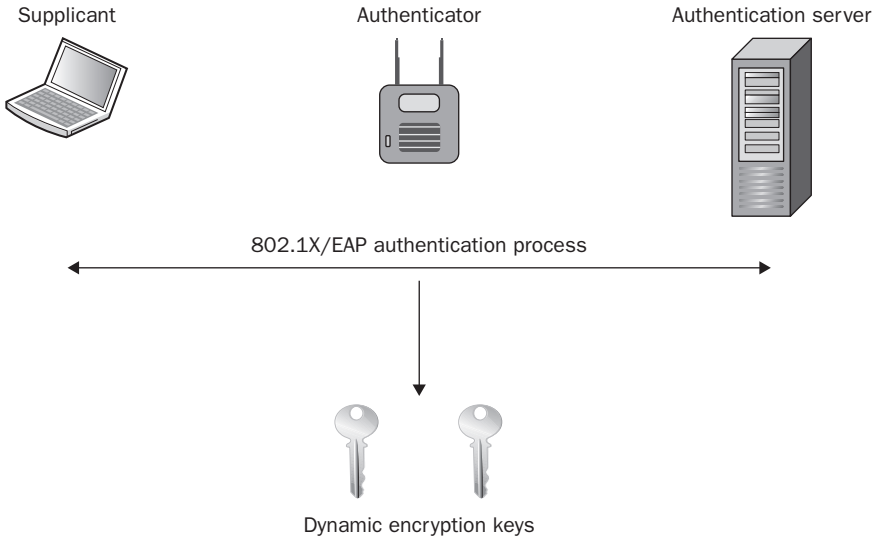
Advantages of Dynamic Encryption

Although the 802.1X/EAP framework does not require encryption, it highly suggests the use of encryption to provide data privacy. You have already learned that the purpose of 802.1X/EAP is authentication and authorization. If a supplicant is properly authenticated by an authentication server using a Layer 2 EAP protocol, the supplicant is allowed through the controlled port of the authenticator and communication at the upper layers of 3–7 can begin for the supplicant. 802.1X/EAP protects network resources so that only validated supplicants are authorized for access. However, as shown in Figure 5.1, an outstanding by-product of 802.1X/EAP can be the generation and distribution of dynamic encryption keys.

EAP protocols that utilize mutual authentication provide "seeding material" that can be used to generate encryption keys dynamically. Mutual authentication is required to generate unique dynamic encryption keys. EAP-TLS, EAP-TTLS, EAP-FAST, EAP-LEAP, and all versions of PEAP utilize mutual authentication and can provide the seeding material needed for dynamic encryption key generation. EAP-MD5 cannot generate dynamic keys because EAP-MD5 only uses one-way authentication.

Until now, you have learned about only static WEP keys. The use of static keys is typically an administrative nightmare, and when the same static key is shared among multiple users, the static key is easy to compromise via social engineering. The first advantage of using dynamic keys rather than static is that they cannot be compromised by social engineering attacks because the users have no knowledge of the keys. The second advantage of dynamic keys is that every user has a different and unique key. If a single user's encryption key was somehow compromised, none of the other users would be at risk because every user has a unique key. The dynamically generated keys cannot be shared between the users.

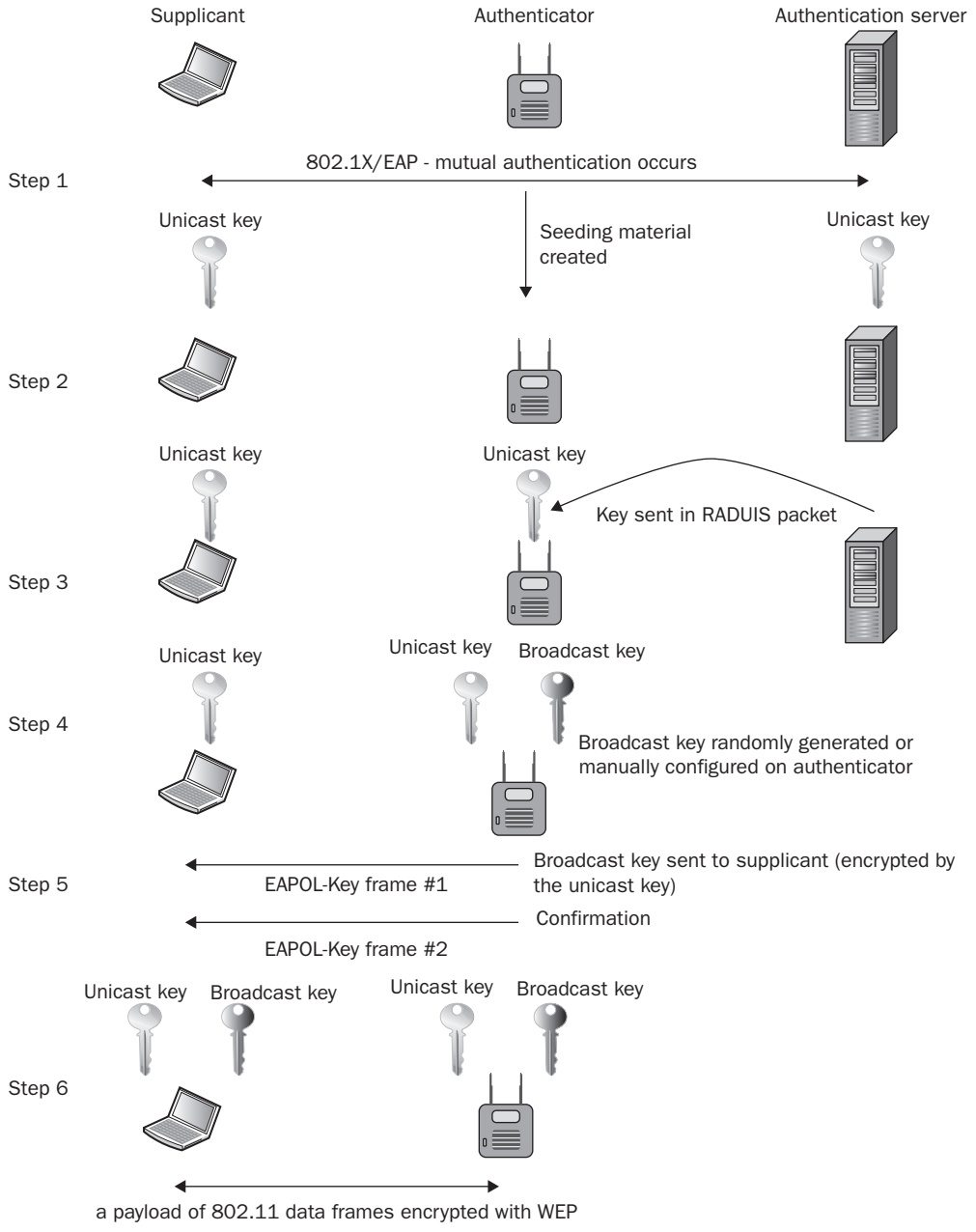
FIGURE 5.1 802.1X/EAP and dynamic keys



In 2004, the 802.11i security amendment was ratified, defining stronger encryption and better authentication methods. The 802.11i amendment, which is now part of the 802.11-2007 standard, fully defines robust security network association (RSNA), which is discussed later in this chapter. RSNA security methods use either TKIP/RC4 or CCMP/AES encryption. Before TKIP/RC4 or CCMP/AES was used, WLAN vendors offered a dynamic key generation security solution using WEP encryption. Many of these solutions were proprietary and did not offer vendor interoperability. Dynamic WEP has never been defined as any part of the 802.11 security and was intended only as a stop-gap dynamic encryption solution until the stronger encryption methods of TKIP/RC4 or CCMP/AES became available.

Dynamic WEP encryption keys can be generated as a by-product of the 802.1X/EAP process. Dynamic WEP is a nonstandard and legacy encryption solution that was mostly used with autonomous access points prior to the widespread use of WLAN controllers. Therefore, the autonomous AP would be considered the authenticator. As shown in step 2 of Figure 5.2, after an EAP frame exchange where mutual authentication is required, both the authentication server and the supplicant now have information about each other due to the mutual authentication exchange of credentials. As shown in step 2, this newfound information is used as *seeding material* or *keying material* to generate a matching dynamic encryption key for both the supplicant and the authentication server. These dynamic keys are generated *per session per user*, meaning that every time a supplicant authenticates, a new key is generated and every user has a unique and separate key. This dynamic session key is often referred to as the *unicast key* because it is the dynamically generated key that is used to encrypt and decrypt all unicast 802.11 data frames.

FIGURE 5.2 Dynamic WEP process



As shown in step 3, after the unicast key is created, the authentication server delivers its copy of the unicast key encapsulated inside a RADIUS packet to the authenticator. The access point and the client station now both have unique unicast keys that can be used to encrypt and decrypt unicast 802.11 data frames. A second key exists on the access point known as the *broadcast key*. As depicted in step 4, the broadcast key can be manually configured on the access point or can be randomly generated. The broadcast key is used to encrypt and decrypt all broadcast and multicast 802.11 data frames. Each client station has a unique and separate unicast key, but every station must share the same broadcast key. As step 5 shows, the broadcast key is delivered from the access point to the client station in a unicast frame encrypted with the client station's unique unicast key. When dynamic WEP is deployed, a two EAPOL-Key frame exchange always follows the EAP frame exchange. The two EAPOL-Key frames are both sent by the authenticator to the supplicant. The first EAPOL-Key frame carries the broadcast key from the access point to the client. The second EAPOL-Key frame is effectively a confirmation that the keys are installed and that the encryption process can begin. Once the client station has both the unicast and broadcast keys, the *MAC service data unit (MSDU)* payload of all 802.11 data frames will now be protected using WEP encryption.

EXERCISE 5.1

Dynamic WEP

In this exercise, you will use a protocol analyzer to view the 802.11 frame exchanges used to create dynamic WEP keys. The following directions should assist you with the installation and use of WildPackets' OmniPeek protocol analyzer demo software. If you have already installed OmniPeek, you can skip steps 1–5.

1. In your web browser, enter the following URL: `www.wildpackets.com/support/downloads`.
2. Under Product Evals, choose OmniPeek Professional. Fill out the OmniPeek evaluation request. A WildPackets representative will send you an email message with a private download URL.
3. Proceed to the private download URL. Download the OmniPeek Professional demo software to your desktop using FTP. This evaluation copy of OmniPeek will be licensed to work for 30 days. Write down the evaluation copy license serial number.
4. Double-click the installation file `omnp602.exe`, and follow the installation prompts. You will need to be connected to the Internet to activate the license. You will be asked to enter the evaluation copy license serial number.
5. This exercise will use frame captures that are on the CD that comes with this book. If you would like to use OmniPeek for live captures, you will need to install the proper drivers for your Wi-Fi radio card. Verify that you have a supported Wi-Fi card.

Information about the supported drivers can be found at `www.wildpackets.com/support/downloads/drivers`. Review the system requirements and supported operating systems. Install the proper driver for your Wi-Fi card.

6. In Windows, choose Start ➢ Programs ➢ WildPackets OmniPeek, and then click the OmniPeek icon. The OmniPeek application should appear.
7. Click the Open Capture File icon and browse the book's CD. Open the packet capture file called `PEAP_WEP.PCAP`.
8. In the left column, click Capture ➢ Packets. Drag the Protocol column so that it can be viewed within the window. Observe that the EAP frame exchange in packets 346–389 is using EAP-PEAP. The access point (authenticator) MAC address is 00:12:43:CB:0F:30. The client radio (supplicant) MAC address is 00:40:96:A3:0C:45.
9. Notice the two EAPOL-Key frames in packets 391 and 393 that are being sent from the access point to the client.
10. Notice that all 802.11 data frames are now encrypted using WEP.

Is Dynamic WEP Encryption Secure?

The generation and distribution of dynamic WEP keys as a by-product of the EAP authentication process has many benefits and is preferable to the use of static WEP keys. When using dynamic WEP, static keys are no longer used and keys do not have to be entered manually. Also, every user has a separate and independent key. If a user's dynamic unicast key was compromised, only that one user's traffic could be decrypted. However, a dynamic WEP key can still be cracked and, if compromised, can indeed be used to decrypt data frames. The current WEP cracking tools such as Aircrack-ng can obtain a WEP key in a matter of minutes. Therefore, dynamic WEP still has severe data privacy risks. Dynamic WEP should only be used with legacy WLAN equipment that does not support the use of TKIP/RC4 or CCMP/AES encryption. Most WLAN vendors have a key interval setting or reauthentication interval setting available on the access point. The configuration setting forces clients to reauthenticate at timed intervals and thus create new dynamic WEP keys. Because WEP can be cracked in such a short time, the key interval settings should be set at about 10 minutes or less on the WLAN access point or controller.

Please understand that dynamic WEP is not the same as RSNA dynamic key management. Later in this chapter, you will learn about RSNAs that define the creation of stronger and safer dynamic TKIP/RC4 or CCMP/AES encryption keys that can also be generated as a by-product of the EAP authentication process.

Robust Security Network (RSN)

The 802.11i amendment, which was ratified and published as IEEE Std. 802.11i-2004, defined stronger encryption and better authentication methods. The 802.11i security amendment is now part of the 802.11-2007 standard. The 802.11-2007 standard defines what is known as a robust security network (RSN) and robust security network associations (RSNAs).

A security association is a set of policies and keys used to protect information. A *robust security network association (RSNA)* requires two 802.11 stations (STAs) to establish procedures to authenticate and associate with each other as well as create dynamic encryption keys through a process known as the *4-Way Handshake*. This association between two stations is referred to as an RSNA. In other words, any two radios must share dynamic encryption keys that are unique between those two radios. CCMP/AES encryption is the mandated encryption method, while TKIP/RC4 is an optional encryption method.

IEEE 802.11-2007 Clause 8

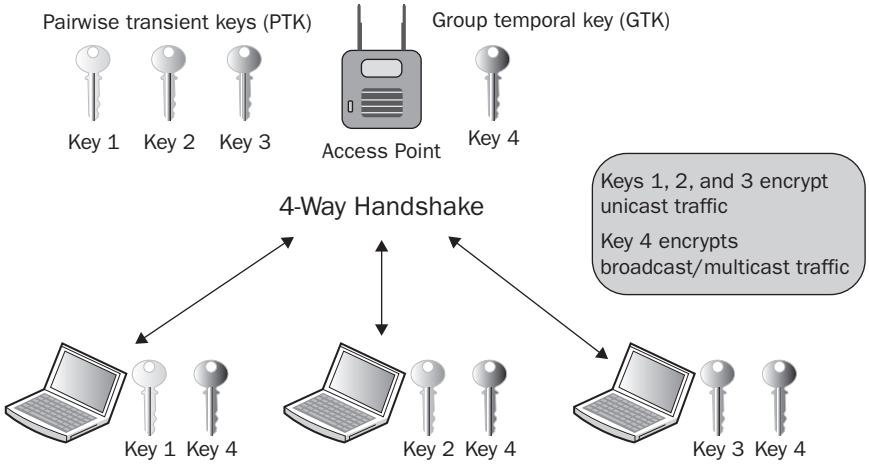
All aspects of robust security network mechanisms can be found in clause 8 of the 802.11-2007 standard.

Anyone who has passed the CWNA certification exam is familiar with the WLAN topologies of a basic service set (BSS) and an independent basic service set (IBSS). *The basic service set (BSS)* is the cornerstone topology of an 802.11 network. The communicating devices that make up a BSS are solely one AP with one or more client stations. Client stations join the AP's wireless domain and begin communicating through the AP. Stations that are members of a BSS have a Layer 2 connection and are called *associated*. The 48-bit (6-octet) MAC address of an access point's radio card is known as the *basic service set identifier (BSSID)*. The BSSID address is the Layer 2 identifier of each individual BSS. Most often, the BSSID is the MAC address of the access point. Do not confuse the BSSID address with the SSID. The *service set identifier (SSID)* is the logical WLAN name that is user configurable, while the BSSID is the Layer 2 MAC address of an AP provided by the hardware manufacturer.

When RSN security associations are used within a BSS, all of the client station radios have unique encryption keys that are shared with the radio of the access point. As shown in Figure 5.3, all the client stations have undergone a unique RSNA process called the 4-Way Handshake where the access point and each client radio has either a unique dynamic

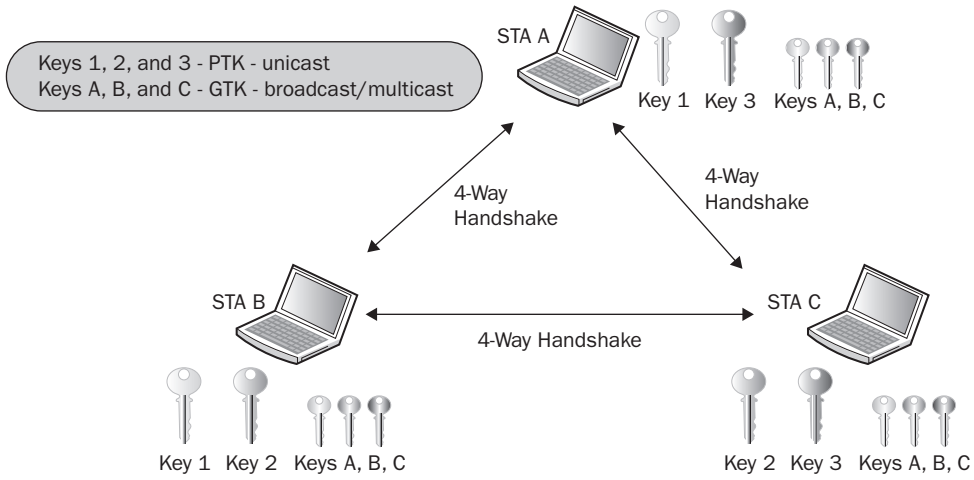
TKIP/RC4 or CCMP/AES key that is shared between the client radio and the access point radio. This key is called the pairwise transient key (PTK) and is used to encrypt/decrypt unicast traffic. All the stations share a broadcast key called the group temporal key (GTK), which is used to encrypt/decrypt all broadcast and multicast traffic. You will learn more about the PTK and GTK keys later in this chapter in the section "4-Way Handshake."

FIGURE 5.3 RSNA within a BSS



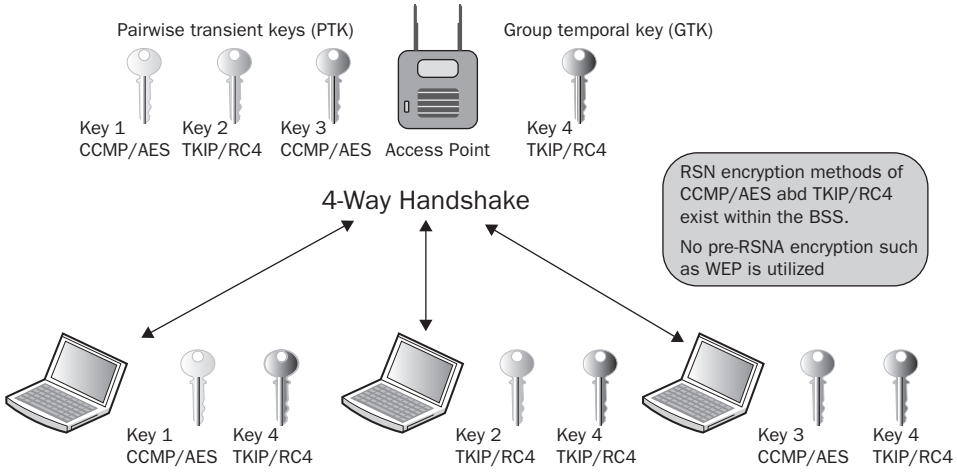
The 802.11 standard also defines a WLAN topology called an *independent basic service set (IBSS)*. The radio cards that make up an IBSS network consist solely of client stations (STAs), and no access point is deployed. An IBSS network that consists of just two STAs is analogous to a wired crossover cable. An IBSS can, however, have multiple client stations in one physical area communicating in an ad hoc fashion. As you can see in Figure 5.4, all the stations within an IBSS have undergone a unique RSNA process (called the 4-Way Handshake) with each other, because all unicast communications are peer to peer. Each station has either a unique dynamic TKIP/RC4 or CCMP/AES pairwise transient key (PTK) that is shared with any other station within the IBSS. In an IBSS, each STA defines its own group temporal key (GTK), which is used for its broadcast/multicast transmissions. Each IBSS station will use either the 4-Way Handshake or the Group Key Handshake to distribute its transmit GTK to its peer stations. PSK authentication is used within the IBSS to seed the 4-Way Handshake. Therefore, every time a client joins an IBSS with a peer station, the client must reauthenticate and create new keys.

FIGURE 5.4 RSNA within an IBSS



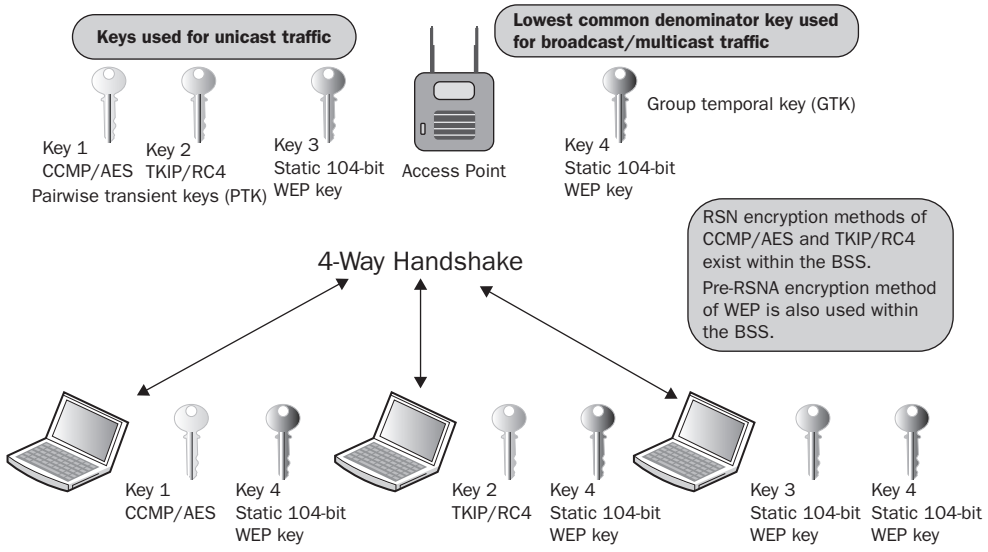
A *robust security network (RSN)* is a network that allows for the creation of only robust security network associations (RSNAs). In other words, a basic service set (BSS) where all the stations are using only TKIP/RC4 or CCMP/AES dynamic keys for encryption would be considered an RSN. Robust security only exists when all devices in the service set use RSNAs. As shown in Figure 5.5, all the stations within the BSS have established an RSNA that resulted in either TKIP/RC4 or CCMP/AES unique dynamic keys. Because only RSNA security is in use, the pictured BSS would be considered a robust security network.

FIGURE 5.5 Robust security network



As you learned in Chapter 2, a pre-RSN security network uses static WEP encryption and legacy authentication methods. A WLAN that uses dynamic WEP encryption keys would also be considered as using pre-RSN security, but the use of dynamic WEP was never defined by either the IEEE or the Wi-Fi Alliance. The 802.11-2007 standard does allow for the creation of *pre-robust security network associations (pre-RSNAs)* as well as RSNAs. In other words, legacy security measures can be supported in the same basic service set (BSS) along with RSN-security-defined mechanisms. A *transition security network (TSN)* supports RSN-defined security as well as legacy security, such as WEP, within the same BSS. As you can see in Figure 5.6, some of the stations within the BSS have established an RSNA that resulted in either TKIP/RC4 or CCMP/AES unique dynamic keys. However, some of the stations are using static WEP keys for encryption. Because both RSNAs and pre-RSNAs are in use, the pictured BSS would be considered a transition security network.

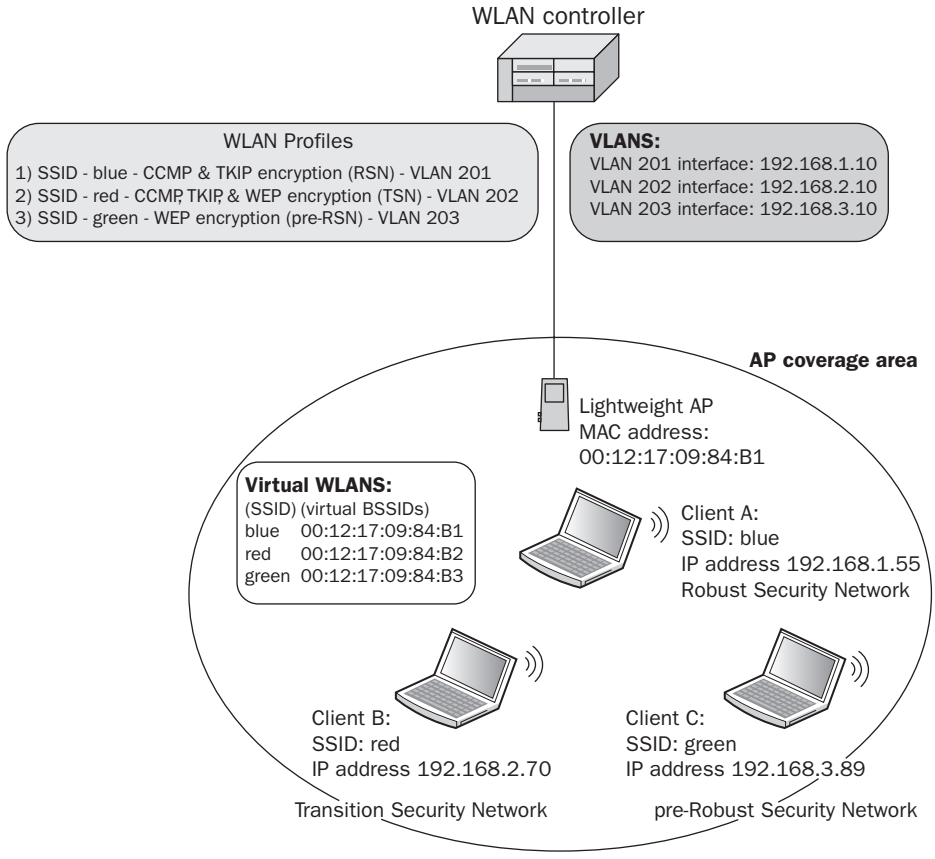
FIGURE 5.6 Transition security network



As you learned earlier in this chapter, each WLAN has a logical name (SSID) and each WLAN BSS has a unique Layer 2 identifier, the basic service set identifier (BSSID). The BSSID is typically the MAC address of the access point's radio card. WLAN controllers have the capability of creating multiple virtual BSSIDs. A WLAN controller allows for the creation of virtual WLANs, each with a unique logical identifier (SSID) that can also be

assigned to a specific VLAN. Because the BSSID is the MAC address of the AP, and because the WLAN controller can support many virtual WLANs on the same physical AP, each virtual WLAN is typically linked with a unique virtual BSSID. Each virtual WLAN has a logical name (SSID) and a unique virtual Layer 2 identifier (BSSID), and each WLAN can be mapped to a unique Layer 3 virtual local area network (VLAN). Each WLAN can also require different types of security associations. Effectively, multiple basic service sets exist within the same coverage cell area of the access point. As shown in Figure 5.7, because multiple virtual BSSIDs exist with different security requirements, an RSN WLAN, a pre-RSNA WLAN, and a TSN WLAN can also exist within the same coverage area of an access point.

FIGURE 5.7 RSN, pre-RSN, and TSN within the same AP cell



Robust Security Networks vs. Transition Security Networks

Most 802.11 radios manufactured between the years of 1997 and 2004 only supported legacy pre-RSNA security that used static WEP encryption. The 802.11i security amendment was ratified in 2004 and full WLAN vendor support for RSNA security became a reality in 2005. All major WLAN vendors fully support RSNA-capable equipment. Any station (STA) that is able to create RSNAs would be considered RSNA-capable. RSNA-capable devices can also use pre-RSNA security to maintain backward compatibility. Therefore, modern WLAN devices support the use of dynamic CCMP/AES encryption, dynamic TKIP/RC4 encryption, and legacy WEP encryption.

As mentioned in Chapter 1, the Wi-Fi Alliance designates the *Wi-Fi Protected Access 2 (WPA2)* security certification. WPA2 certified devices can support CCMP/AES, TKIP/RC4, and WEP encryption. The earlier *Wi-Fi Protected Access (WPA)* certified devices only support TKIP/RC4 and WEP encryption. Any devices that are not WPA or WPA2 certified will only support WEP encryption.

Many legacy WLAN devices are still deployed in enterprise environments that do not support RSNA capabilities. Therefore, the existence of transition security networks (TSNs) that support both RSN-defined security as well as legacy WEP security is still very commonplace. The security of many WLANs is still considered transitional. Legacy devices that only support WEP encryption can often be upgraded to support TKIP encryption with a simple WPA firmware upgrade that is available from the WLAN vendor support website. In most cases, legacy radios cannot be upgraded to support WPA2 because they do not have the processing power to handle CCMP/AES encryption. Whenever possible, deploying a "pure" robust security network using strictly CCMP/AES encryption is highly recommended. However, a robust security network can also still be accomplished if all the devices in the WLAN are WPA/WPA2 certified and only TKIP/RC4 and CCMP/AES dynamic encryption is utilized.

Efforts should be made to upgrade to WPA2-compliant WLAN devices as soon as possible. If legacy WLAN devices such as older wireless barcode scanners are still deployed, static WEP should be used for data privacy and the devices should be segmented into a separate wireless VLAN. MAC authentication security should also be considered for the legacy devices.

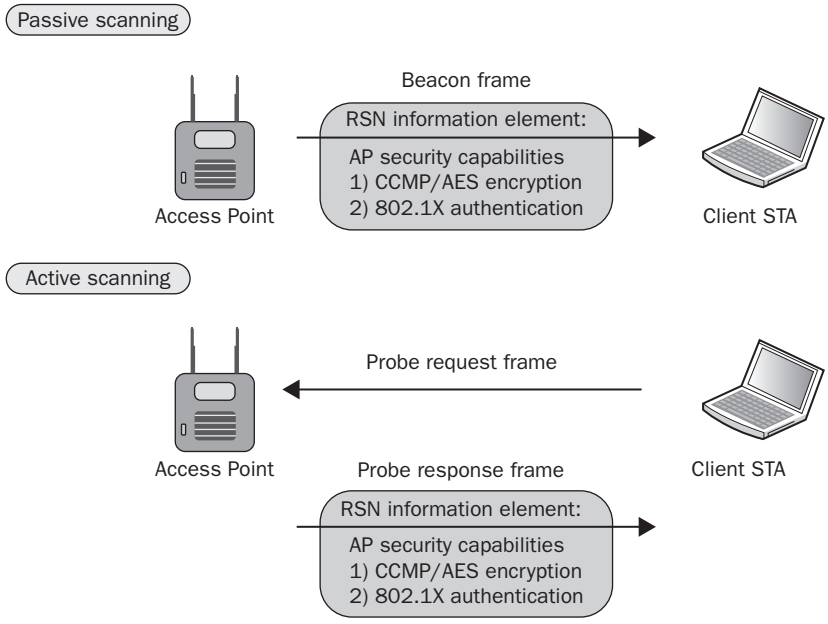
RSN Information Element

Within a BSS, how can client stations and an access point notify each other about their RSN capabilities? RSN security can be identified by a field found in certain 802.11 management frames. This field is known as the *robust security network information element (RSNIE)* and is often referred to simply as the *RSN information element*.

An information element is an optional field of variable length that can be found in 802.11 management frames. The RSN information element can identify the encryption capabilities of each station. The RSN information element will also indicate whether 802.1X/EAP authentication or preshared key (PSK) authentication is being used.

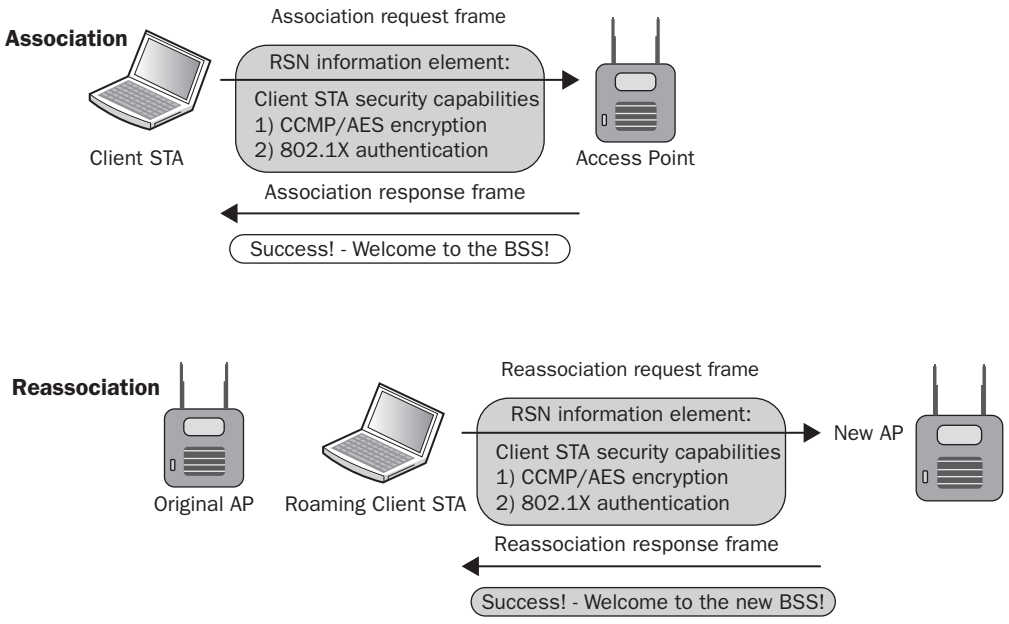
The RSN information element field is found in four different 802.11 management frames: beacon management frames, probe response frames, association request frames, and reassociation request frames. Within a basic service set, an access point and client stations use the RSN information element within these four management frames to communicate with each other about their security capabilities prior to establishing association. As shown in Figure 5.8, access points will use beacons and probe response frames to inform client stations of the AP security capabilities.

FIGURE 5.8 Access point RSN security capabilities



As you can see in Figure 5.9, client stations use the association request frame to inform the access point of the client station security capabilities. When stations roam from one access point to another access point, they use the reassociation request frame to inform the new access point of the roaming client station's security capabilities. The security capabilities include supported encryption cipher suites and supported authentication methods.

FIGURE 5.9 Client station RSN security capabilities



All 802.11 radios will use one cipher suite for unicast encryption and another cipher suite for encrypting multicast and broadcast traffic. Pairwise unicast encryption keys are created that are unique between two stations—the AP and a single client station. The pairwise cipher suite of the RSN information element contains the cipher suite information used by stations for unicast traffic. The cipher suite selector 00-0F-AC-04 (CCMP) is the default cipher suite value. The cipher suite selector 00-0F-AC-02 (TKIP) is optional. A group key is also created that is shared by all stations for broadcast and multicast traffic. The Group Cipher Suite field of the RSN information element contains the cipher suite information used by the BSS to protect broadcast/multicast traffic. The actual creation process of the pairwise and group keys is discussed later in this chapter in the section "4-Way Handshake."

Figure 5.10 shows a capture of a beacon frame from an access point configured to use only CCMP/AES encryption. The RSN information element indicates that CCMP/AES encryption is being used for both the group cipher suite and the pairwise cipher suite. The access point is using the RSN information element to inform all client stations that the AP will be using CCMP encryption for all broadcast/multicast and will also be using CCMP/AES encryption for any unicast traffic. Any client station must support those exact ciphers for the client stations to be able to establish a robust secure network association (RSNA) with the AP and to create dynamic encryption keys. In other words, the client stations must support CCMP/AES encryption to be allowed to join the AP's basic service set.

FIGURE 5.10 RSN Information element—CCMP pairwise and CCMP group cipher

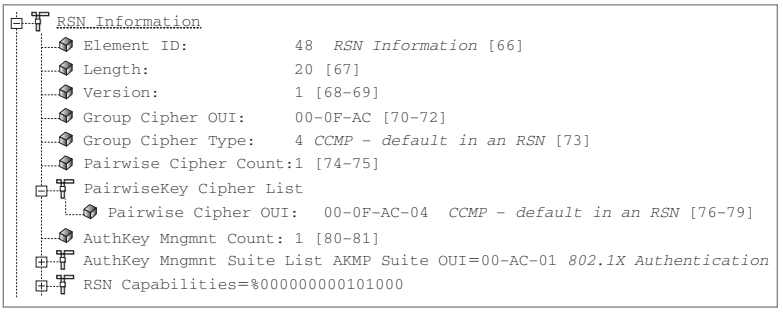
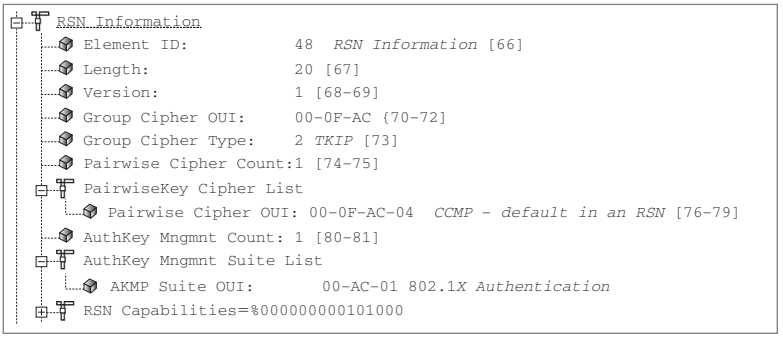


Figure 5.11 shows a beacon frame from an access point configured to support both CCMP/AES and TKIP/RC4 encryption. The RSN information element indicates that TKIP encryption is being used for the group cipher suite. CCMP/AES is the default cipher for the pairwise cipher suite. The access point is using the RSN information element to inform all client stations that the AP will support either CCMP/AES or TKIP/RC4 encryption for any unicast traffic. However, only TKIP/RC4 encryption can be used for broadcast/multicast traffic. In this situation, the client stations must support either CCMP or TKIP to be allowed to join the AP's basic service set. Because all the stations share a single group encryption key for broadcast and multicast traffic, the lowest common denominator must be used for the group cipher. In this case, the group cipher is TKIP.

FIGURE 5.11 RSN information element—CCMP pairwise and TKIP group cipher

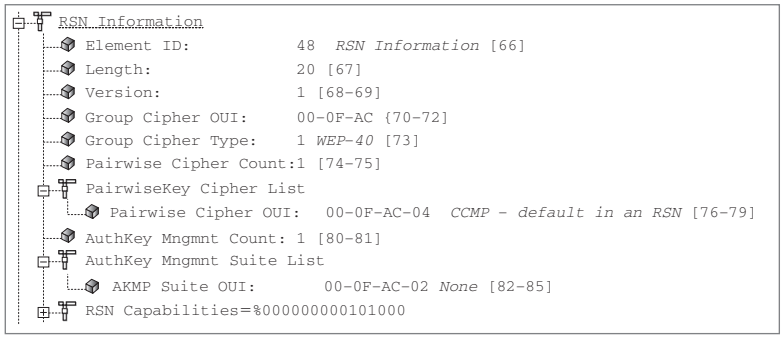


The cipher suite selectors 00-0F-AC-01 (WEP-40) and 00-0F-AC-05 (WEP-104) are used as a group cipher suite in a transition security network (TSN) to allow pre-RSNA devices to join a BSS. For example, an access point might support CCMP, TKIP, and WEP encryption. WPA2-capable clients will use CCMP encryption for unicast traffic between the client STA and the AP. WPA capable clients will use TKIP encryption for unicast traffic between the client STAs and the AP. Legacy clients will use WEP encryption for unicast traffic between the client STAs and the AP. All of the clients will use WEP encryption for the broadcast and multicast traffic. Because all the stations share a single group encryption

key for broadcast and multicast traffic, the lowest common denominator must be used for the group cipher. In the case of a TSN, the group cipher is WEP.

Figure 5.12 shows a capture of a beacon frame from an access point configured to support both CCMP/AES and TKIP/RC4 static WEP encryption using a 40-bit static key. The RSN information element indicates that WEP-40 encryption is being used for the group cipher suite. CCMP/AES is the default cipher for the pairwise cipher suite. The access point is using the RSN information element to inform all client stations that the AP can support CCMP/AES, TKIP/RC4 encryption, or WEP-40 for any unicast traffic. However, only WEP-40 encryption can be used for broadcast/multicast traffic. In this situation, the client stations can support CCMP/AES, TKIP, or WEP-40 and be allowed to join the AP's basic service set.

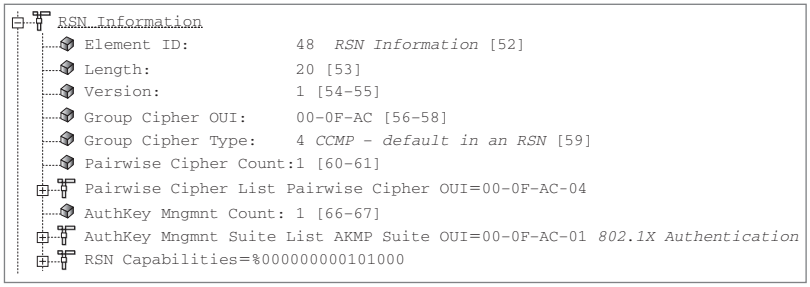
FIGURE 5.12 RSN information element—CCMP pairwise and WEP-40 group cipher



The RSN information element can also be used to indicate what authentication methods are supported. The authentication key management (AKM) suite field in the RSN information element indicates whether the station supports either 802.1X authentication or PSK authentication. If the AKM suite value is 00-0F-AC-01, authentication is negotiated over an 802.1X infrastructure using an EAP protocol. If the AKM suite value is 00-0F-AC-02 (PSK), then PSK is the authentication method that is being used.

Figure 5.13 shows a capture of an association request frame from a client station configured to 802.1X/EAP. The AKM suite field in the RSN information element indicates that 802.1X is the chosen authentication method.

FIGURE 5.13 RSN information element—AKM suite field: 802.1X



We further discuss the RSN information element in Chapter 7, "802.11 Fast Secure Roaming."

Authentication and Key Management (AKM)

The 802.11-2007 standard defines *authentication and key management (AKM)* services. The AKM services consist of a set of one or more algorithms designed to provide authentication and key management, either individually or in combination with higher-layer authentication and key-management algorithms, which are often outside the scope of the 802.11-2007 standard. Non-IEEE-802 protocols may be used for authentication and key management (AKM) services. Many of these non-IEEE-802 protocols are defined by other standards organizations, such as the Internet Engineering Task Force (IETF). In Chapter 4, you learned about the various EAP protocols used within an 802.1X framework for authentication. EAP protocols are also used during AKM services. An *authentication and key management protocol (AKMP)* can be either a preshared key (PSK) or an EAP protocol used during 802.1X authentication.

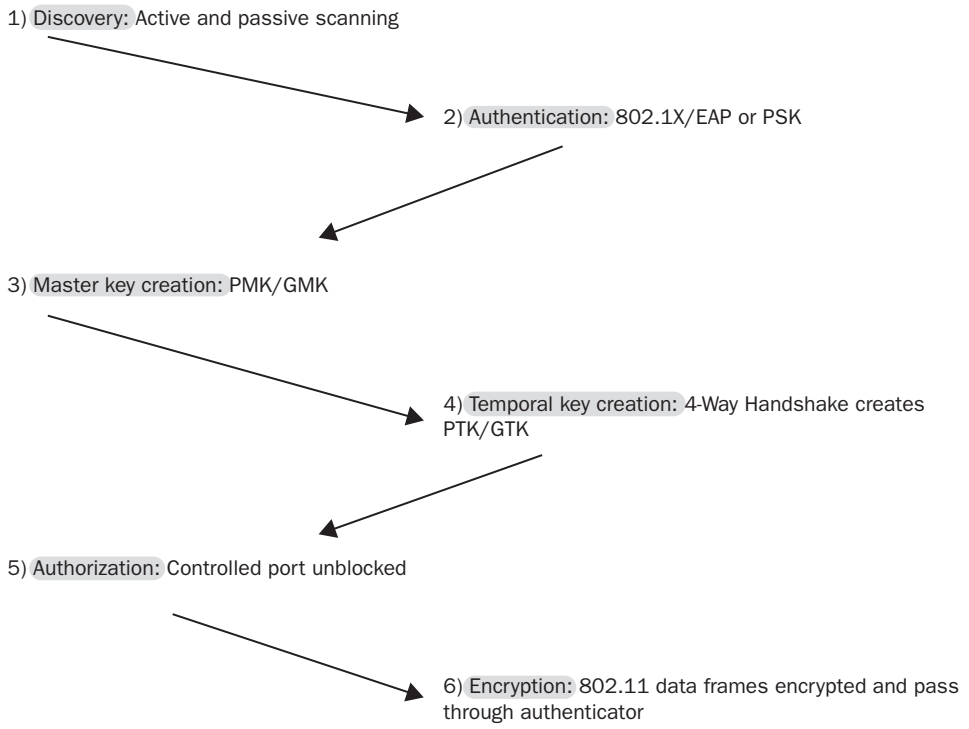
As you have previously learned, the main goal of 802.1X/EAP is twofold:

Authentication Validate the credentials of a client station seeking access to network resources via the WLAN portal.

Authorization Grant access for the client station to network resources via the WLAN portal.

You also have learned that the goal of encryption is to provide data privacy for the MSDU payload in 802.11 data frames. AKM services require both authentication processes and the generation and management of encryption keys. Although authentication and encryption have different goals and are different processes, they are linked together in AKM services. In other words, an authentication process is necessary to generate dynamic encryption keys. The 802.1X/EAP and PSK authentication processes generate the seeding material needed to create dynamic encryption keys. Furthermore, until dynamic encryption keys are created, the controlled port of an 802.1X authenticator will not open. As shown in Figure 5.14, a symbiotic relationship exists between authentication and dynamic encryption. Authorization is not finalized until encryption keys are created and encryption keys cannot be created without authentication.

FIGURE 5.14 Authentication and key management (AKM)—overview

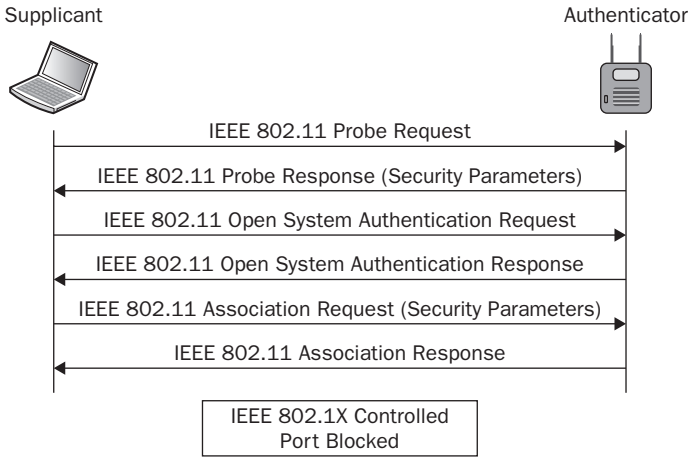


When an 802.1X/EAP authentication solution is used, AKM operations include the following:

Secure Channel The 802.11-2007 standard makes the assumption that the authenticator and authentication server (AS) have established a secure channel. The security of the channel between the authenticator and the AS is outside the scope of the 802.11-2007 standard. Authentication credentials must be distributed to the supplicant and authentication server prior to association. Many of the processes were discussed in Chapter 4.

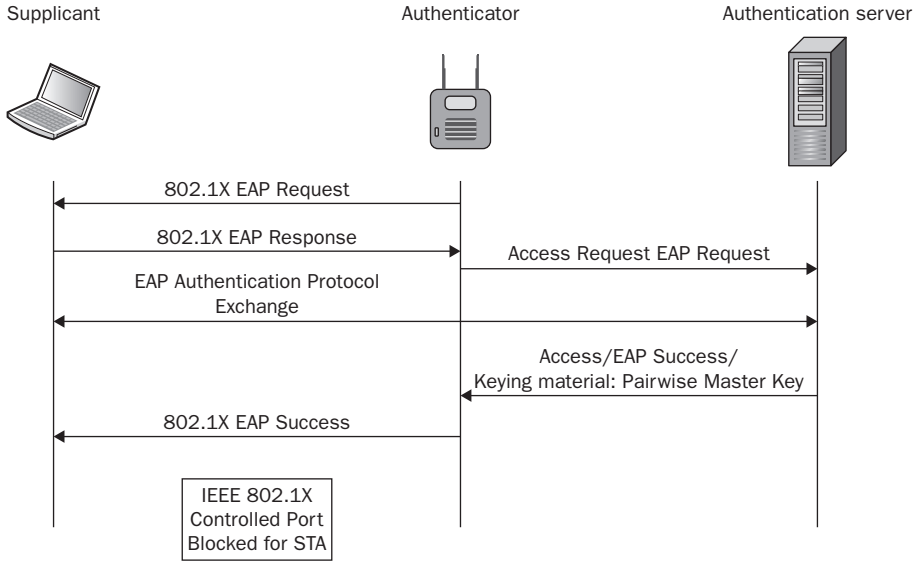
Discovery As shown in Figure 5.15, a client station discovers the access point's security requirements by passively monitoring for beacon frames or through active probing. The access point's security information can be found in the RSN information element field inside beacon and probe response frames. The client station security requirements are delivered to the AP in association and reassociation frames.

FIGURE 5.15 Authentication and key management (AKM)—discovery component



Authentication As shown in Figure 5.16, the authentication process starts when the AP's authenticator sends an EAP-Request or the client station supplicant sends an EAPOL-Start message. As you learned in Chapter 4, EAP authentication frames are then exchanged between the supplicant and authentication server via the authenticator's uncontrolled port. The supplicant and the authentication server validate each other's credentials. The controlled port remains blocked.

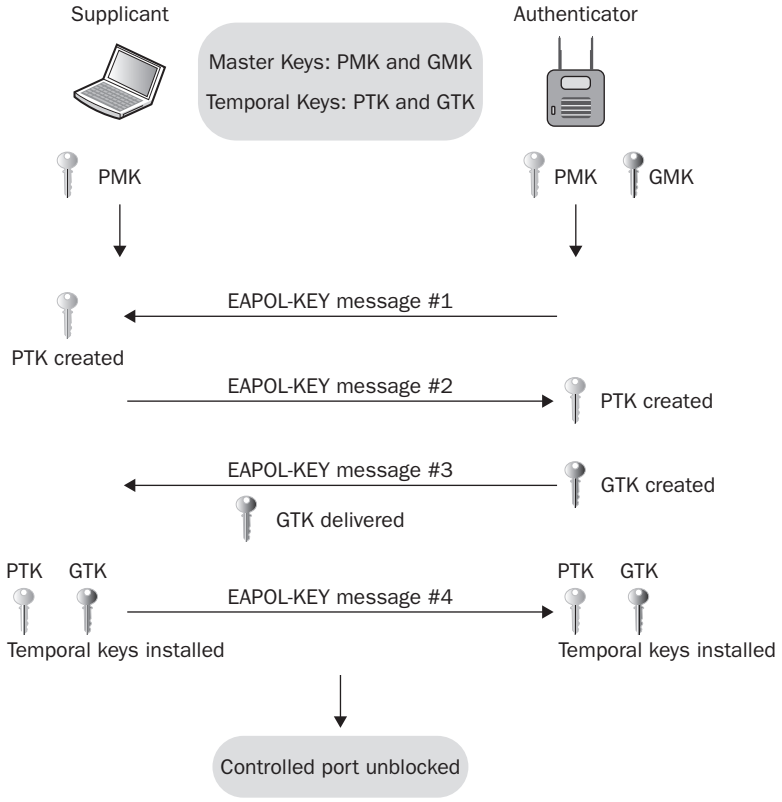
FIGURE 5.16 Authentication and key management (AKM)—authentication and master key generation component



Master Key Generation As you can see in Figure 5.16, the supplicant and authentication server generate a master encryption key called the pairwise master key (PMK). The PMK is sent from the authentication server to the authenticator over the secure channel described earlier. The controlled port is still blocked.

Temporal Key Generation and Authorization As shown in Figure 5.17, a 4-Way Handshake frame exchange between the supplicant and the authenticator utilizing EAPOL-Key frames is used to generate temporary encryption keys that are used to encrypt and decrypt the MSDU payload of 802.11 data frames. The 4-Way Handshake will be discussed in detail in the next section of this chapter. Once the temporal keys are created and installed, the controlled port of the authenticator opens, and the supplicant can then send encrypted 802.11 data frames through the controlled port onward to network resources.

FIGURE 5.17 Authentication and key management (AKM)—temporal key generation and authorization



EXERCISE 5.2

Authentication and Key Management

In this exercise, you will use a protocol analyzer to view all the 802.11 frame exchanges used during AKM services. The following directions should assist you with the installation and use of WildPackets' OmniPeek protocol analyzer demo software. If you have already installed OmniPeek, you can skip steps 1–5.

1. In your web browser, enter the following URL: `www.wildpackets.com/support/downloads`.
2. Under Product Evals, choose OmniPeek Professional. Fill out the OmniPeek evaluation request. A WildPackets representative will send you an email message with a private download URL.
3. Proceed to the private download URL. Download the OmniPeek Professional demo software to your desktop using FTP. This evaluation copy of OmniPeek will be licensed to work for 30 days. Write down the evaluation copy license serial number.
4. Double-click the installation file `omnp602.exe`, and follow the installation prompts. You will need to be connected to the Internet to activate the license. You will be asked to enter the evaluation copy license serial number.
5. This exercise will use frame captures that are on the CD that comes with this book. If you would like to use OmniPeek for live captures, you will need to install the proper drivers for your Wi-Fi radio card. Verify that you have a supported Wi-Fi card. Information about the supported drivers can be found at `www.wildpackets.com/support/downloads/drivers`. Review the system requirements and supported operating systems. Install the proper driver for your Wi-Fi card.
6. From Windows, choose Start ➢ Programs ➢ WildPackets OmniPeek, and then click the OmniPeek icon. The OmniPeek application should appear.
7. Click the Open Capture File icon, and browse the book's CD. Open the packet capture file called `AKM.PCAP`.
8. In the left column, click Capture ➢ Packets. Drag the Protocol column so that it can be viewed within the window. Observe the beacon and probing frames in packets 196–199. Normal open system authentication and association occurs during frames 201–207.
9. Packets 209–253 shows the EAP authentication frames that are exchanged between the supplicant and authentication server via the authenticator's uncontrolled port. The supplicant and the authentication server validate each other's credentials. The controlled port remains blocked.
10. Observe packets 255–261. A 4-Way Handshake exchange between the supplicant and the authenticator utilizing EAPOL-Key frames is used to generate temporary encryption keys. Notice that all 802.11 data frames are now encrypted.

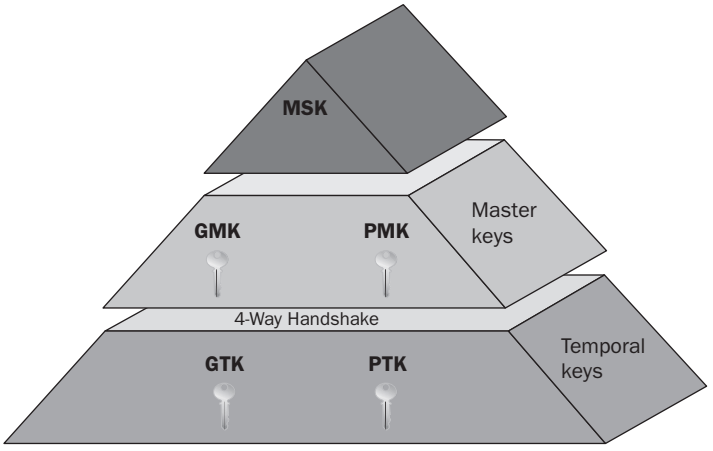
As you can see, a good portion of AKM is the authentication process. In the next sections of this chapter, you will learn in greater detail about the generation of both master and temporary keys, which is the other key component of AKM. Remember that authentication and encryption key management are dependent on each other.

Included on the CD that comes with this book is a white paper titled "802.11i Authentication and Key Management (AKM)," written by Devin Akin. This white paper is often referred to as the "chicken-and-egg" white paper and is recommended extra reading when studying for the CWSP exam. The paper covers much of the same material that is covered in this chapter. It should be noted that this paper was written in May 2005, before the 802.11i amendment was rolled into the 802.11-2007 standard, and the paper will refer often to the 802.11i security amendment.

RSNA Key Hierarchy

AKM services also include the creation of encryption keys. Some of the encryption keys are derived from the authentication process, some of the keys are master keys, and some are the final keys that are used to encrypt/decrypt 802.11 data frames. As Figure 5.18 shows, a total of five keys make up a top-to-bottom hierarchy that is needed to establish a final robust security network association (RSNA). This key hierarchy includes a key derived from either an 802.1X/EAP authentication or derived from PSK authentication. One set of keys is considered to be *group* keys, which are keys that are used to protect multiple destinations. Another set of keys is considered to be *pairwise*. A pairwise relationship can be defined as two entities that are associated with each other: for example, an access point (AP) and an associated station (STA), or two stations communicating in an independent basic service set (IBSS).

FIGURE 5.18 RSN key hierarchy



Master Session Key (MSK)

At the top of the RSNA key hierarchy is the *master session key (MSK),* which is also sometimes referred to as the *AAA key*. The MSK is generated either from an 802.1X/EAP process or is derived from PSK authentication. You will learn how the master session key (MSK) is derived from PSK authentication later in this chapter in the section "Passphrase-PSK Mapping." When an 802.1X/EAP infrastructure is deployed, both the authentication server and the supplicant will know information about each other after the mutual authentication exchange of credentials. The MSK is the keying material that is derived from the EAP process and exported by the EAP method to the supplicant and authentication server. The MSK is at least 64 octets in length. How the MSK is generated from the EAP process is outside of the scope of the 802.11-2007 standard and is EAP method specific.

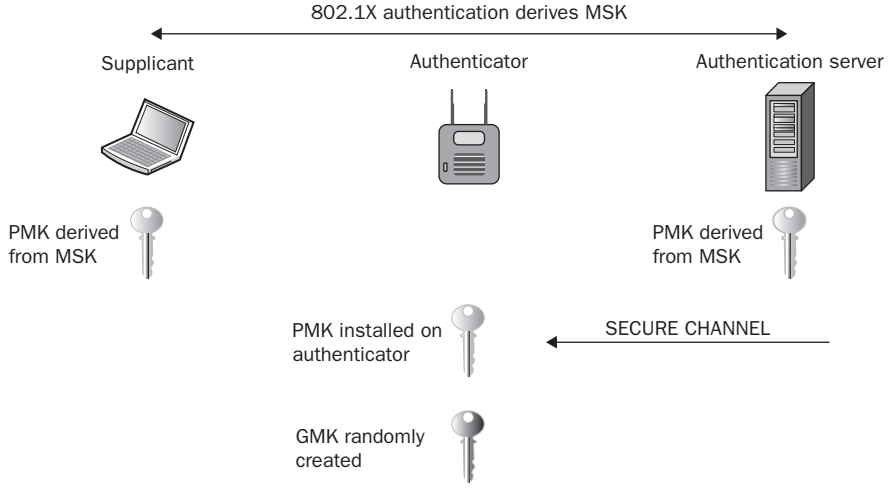
Master Keys

After the creation of the MSK as a result of 802.1X/EAP, two master keys are created. Try to think of the MSK as seeding material or keying material that is a result of 802.1X/EAP mutual authentication. The MSK seeding material is then used to create a master key called the *pairwise master key (PMK)*.

The pairwise master key (PMK) is derived from the MSK seeding material. The PMK is simply computed as the first 256 bits (bits 0–255) of the MSK. Because the pairwise master key (PMK) is derived from the MSK seeding material, a PMK now resides on both the supplicant and the authentication server. Effectively a portion of the MSK seeding material becomes the PMK. A new, unique PMK is generated every time a client authenticates or reauthenticates. It is very important to understand that when 802.1X/EAP is used, every client's PMK is unique to that individual client.

As shown in Figure 5.19, the PMK is then sent from the authentication server over a secure channel to the authenticator. The security of the channel between the authenticator and the AS is outside the scope of the 802.11-2007 standard. A PMK is now installed on both the client station, which is the supplicant, and the access point, which is the authenticator.

FIGURE 5.19 Master keys



Another master key, called the *group master key (GMK),* is randomly created on the access point/authenticator. Any group master key (GMK) may be regenerated at a time interval configured on the AP to reduce the risk of the GMK being compromised.

Keep in mind that master keys are not used to encrypt or decrypt 802.11 data. The master keys are now the seeding material for the 4-Way Handshake process. The 4-Way Handshake process is used to create the keys that are used to encrypt and decrypt data. The keys generated from the 4-Way Handshake are called the pairwise transient key (PTK) and the group temporal key (GTK). The pairwise master key (PMK) is used to create the pairwise transient key (PTK), and the group master key (GMK) is used to create the group temporal key (GTK). In other words, the master keys are used to produce the temporal keys that are used to encrypt 802.11 data frames. The 4-Way Handshake process used to create the temporal encryption keys can begin when the GMK is created and installed on the authenticator, and the PMK is created and installed on both the supplicant and authenticator.

Temporal Keys

As you will learn repeatedly, the 4-Way Handshake process creates temporal keys that are used by the client station and the access point to encrypt and decrypt 802.11 data frames. The *pairwise transient key (PTK)* is used to encrypt all unicast transmissions between a client station and an access point. As discussed earlier in this chapter, each PTK is unique between each individual client station and the access point. Every client station possesses a unique PTK for unicast transmissions between the client STA and the AP. PTKs are used between a single supplicant and a single authenticator.

The *group temporal key (GTK)* is used to encrypt all broadcast and multicast transmissions between the access point and multiple client stations. Although the GTK is dynamically generated, it is shared among all client STAs for broadcast and multicast frames. The GTK is used between all supplicants and a single authenticator.

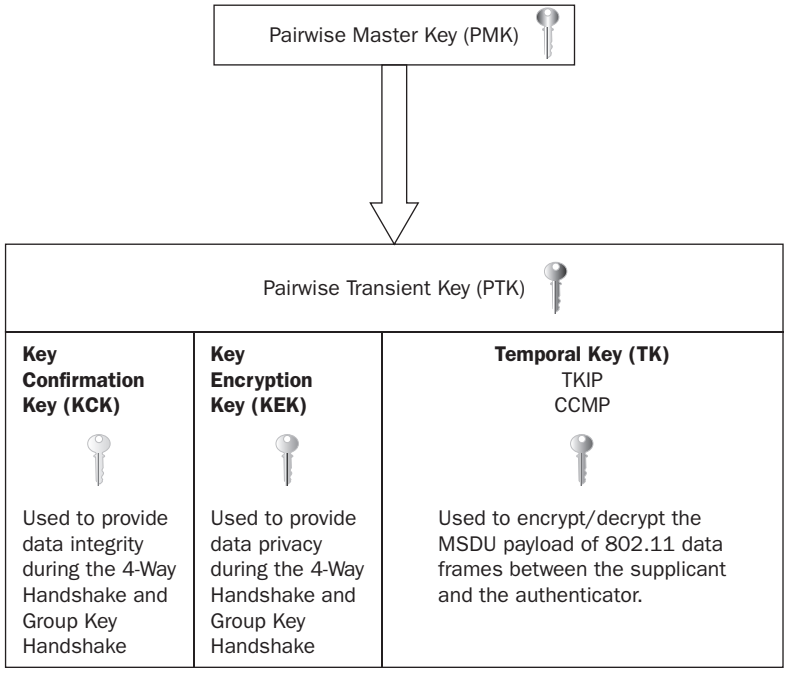
As shown in Figure 5.20, the pairwise transient key (PTK) is derived from the pairwise master key (PMK). The PTK is composed of three sections:

Key Confirmation Key (KCK) The KCK is used to provide data integrity during the 4-Way Handshake and Group Key Handshake.

Key Encryption Key (KEK) The KEK is used by the EAPOL-Key frames to provide data privacy during the 4-Way Handshake and Group Key Handshake.

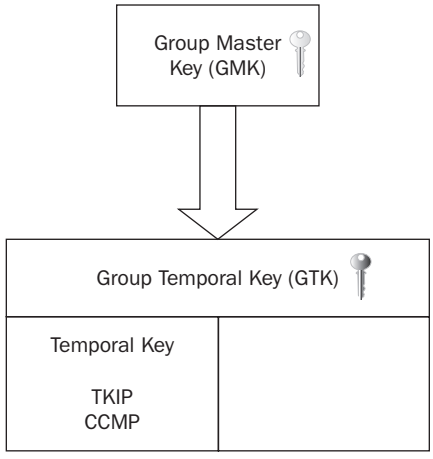
Temporal Key (TK) The TK is the temporal encryption key used to encrypt and decrypt the MSDU payload of 802.11 data frames between the supplicant and the authenticator.

FIGURE 5.20 Pairwise transient key (PTK)



As shown in Figure 5.21, the group temporal key (GTK) is derived from the group master key (GMK). The GTK is a temporal key used to provide data privacy for broadcast/multicast communication. GTKs are used between a single authenticator and all the supplicants that are communicating with the authenticator.

FIGURE 5.21 Group temporal key (GTK)



It should be understood that the PTK/GTKs used for encryption are either CCMP/AES or TKIP/RC4 as defined by the 802.11-2007 standard. However, the 4-Way Handshake can also be used to generate keys for proprietary encryption such as xSec. As you learned in Chapter 3, Aruba Networks and Funk Software jointly developed xSec, which is a Layer 2 encryption cipher that uses 256-bit AES.

4-Way Handshake

The 802.11-2007 standard requires EAPOL-Key frames be used to exchange cryptographic information between the client STA supplicants and the authenticator, which is usually an access point. EAPOL-Key frames are used for the implementation of three different frame exchanges:

- 4-Way Handshake
- Group Key Handshake
- PeerKey Handshake

As already mentioned, the 4-Way Handshake is a final process used to generate pairwise transient keys for encryption of unicast transmissions and a group temporal key for encryption of broadcast/multicast transmissions.

The 4-Way Handshake uses four EAPOL-Key frame messages between the authenticator and the supplicant for six major purposes:

- Confirm the existence of the PMK at the peer station
- Ensure that the PMK is current
- Derive a new pairwise transient key (PTK) from the PMK
- Install the PTK on the supplicant and the authenticator
- Transfer the GTK from the authenticator to the supplicant and install the GTK on the supplicant and, if necessary, the authenticator
- Confirm the selection of the cipher suites

802.1X/EAP authentication is completed when the access point sends an EAP-Success frame and the AP can now initiate the 4-Way Handshake. Keep in mind that the authentication process has already generated the master keys (PMK and GMK), which will be used by the 4-Way Handshake to derive the temporal keys.

Before we explain the 4-Way Handshake process, it is necessary to define several key terms. The 4-Way Handshake uses pseudo-random functions. A *pseudo-random function (PRF)* hashes various inputs to derive a pseudo-random value. The PMK is one of the inputs combined with other inputs to create the pairwise transient key (PTK). Some of the other inputs used by the pseudo-random function are called nonces. A *nonce* is a random numerical value that is generated one time only. A nonce is used in cryptographic operations and is associated with a given cryptographic key. In the case of the 4-Way

Handshake, a nonce is associated with the PMK. A nonce is only used once and is never used again with the PMK. Two nonces are created by the 4-Way Handshake: the *authenticator nonce (ANonce)* and the *supplicant nonce (SNonce)*.

To create the pairwise transient key, the 4-Way Handshake uses a pseudo-random function that combines the pairwise master key, a numerical authenticator nonce, a supplicant nonce, the authenticator's MAC address (AA), and the supplicant's MAC address (SPA).

The following is a simplified depiction of the formula used by the pseudo-random function (PRF) to derive a pairwise transient key:

PTK = PRF (PMK + ANonce + SNonce + AA + SPA)

As Figure 5.22 shows, the 4-Way Handshake consists of the following steps:

4-Way Handshake Message 1 The authenticator and supplicant each randomly create their respective nonces. The authenticator sends an EAPOL-Key frame containing an ANonce to the supplicant. The supplicant now has all the necessary inputs for the pseudo-random function. The supplicant derives a PTK from the PMK, ANonce, SNonce, and MAC addresses. The supplicant is now in possession of a pairwise transient key that can be used to encrypt unicast traffic.

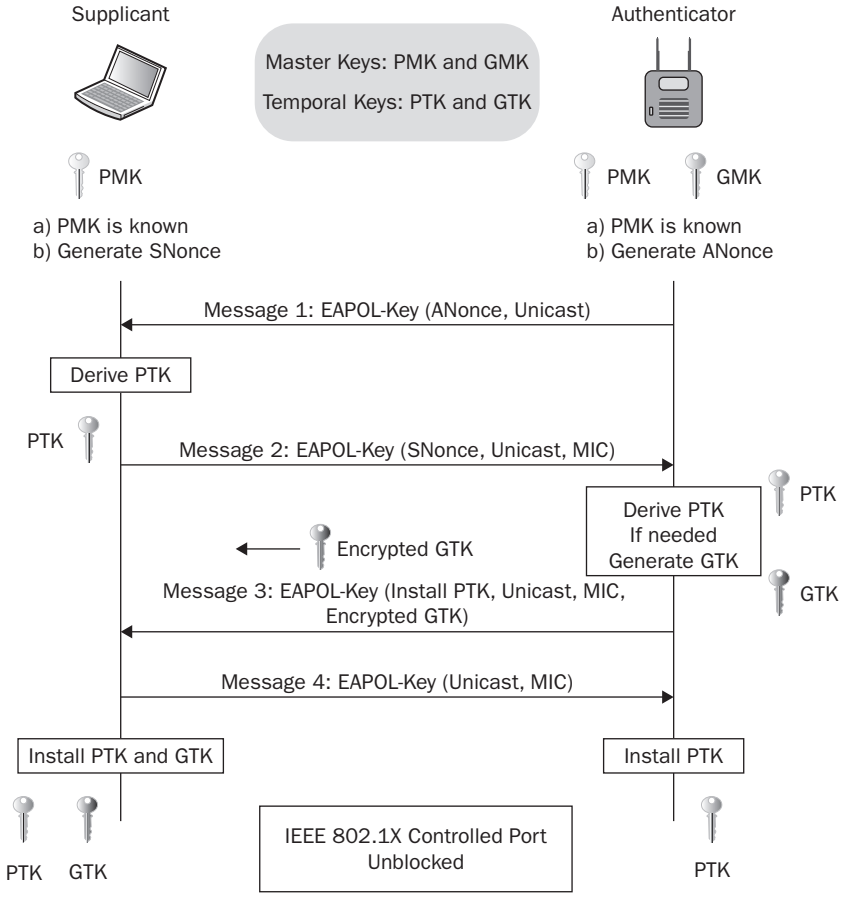
4-Way Handshake Message 2 The supplicant sends an EAPOL-Key frame containing an SNonce to the authenticator. The authenticator now has all the necessary inputs for the pseudo-random function. The supplicant also sends its RSN information element capabilities to the authenticator and a message integrity code (MIC). The authenticator derives a PTK from the PMK, ANonce, SNonce, and MAC addresses. The authenticator also validates the MIC. The authenticator is now in possession of a pairwise transient key that can be used to encrypt unicast traffic.

4-Way Handshake Message 3 If necessary, the authenticator derives a GTK from the GMK. The authenticator sends an EAPOL-Key frame to the supplicant containing the ANonce, the authenticator's RSN information element capabilities, and a MIC. The EAPOL-Key frame may also contain a message to the supplicant to install the temporal keys. Finally, the GTK will be delivered inside this unicast EAPOL-Key frame to the supplicant. The confidentiality of the GTK is protected because it will be encrypted with the PTK.

4-Way Handshake Message 4 The supplicant sends the final EAPOL-Key frame to the authenticator to confirm that the temporal keys have been installed.

Controlled Port Unlocked The virtual controlled port opens on the authenticator, and now, encrypted 802.11 data frames from the supplicant can pass through the authenticator and on to their final destination. All unicast traffic will now be encrypted with the PTK, and all multicast and broadcast traffic will now be encrypted with the GTK.

FIGURE 5.22 The 4-Way Handshake



EXERCISE 5.3

The 4-Way Handshake

In this exercise, you will use a protocol analyzer to view the 4-Way Handshake EAPOL-Key frames that are used to generate the temporal keys used for encryption. The following directions should assist you with the installation and use of WildPackets' OmniPeek protocol analyzer demo software. If you have already installed OmniPeek, you can skip steps 1–5.

1. In your web browser, enter the following URL: `www.wildpackets.com/support/downloads`.
2. Under Product Evals, choose OmniPeek Professional. Fill out the OmniPeek evaluation request. A WildPackets representative will send you an email message with a private download URL.

3. Proceed to the private download URL. Download the OmniPeek Professional demo software to your desktop using FTP. This evaluation copy of OmniPeek will be licensed to work for 30 days. Write down the evaluation copy license serial number .
4. Double-click the installation file `omnp602.exe`, and follow the installation prompts. You will need to be connected to the Internet to activate the license. You will be asked to enter the evaluation copy serial number.
5. This exercise will use frame captures that are on the CD that comes with this book. If you would like to use OmniPeek for live captures, you will need to install the proper drivers for your Wi-Fi radio card. Verify that you have a supported Wi-Fi card. Information about the supported drivers can be found at `www.wildpackets.com/support/downloads/drivers`. Review the system requirements and supported operating systems. Install the proper driver for your Wi-Fi card.
6. In Windows, choose Start ➢ Programs ➢ WildPackets OmniPeek, and then click the OmniPeek icon. The OmniPeek application should appear.
7. Click the Open Capture File icon, and browse the book's CD. Open the packet capture file called `4WAY_HANDSHAKE.PCAP`.
8. In the left column, click Capture ➢ Packets. Drag the Protocol column so that it can be viewed within the window. Observe the EAP-Success frame at packet 66. At this point, 802.1X/EAP authentication is completed, and the AP can now initiate the 4-Way Handshake. The access point (authenticator) MAC address is 00:12:43:CB:0F:30. The client station (supplicant) MAC address is 00:40:96:A3:0C:45.
9. Observe the EAPOL-Key frames of the 4-Way Handshake in packets 68, 70, 72, and 74. Open the first EAPOL-Key frame in packet 68. Notice that the AP is sending the client station an ANonce.
10. Open the second EAPOL-Key frame in packet 70. Notice that the client station is sending the AP an SNonce, an RSN information element, and a MIC.
11. Open the third EAPOL-Key frame in packet 72. Notice the AP is sending the supplicant a MIC and instructions to install the temporal keys.
12. Open the fourth EAPOL-Key frame in packet 74. The supplicant is now sending a message to the authenticator that the temporal keys are installed.

Group Key Handshake

The 802.11-2007 standard also defines a two-frame handshake that is used to distribute a new group temporal key (GTK) to client stations that have already obtained a PTK and GTK in a previous 4-Way Handshake exchange. The *Group Key Handshake* is used only to issue a new group temporal key (GTK) to client stations that have previously formed

security associations. Effectively, the Group Key Handshake is identical to the last two frames of the 4-Way Handshake. Once again, the purpose of the Group Key Handshake is to deliver a new GTK to all client stations that already have an original GTK generated by an earlier 4-Way Handshake.

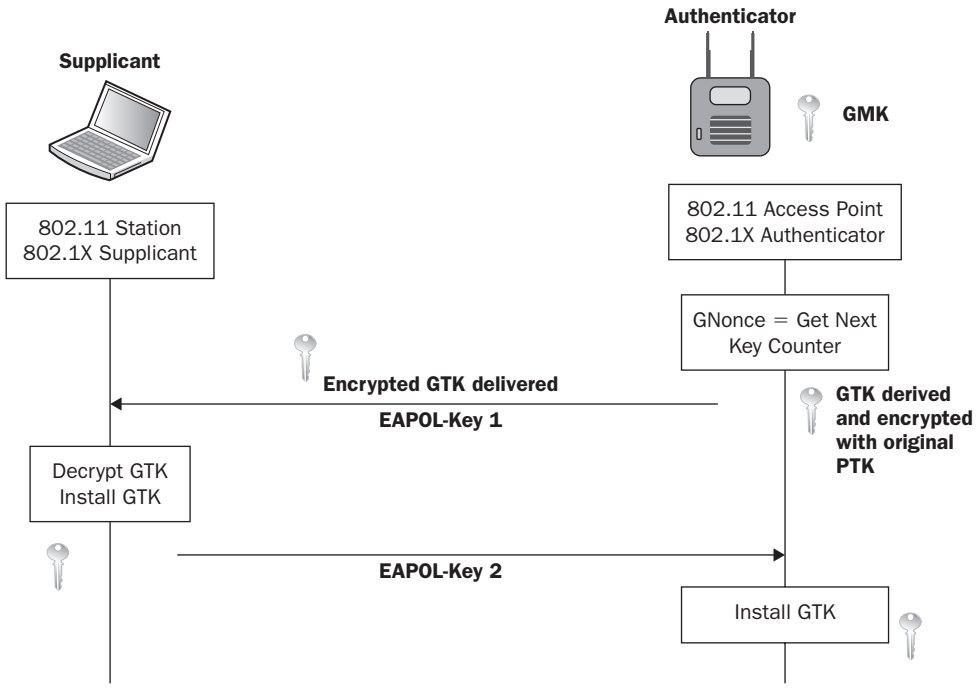
The authenticator can update the GTK for a number of reasons. For example, the authenticator may change the GTK on disassociation or deauthentication of a client station. WLAN vendors may also offer a configuration setting to trigger the creation of a new GTK based on a timed interval.

As shown in Figure 5.23, the Group Key Handshake consists of the following steps:

Group Key Handshake Message 1 The authenticator derives a new GTK from the GMK. The new GTK is sent in a unicast EAPOL-Key frame to the supplicant. The confidentiality of the new GTK is protected because it will be encrypted with the original PTK from the initial 4-Way Handshake. The authenticator also sends a message integrity code (MIC). The supplicant validates the MIC when it receives the EAPOL-Key frame. The supplicant decrypts and installs the new GTK.

Group Key Handshake Message 2 The supplicant sends an EAPOL-Key frame to the authenticator to confirm that the GTK has been installed. The supplicant also sends a message integrity code (MIC). The authenticator validates the MIC when it receives the EAPOL-Key frame.

FIGURE 5.23 The Group Key Handshake



Please do not confuse Group Key Handshake with the two EAPOL-Key frame exchange that is used to distribute dynamic WEP keys. Although both handshakes use a two EAPOL-Key frame exchange, each handshake has an entirely different purpose. Also remember that dynamic WEP is proprietary and that the two EAPOL-Key frame exchange used by dynamic WEP is not an RSN security association.

PeerKey Handshake

Most WLAN communications do not involve peer-to-peer applications between clients; however, peer-to-peer connectivity within a BSS is possible. If two client stations are associated to an AP, peer-to-peer communications from one client station to another client station can occur as long as the traffic is forwarded through the AP. One client station would have to send a unicast frame to the AP, which would then be forwarded through the AP to a peer client station (STA).

Unlike a typical peer-to-peer communications within a BSS, the 802.11-2007 standard defines a method that gives client stations the option to securely communicate with each other in a BSS without sending their frames through the access point. After client STAs have already established individual security associations with an access point, a *station-to-station link (STSL)* can also be established. An STSL is a direct link established between two stations while associated to a common access point.

The client stations within the BSS use a *PeerKey Handshake* management protocol to create PeerKeys that are unique to two client STAs so that they can communicate directly and securely in a station-to-station link (STSL) within the BSS. The PeerKey Handshake is used to establish security for data frames passed directly between two STAs associated with the same AP. The AP must establish an RSNA with each STA prior to the PeerKey Handshake.

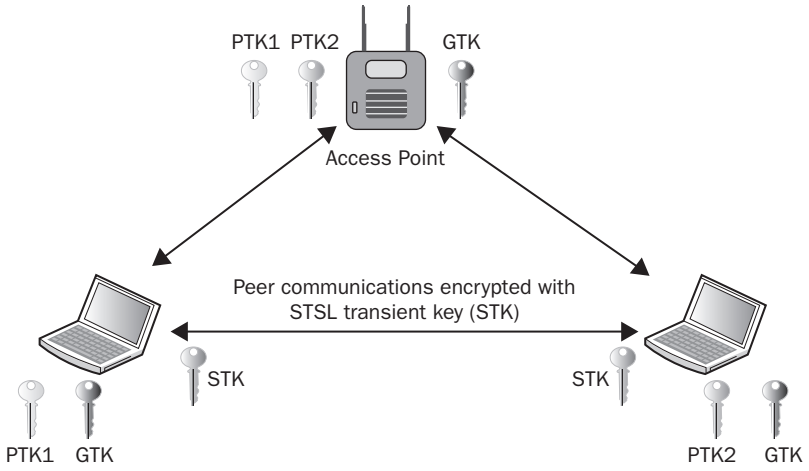
The PeerKey Handshake is actually two different handshakes:

SMK Handshake This frame exchange is used by the two peer stations to create a master key called the *STSL master key (SMK)*. One of the client stations must initiate this exchange through the AP to create the SMK with another client station that also associated to the AP.

4-Way STK Handshake This frame exchange uses the SMK as seeding material to create an *STSL transient key (STK)*. The STK is the final key that is used to encrypt the unicast communications between the two peer client stations while they are still associated to the AP.

As shown in Figure 5.24, the peer stations will remain associated to the AP and use the STK for secure STSL communications. The stations can also still securely communicate within the AP using their original unique pairwise transient keys (PTKs).

FIGURE 5.24 Station-to-station link (STSL)



Although defined by the 802.11-2007 standard, widespread use of the PeerKey Handshake has yet to occur. The 802.11z draft amendment defines enhanced mechanisms for direct link setup (DLS) between two peer stations within a BSS.

RSNA Security Associations

Security associations can be defined as group policies and keys used to protect information. A robust security network association (RSNA) requires two 802.11 stations (STAs) to establish procedures to authenticate and associate with each other as well as create dynamic encryption keys through a 4-Way Handshake. This association between two stations is referred to as an RSNA. The 802.11-2007 standard defines multiple RSNA security associations that are established during the many procedures already discussed in this chapter:

Pairwise Master Key Security Association (PMKSA) The conditions resulting from a successful 802.1X authentication exchange between the supplicant and authentication server or from a preshared key (PSK).

Pairwise Transient Key Security Association (PTKSA) The conditions resulting from a successful 4-Way Handshake exchange between the supplicant and authenticator.

Group Temporal Key Security Association (GTKSA) The conditions resulting from a successful group temporal key (GTK) distribution exchange via either a 4-Way Handshake or a Group Key Handshake.

STSL Master Key Security Association (SMKSA) An SMKSA is the result of a successful SMK Handshake by the initiator STA. It is derived from parameters provided by the access point and the client stations.

STSL Transient Key Security Association (STKSA) The STKSA is a result of the successful completion of the 4-Way STK Handshake. This security association is bidirectional between the initiator and the peer STAs. The STKSA is used to create session keys to protect the station-to-station link.

Passphrase-to-PSK Mapping

As discussed earlier, an authentication and key management protocol (AKMP) can either be derived from an EAP protocol used during 802.1X or by a preshared key (PSK). When a PSK authentication solution is used, AKM operations include the following:

Discovery A client station discovers the access point's security requirements by passively monitoring for beacon frames or through active probing. The access point's security information can be found in the RSN information element field inside beacon and probe response frames. The client station security requirements are delivered to the AP in association and reassociation frames.

Negotiation The client STA associates with an AP and negotiates a security policy. The preshared key (PSK) becomes the pairwise master key (PMK).

Temporal Key Generation and Authorization The 4-Way Handshake exchange between the supplicant and the authenticator utilizing EAPOL-Key frames is used to generate temporary encryption keys that are used to encrypt and decrypt the MSDU payload of 802.11 data frames. Once the temporal keys are created and installed, the controlled port of the authenticator opens and the supplicant can now send traffic through the controlled port onward to network resources.

The PSK authentication used during RSNA is often known by the more common name of WPA-Personal or WPA2-Personal. PSK authentication is meant to be used in small office, home office (SOHO) environments when the stronger WPA2-Enterprise 802.1X authentication solutions are not available.

Vendor Terminology

Many individuals often confuse Shared Key authentication with the preshared key (PSK) authentication used in WPA/WPA2-Personal. As discussed in Chapter 2, Shared Key authentication is a legacy 802.11 authentication method that requires the use of a static WEP key. Do not confuse Shared Key authentication with PSK authentication.

Furthermore, WLAN vendors often add to the confusion with the use of their own terminology. Vendors have many names for PSK authentication, including WPA/WPA2-Passphrase, WPA/WPA2-PSK, and WPA/WPA2-Preshared Key. The correct Wi-Fi Alliance terminology is WPA/WPA2 Personal. All of these terms refer to PSK authentication.

A WPA/WPA2 preshared key is a static key that is configured on the access point and all the clients. The same static PSK is used by all members of the basic service set (BSS). The RSNA PSK is 256 bits in length or 64 characters when expressed in hex. Most end users are not comfortable configuring an AP and client stations with a long, 64-character hexadecimal key. Most end users are, however, very comfortable configuring short ASCII passwords or passphrases. Therefore, a *passphrase-PSK mapping* formula is defined by the 802.11-2007 standard to allow end users to use a simple ASCII passphrase that is then converted to the 256-bit PSK. The PSK is generated using a password-based key generation function (PBKDF).

Here is the formula to convert a passphrase to a PSK:

PSK = PBKDF2(*PassPhrase*, *ssid*, *ssidLength*, 4096, 256)

- The *PassPhrase* is a sequence of between 8 and 63 ASCII-encoded characters. The limit of 63 is mandated so as to differentiate between an ASCII passphrase and a PSK that is 64 hexadecimal characters.
- Each character in the passphrase must have an encoding in the range of 32 to 126 (decimal), inclusive.
- *ssid* is the SSID of the ESS or IBSS where this passphrase is in use, encoded as an octet string used in the beacon and probe response frames for the ESS or IBSS.
- *ssidLength* is the number of octets of the *ssid*.
- 4096 is the number of times the passphrase is hashed.
- 256 is the number of bits output by the passphrase mapping.

As you can see, a simple passphrase is combined with the SSID and hashed to produce a 256-bit PSK.

Previously, you have learned that the 802.1X/EAP process generates a PMK and that every supplicant has a unique PMK. The same cannot be said when PSK authentication is used. The preshared key is the PMK. Because every client station uses the same PSK or passphrase that is converted to a PSK, every client station has the same pairwise master key (PMK). This presents a serious security risk. You already learned in this chapter that the 4-Way Handshake uses a pseudo-random function to combine the PMK with the ANonce, SNonce, AA, and SPA to create a pairwise transient key (PTK). The ANonce, SNonce, and the MAC addresses of the supplicant and authenticator are all seen in cleartext during the 4-Way Handshake frame exchange. If a hacker was able to maliciously obtain the passphrase, the hacker could use the passphrase-PSK mapping formula to create the 256-bit PSK. Remember that the PSK is also used as the pairwise master key. If the hacker has the PMK and captures the 4-Way Handshake with a protocol analyzer, the attacker has all the variables needed to duplicate the pairwise transient key. If the hacker can duplicate the PTK, the hacker can then decrypt any unicast traffic between the AP and the individual client station that performed the 4-Way Handshake.

Passphrases are static and highly susceptible to social engineering attacks. Also, weak passphrases are susceptible to offline dictionary attacks. A policy mandating very strong passphrases of a minimum of 20 characters or more should always be in place whenever a

WPA/WPA2-Personal solution is deployed. To prevent social engineering attacks, policy must dictate that only the administrators have knowledge of any static passphrases and that the passphrases never be shared with end users. Passphrases are intended for use in a home WLAN environment. In the enterprise, passphrases should only be used as a last resort. It is recommended that the full 256-bit key (64 hex characters) be used to prevent social engineering and reduce the likelihood of a security breach. Although the PSK method is not as secure as an 802.1X method, it is still far more secure than the traditional WEP. If an 802.1X EAP method is not available, the next best thing would be to implement WPA/WPA2-Personal.

Roaming and Dynamic Keys

Every time a client station roams from one access point to another, the client STA will send a reassociation request frame to initiate the roaming handoff. The client station uses the RSN information element to inform the access point about the client's security capabilities, including supported encryption cipher suites and supported authentication methods.

Every time a client roams, unique encryption keys must be generated using a 4-Way Handshake process between the access point and the client STA. As you have already learned, either an 802.1X or PSK authentication process is needed to produce the pairwise master key (PMK) that seeds the 4-Way Handshake. Therefore, every time a client roams, the client must reauthenticate.

Roaming can be especially troublesome for VoWiFi and other time-sensitive applications when using a WPA-Enterprise or WPA2-Enterprise security solution, which requires the use of a RADIUS server. Due to the multiple frame exchanges between the authentication server and the supplicant, an 802.1X/EAP authentication often takes 700 milliseconds or greater for the client to authenticate. VoWiFi requires a handoff of 150 milliseconds or less to avoid a degradation of the quality of the call or, even worse, a loss of connection. One advantage of using WPA/WPA2-Personal is that PSK authentication does not have the latency issues of 802.1X/EAP. PSK authentication only requires the 4-Way Handshake exchange, and the roaming handoff can occur in less than 150 milliseconds.

The recently ratified 802.11r-2008 amendment is known as *the fast basic service set transition (FT)* amendment. The technology is more often referred to as *fast secure roaming* because it defines faster handoffs when roaming occurs between cells in a WLAN using 802.1X/EAP. You can find a detailed discussion about fast BSS transition methods in Chapter 7, "802.11 Fast Secure Roaming."

Summary

It is important to remember that authentication and key management (AKM) uses the authentication and encryption processes together to provide authorized protection for the WLAN portal as well as data privacy for the 802.11 data frames. The authentication and encryption key generation processes are linked together and are dependent on each other.

Many vendors initially linked authentication and encryption together using dynamic WEP. However, dynamic WEP security was proprietary and still susceptible to WEP-cracking attacks. The 802.11-2007 standard now defines robust security network associations (RSNAs), which require two 802.11 stations (STAs) to establish procedures to authenticate and associate with each other as well as create dynamic encryption keys through the 4-Way Handshake process. RSNAs use either TKIP/RC4 or CCMP/AES encryption protocols. Dynamic keys prevent social engineering attacks, and all client STAs have unique keys.

Exam Essentials

Explain dynamic WEP. Be able to explain processes used to generate dynamic WEP keys. Understand that dynamic WEP is not the same as RSNA dynamic key management.

Describe the differences between an RSN, TSN, and pre-RSN security network. Understand that a robust security network utilizes only TKIP/RC4 and CCMP/AES encryption. A TSN can use TKIP/RC4, CCMP/AES, and legacy encryption such as WEP. A pre-RSN security network only uses legacy encryption.

Explain the purpose of the RSN information element field. Know what type of security capability information is in the RSNIE. Know which 802.11 management frames are used to deliver the RSNIE and how the management frames are used.

Understand the concept of AKM. Describe the symbiotic relationship between authentication and dynamic encryption. Understand that an 802.1X/EAP or PSK process provides the seeding material to generate dynamic encryption keys.

Describe the RSNA key hierarchy. Understand the relationship between all the various keys. Know the difference between master and temporal keys. Explain the difference between pairwise and group keys. Know the three keys that comprise a PTK.

Explain all phases of the 4-Way Handshake in detail. Understand that the 4-Way Handshake is used to produce the final temporal keys used for encryption. Know the purpose of each EAPOL-Key frame. Explain all of the components needed to create a PTK.

Explain the purpose of the Group Key Handshake. Understand that the Group Key Handshake is used to create a new GTK for broadcast/multicast traffic after a previous 4-Way Handshake has already occurred.

Understand the concept of RSN security associations. Explain all five associations, why they are needed, and when they occur.

Describe passphrase-to-PSK mapping. Explain how a PSK is derived from a passphrase and why. Explain the security weaknesses when PSK authentication is deployed.

Key Terms

Before you take the exam, be certain you are familiar with the following terms:

4-Way Handshake

AAA key

authentication and key management (AKM)

authentication and key management protocol (AKMP)

authenticator nonce (ANonce)

basic service set identifier (BSSID)

broadcast key

fast secure roaming

group

Group Key Handshake

group master key (GMK)

group temporal key (GTK)

independent basic service set (IBSS)

Key Confirmation Key (KCK)

Key Encryption Key (KEK)

keying material

MAC service data unit (MSDU)

master session key (MSK)

nonce

pairwise

pairwise master key (PMK)

pairwise transient key (PTK)

passphrase-PSK mapping

PeerKey Handshake

per session, per user

pre-robust security network associations (pre-RSNAs)

pseudo-random function (PRF)

robust security network (RSN)

robust security network association (RSNA)

robust security network information element (RSNIE)

RSN information element

seeding material

service set identifier (SSID)

station-to-station link (STSL)

STSL master key (SMK)

STSL transient key (STK)

supplicant nonce (SNonce)

Temporal Key (TK)

The basic service set (BSS)

the fast basic service set transition (FT)

transition security network (TSN)

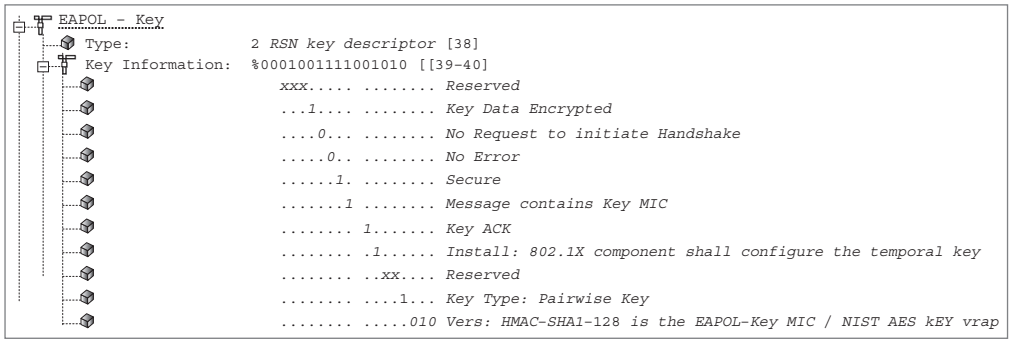
unicast key

Review Questions

1. What must occur in order for dynamic TKIP/RC4 or CCMP/AES encryption keys to be generated? (Choose all that apply.)
   - **A.** Shared Key authentication and 4-Way Handshake
   - **B.** 802.1X/EAP authentication and 4-Way Handshake
   - **C.** Open System authentication and 4-Way Handshake
   - **D.** PSK authentication and 4-Way Handshake

2. Which encryption types can be used to encrypt and decrypt unicast traffic with the pairwise transient key (PTK) that is generated from a 4-Way Handshake? (Choose all that apply.)
   - **A.** Temporal Key Integrity Protocol
   - **B.** 3-DES
   - **C.** Dynamic WEP
   - **D.** CCMP
   - **E.** Proprietary encryption
   - **F.** Static WEP

3. View the frame capture of the 4-Way Handshake in the graphic shown here. Which EAPOL-Key message frame is displayed?



   - **A.** 4-Way Handshake message 1
   - **B.** 4-Way Handshake message 2
   - **C.** 4-Way Handshake message 3
   - **D.** 4-Way Handshake message 4

4. What are the keys that make up a pairwise transient key? (Choose all that apply.)
   - **A.** STK
   - **B.** KEK
   - **C.** SMK
   - **D.** TK
   - **E.** KCK

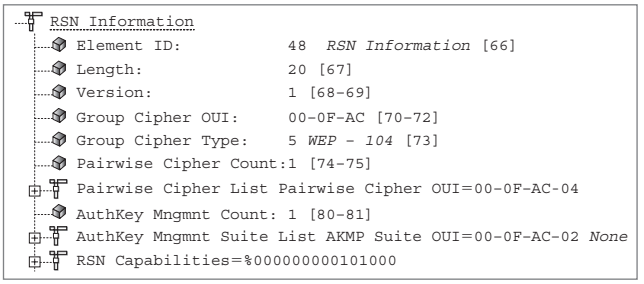
5. What are some of the variables that are used during the 4-Way Handshake to produce a pairwise transient key (PTK)? (Choose all that apply.)
   - **A.** Pairwise Master Key
   - **B.** Master Session Key
   - **C.** Group Master Key
   - **D.** Nonces
   - **E.** Authenticator MAC address

6. After viewing the frame capture in the graphic shown here, identify which type of encryption method is being used.

Source	Destination	Protocol
00:12:43:CB:0F:30	00:40:96:A3:0C:45	802.11 Ack
00:12:43:CB:0F:30	00:40:96:A3:0C:45	EAP Request
00:40:96:A3:0C:45	00:12:43:CB:0F:30	802.11 Ack
00:40:96:A3:0C:45	00:12:43:CB:0F:30	EAP Response
00:12:43:CB:0F:30	00:40:96:A3:0C:45	802.11 Ack
00:12:43:CB:0F:30	00:40:96:A3:0C:45	EAP Success
00:40:96:A3:0C:45	00:12:43:CB:0F:30	802.11 Ack
00:12:43:CB:0F:30	00:40:96:A3:0C:45	EAPOL-Key
00:40:96:A3:0C:45	00:12:43:CB:0F:30	802.11 Ack
00:12:43:CB:0F:30	00:40:96:A3:0C:45	EAPOL-Key
00:40:96:A3:0C:45	00:12:43:CB:0F:30	802.11 Ack

   - **A.** TKIP
   - **B.** CCMP
   - **C.** xSec
   - **D.** Fortress
   - **E.** WEP
   - **F.** AES

7. After viewing the frame capture in the graphic shown here, identify which type of security network is being used.



A. Robust Security Network

B. Rotund Security Network

C. Transition Security Network

D. WPA Security Network

E. WPA

8. What are some of the frames that carry the security capabilities found in the RSN information element? (Choose all that apply.)

A. Beacon management frame

B. Probe request frame

C. Probe response frame

D. Association request frame

E. EAPOL-Key frame

F. Request-to-Send frame

9. The _____ key is used to encrypt/decrypt unicast 802.11 frames, and the _____ key is used to encrypt/decrypt broadcast and multicast 802.11 frames.

A. Group Master, Group Temporal

B. Pairwise Master, Group Temporal

C. Master Session, Pairwise Transient

D. Pairwise Transient, Group Temporal

E. Pairwise Master, Pairwise Transient

10. In a robust security network (RSN), which 802.11 management frames are used by client stations to inform an access point about the RSNA security capabilities of the client STAs? (Choose all that apply.)
    - **A.** Beacon management frame
    - **B.** Probe request frame
    - **C.** Probe response frame
    - **D.** Association request frame
    - **E.** Reassociation response frame
    - **F.** Reassociation request frame
    - **G.** Association response frame

11. Bob's WLAN controller has been configured with the following settings:

    Management VLAN: interface 10.1.20.2

    User VLANS:

    VLAN91: interface 10.1.21.2

    VLAN92: interface 10.1.22.2

    VLAN93: interface 10.1.23.2

    WLAN profiles:

    Profile1: SSID: (employee) security: (802.1X/EAP/CCMP) - VLAN91 - BSSID (00:08:12:43:0F:30)

    Profile2: SSID (voice) security: (PSK/TKIP and WEP) - VLAN92 - BSSID (00:08:12:43:0F:31)

    Profile3: SSID: (guest) security: (WEP) - VLAN93 - BSSID (00:08:12:43:0F:32)

    Based on the settings on Bob's WLAN controller, what type of WLAN security exits within the coverage area of a single controller-based access point? (Choose all that apply.)
    - **A.** Closed security network
    - **B.** Transition security network
    - **C.** Pre-RSNA security network
    - **D.** Open security network
    - **E.** Robust security network

12. Which authentication methods provide the seeding material that is needed by the 4-Way Handshake to create temporal keys for encrypting 802.11 MSDU payloads? (Choose all that apply.)
    - **A.** Shared Key authentication
    - **B.** PSK
    - **C.** 802.1X/EAP
    - **D.** Captive Portal
    - **E.** WPA2-Personal

13. Client stations must authenticate and create new dynamic encryption keys under which conditions? (Choose all that apply.)

- **A.** When probing a BSS
- **B.** When joining a BSS
- **C.** When joining an IBSS
- **D.** When roaming to a new BSS
- **E.** When leaving a BSS

14. When RSN security is in place, which security handshake is used to distribute keys to encrypt broadcast/multicast traffic even though a previous security association has already occurred?

- **A.** PeerKey Handshake
- **B.** Group Key Handshake
- **C.** 4-Way Handshake
- **D.** 2-Way Handshake

15. What can happen when a hacker compromises the preshared key used during PSK authentication? (Choose all that apply.)

- **A.** Decryption
- **B.** Spoofing
- **C.** Encryption cracking
- **D.** Access to network resources

16. After viewing the frame capture shown here, identify the type of authentication method being used.

```
RSN Information
    Element ID:            48  RSN Information [88]
    Length:                20 [89]
    Version:               1 [90-91]
    Group Cipher OUI:      00-0F-AC [92-94]
    Group Cipher Type:     4 CCMP - default in an RSN [95]
    Pairwise Cipher Count:1 [96-97]
  + Pairwise Cipher List Pairwise Cipher OUI=00-0F-AC-04
    AuthKey Mngmnt Count: 1 [102-103]
  + AuthKey Mngmnt Suite List AKMP Suite OUI=00-0F-AC-02 None
  + RSN Capabilities=%000000000000000
```

- **A.** EAP-TTLS
- **B.** Open System
- **C.** PSK
- **D.** EAP-TLS
- **E.** PEAP

17. What type of RSNA security association is established as the result of a successful 802.1X authentication exchange between the supplicant and authentication server, or from a preshared key (PSK)?

A. PMKSA

B. GMKSA

C. SMKSA

D. PTKSA

18. What are the advantages of using dynamic encryption keys instead of static keys? (Choose all that apply.)

A. Every client STA has a unique key.

B. Dynamic encryption uses compression.

C. All client STAs share a broadcast key.

D. Authentication is optional with dynamic encryption.

19. What operations must occur before the virtual controlled port of the authenticator becomes unblocked? (Choose all that apply.)

A. 802.1X/EAP authentication

B. 4-Way Handshake

C. 2-Way Handshake

D. RADIUS proxy

20. What are some of the purposes of the 4-Way Handshake? (Choose all that apply.)

A. Transfer the GTK to the supplicant

B. Derive a PTK from the PMK

C. Transfer the GMK to the supplicant

D. Confirm cipher suites

Answers to Review Questions

1. B, D. Open System and Shared Key authentication are legacy authentication methods that do not provide seeding material to generate dynamic encryption keys. A robust security network association requires a four-frame EAP exchange known as the 4-Way Handshake that is used to generate dynamic TKIP or CCMP keys. The handshake may occur either after an 802.1X/EAP exchange or as a result of PSK authentication.

2. A, D, E. The PTK/GTKs are generated by the 4-Way Handshake. As defined by the 802.11-2007 standard, the temporal keys generated by the 4-Way handshake use either CCMP/AES or TKIP/RC4 ciphers. However, the 4-Way Handshake can also be used to generate keys for proprietary encryption such as xSec. Aruba Networks and Funk Software jointly developed xSec, which is a Layer 2 encryption cipher that uses 256-bit AES. Although WEP can be dynamically generated, a simpler two EAPOL-Key frame exchange is used to generate the WEP keys instead of a 4-Way Handshake.

3. C. The third EAPOL-Key frame of the 4-Way Handshake may also contain a message to the supplicant to install the temporal keys. The frame capture indicates that the temporal key is to be installed. The third EAPOL-Key frame also sends the supplicant the ANonce, the authenticator's RSN information element capabilities, and a MIC. If a GTK has been generated, the GTK will be inside the third EAPOL-Key frame. The GTK confidentiality is protected because it will be encrypted with the PTK.

4. B, D, E. The pairwise transient key (PTK) is comprised of the three separate keys. The Key Confirmation Key (KCK) is used to provide data integrity during the 4-Way Handshake and Group Key Handshake. The Key Encryption Key (KEK) is used by the EAPOL-Key frames to provide data privacy during the 4-Way Handshake and Group Key Handshake. The Temporal Key (TK) is the temporal encryption key used to encrypt/decrypt the MSDU payload of 802.11 data frames between the supplicant and the authenticator. The STSL transient key (STK) and STSL master key (SMK) are used during the PeerKey Handshake.

5. A, D, E. To create the pairwise transient key (PTK), the 4-Way Handshake uses a pseudo-random function that combines the pairwise master key, the authenticator nonce (ANonce), the supplicant nonce (SNonce), the authenticator's MAC address (AA), and the supplicant's MAC address (SPA). The master session key (MSK) is used to derive the pairwise master key (PMK). The group master key (GMK) is used to create the group temporal key (GTK).

6. E. The frame capture depicts a two EAPOL-Key frame exchange. When dynamic WEP is deployed, a two EAPOL-Key frame exchange always follows the EAP frame exchange. The two EAPOL-Key frames are both sent by the authenticator to the supplicant. The first EAPOL-Key frame carries the broadcast key from the access point to the client. The second EAPOL-Key frame is effectively a confirmation that the keys are installed and that the WEP encryption process can begin.

7. C. The frame capture shows an RSN information element field that can be found in a management frame. The RSN information element shows that the group cipher that is being used is WEP. A transition security network (TSN) supports RSN-defined security as well as legacy security such as WEP within the same BSS. Within a TSN, some client stations will use RSNA security using TKIP/RC4 or CCMP/AES for encrypting unicast traffic.

However, some legacy stations are still using static WEP keys for unicast encryption. All of the clients will use WEP encryption for the broadcast and multicast traffic. Because all the stations share a single group encryption key for broadcast and multicast traffic, the lowest common denominator must be used for the group cipher.

8. A, C, D, E. The RSN information element field is found in four different 802.11 management frames: beacon management frames, probe response frames, association request frames, and reassociation request frames. The RSN information element can also be found in the second and third EAPOL-Key frames of the 4-Way Handshake.

9. D. The 4-Way Handshake process creates temporal keys that are used by the client station and the access point to encrypt and decrypt 802.11 data frames. The pairwise transient key (PTK) is used to encrypt all unicast transmissions between a client station and an access point. Each PTK is unique between each individual client station and the access point. Every client station possesses a unique PTK for unicast transmissions between the client STA and the AP. PTKs are used between a single supplicant and a single authenticator. The group temporal key (GTK) is used to encrypt all broadcast and multicast transmissions between the access point and multiple client stations. Although the GTK is dynamically generated, it is shared among all client STAs for broadcast and multicast frames. The GTK is used between all supplicants and a single authenticator.

10. D, F. The RSN information element field is found in four different 802.11 management frames: beacon management frames, probe response frames, association request frames, and reassociation request frames. Within a basic service set, an access point and client stations use the RSN information element within these four management frames to communicate with each other about their security capabilities prior to establishing association. Client stations use the association request frame to inform the access point of the client station security capabilities. When stations roam from one access point to another access point, they use the reassociation request frame to inform the new access point of the roaming client station's security capabilities. The security capabilities include supported encryption cipher suites and supported authentication methods.

11. B, C, E. The WLAN controller is configured with three WLANs each with a unique logical identifier (SSID) that is also assigned to a specific VLAN. Because the BSSID is the MAC address of the AP, and because the WLAN controller can support many WLANs on the same physical AP, each virtual WLAN profile is linked with a unique virtual BSSID. Each WLAN has a logical name (SSID) and a unique virtual Layer 2 identifier (BSSID), and each WLAN is mapped to a unique Layer 3 virtual local area network (VLAN). Each WLAN also has different types of security associations. Because multiple virtual BSSIDs exist with different security requirements, an RSN WLAN, a pre-RSNA WLAN, and a TSN WLAN all exist within the same coverage area of an access point. Effectively, three basic service sets (BSS) exist within the same coverage cell, each with different security. WLAN #1 is a robust security network (RSN) because it is only using CCMP encryption. WLAN #2 is a transition security network (TSN) because it is using TKIP and legacy WEP encryption. WLAN #3 is a pre-RSNA security network because it is only using legacy WEP encryption.

12. B, C, E. The 802.11-2007 standard defines authentication and key management (AKM) services. The AKM services are a set of one or more algorithms designed to provide authentication and key management, either individually or in combination with higher layer authentication and key management algorithms. An authentication and key management

protocol (AKMP) can either be a preshared key (PSK) or an EAP protocol used during 802.1X/EAP authentication. WPA2-Personal uses PSK authentication. WPA2-Enterprise uses 802.1/EAP.

13. B, C, D. Whenever a client joins a basic service set (BSS) for the first time, the client must authenticate and create new keys. Either an 802.1X or PSK authentication process is needed to produce the pairwise master key (PMK) that seeds the 4-Way Handshake. Every time a client roams, unique encryption keys must be generated using a 4-Way Handshake process between the access point and the client STA. Therefore, every time a client roams to a new BSS, the client must reauthenticate and create new keys. All the stations within an IBSS also have to utilize the 4-Way Handshake with each other because all unicast communications are peer-to-peer. PSK authentication is used within the IBSS to seed the 4-Way Handshake. Therefore, every time a client joins an IBSS with a peer station, the client must reauthenticate and create new keys.

14. B. The 802.11-2007 standard defines a two-frame handshake that is used to distribute a new group temporal key (GTK) to client stations that have already obtained a PTK and GTK in a previous 4-Way Handshake exchange. The Group Key Handshake is used only to issue a new group temporal key (GTK) that has previously formed security associations. Effectively, the Group Key Handshake is identical to the last two frames of the 4-Way Handshake. The purpose of the Group Key Handshake is to deliver a new GTK to all client stations that already have an original GTK generated by an earlier 4-Way Handshake.

15. A, D. After obtaining the passphrase, the hacker can also associate to the AP using PSK authentication and thereby access network resources. The encryption technology is not cracked, but the key can be re-created. The ANonce, SNonce, and the MAC addresses of the supplicant and authenticator are all seen in cleartext during the 4-Way Handshake frame exchange. If a hacker was able maliciously to obtain the passphrase, the hacker could use the passphrase-PSK mapping formula to create the 256-bit PSK. The PSK is also used as the pairwise master key. If the hacker has the PMK and captures the 4-Way Handshake with a protocol analyzer, the hacker has all the variables needed to duplicate the pairwise transient key. If the hacker can duplicate the PTK, the hacker can then decrypt any unicast traffic between the AP and the individual client station that performed the 4-Way Handshake.WPA/WPA2-Personal is not considered a strong security solution for the enterprise because, if the passphrase is compromised, the attacker can access network resources and decrypt traffic.

16. C. The RSN information element can also be used to indicate what authentication methods are supported. The authentication key management (AKM) suite field in the RSN information element indicates whether the station supports either 802.1X authentication or PSK authentication. If the AKM suite value is 00-0F-AC-01, authentication is negotiated over an 802.1X infrastructure using an EAP protocol. If the AKM suite value is 00-0F-AC-02, then PSK is the authentication method that is being used.

17. A. Security associations can be defined as group policies and keys used to protect information. A robust security network association (RSNA) requires two 802.11 stations (STAs) to establish procedures to authenticate and associate with each other as well as to create dynamic encryption keys. The 802.11-2007 standard defines multiple RSNA

security associations. A pairwise master key security association (PMKSA) is defined as the conditions resulting from a successful 802.1X authentication exchange between the supplicant and authentication server, or from a preshared key (PSK).

18. A, C. The main advantage of using dynamic keys is that the keys are not static and are not compromised by social engineering attacks because the users have no knowledge of the keys. Another advantage of dynamic keys is that every user has a different and unique key. If a single user's encryption key is somehow compromised, none of the other users would be at risk because every user has a unique key.

19. A, B. 802.1X/EAP authentication must first occur to achieve mutual validation of both the supplicant and authentication server credentials. 802.1X/EAP provides the PMK necessary for the 4-Way Handshake. The 4-Way Handshake then generates the temporal keys used for encryption. Once the temporal keys are created and installed, the controlled port of the authenticator is no longer blocked and the supplicant can now send encrypted 802.11 data frames through the controlled port onward to network resources. No traffic can pass through the controlled port until mutual authentication occurs and dynamic keys are created.

20. A, B, D. The purpose of the 4-Way Handshake is to confirm the existence of the PMK at the peer station and ensure that the PMK is current. A pairwise transient key (PTK) must be derived from the PMK and installed on both the supplicant and authenticator. The GTK must be transferred from the authenticator, and the GTK must be installed on the supplicant and, if necessary, the authenticator. The 4-Way Handshake is also used to confirm the selection of encryption cipher suites.

Chapter 6

SOHO 802.11 Security

IN THIS CHAPTER, YOU WILL LEARN ABOUT THE FOLLOWING:

- ✓ **WPA/WPA2-Personal**
  - Preshared keys (PSK) and passphrases
  - WPA/WPA2-Personal risks
  - Entropy
  - Proprietary PSK
- ✓ **Wi-Fi Protected Setup (WPS)**
  - WPS architecture
- ✓ **SOHO security best practices**

This chapter discusses security design concepts, operations, and best practices for small Wi-Fi deployments such as with *small office, home office (SOHO)* environments. PSK authentication is meant to be used in SOHO environments because the stronger enterprise 802.1X authentication solutions require expensive infrastructure and complex configuration. PSK authentication is also known by the more common name of WPA-Personal or WPA2-Personal. Most SOHO wireless networks are secured with WPA/WPA2-Personal mechanisms. However, the Wi-Fi Alliance has defined new methods to enable fast and easy security configuration in a SOHO environment. We will explore the basics of these new simple SOHO security methods called Wi-Fi Protected Setup (WPS).

Chances are, if you bought this book and strive to be a Certified Wireless Security Professional, you are probably—at best—moderately interested in reading a chapter on SOHO security. It is nonetheless important to understand the differences between the SOHO solutions that are in use today. This information can be used to help provide consultation to network operators on the strengths and weaknesses of SOHO methods.

WPA/WPA2-Personal

As you have previously learned, the IEEE 802.11i security amendment, which was ratified and published as IEEE Standard 802.11i-2004, defined a *robust security network (RSN)* using stronger encryption and better authentication methods. The 802.11i amendment is now part of the IEEE 802.11-2007 standard. As you learned in Chapter 5, "802.11 Dynamic Encryption Key Generation," the 802.11-2007 standard defines *authentication and key management (AKM)* services. AKM services require both authentication processes and the generation and management of encryption keys. An *authentication and key management protocol (AKMP)* can be either a *preshared (PSK)* or an EAP protocol used during 802.1X authentication. 802.1X/EAP requires a RADIUS server and advanced skills. The average home Wi-Fi user has no knowledge of 802.1X/EAP and does not have a RADIUS server in their living room. PSK authentication is meant to be used in SOHO environments because the stronger enterprise 802.1X authentication solutions are not available. Therefore, the security used in SOHO environments is PSK authentication. WPA/WPA2-Personal is the same thing as PSK authentication.

Most SOHO wireless networks are secured with WPA/WPA2-Personal mechanisms. Prior to the IEEE ratification of the 802.11i amendment, the Wi-Fi Alliance introduced the *Wi-Fi Protected Access (WPA)* certification as a snapshot of the not-yet-released 802.11i

amendment, supporting only TKIP/RC4 dynamic encryption-key generation. 802.1X/EAP authentication was required in the enterprise, and a passphrase authentication method called *WPA-Personal* was required in a SOHO environment.

The intended goal of WPA-Personal was no more fixed key sizes and no more nasty HEX and ASCII designations of input. WPA-Personal allows an end-user to enter a simple ASCII character string, dubbed a passphrase, anywhere from 8 to 63 characters in size. Behind the scenes, a "pass-phrase to PSK mapping" function took care of the rest. Therefore, all the user had to know was a single, secret passphrase to allow access to the WLAN.

In June 2004, the IEEE 802.11 TGi working group formally ratified 802.11i, which added support for CCMP/AES encryption. The Wi-Fi Alliance therefore revised the previous WPA specification to WPA2, incorporating the CCMP/AES cipher. Therefore, the only practical difference between WPA and WPA2 has to do with the encryption cipher. WPA-Personal and WPA2-Personal both use the PSK authentication method; however, WPA-Personal specifies TKIP/RC4 encryption and *WPA2-Personal* specifies CCMP/AES. WLAN vendors have many names for PSK authentication, including WPA/WPA2-Passphrase, WPA/WPA2-PSK, and WPA/WPA2-Preshared Key. For example, Figure 6.1 shows a Linksys Wi-Fi router that uses the term WPA-Preshared Key. The correct Wi-Fi Alliance terminology is WPA/WPA2-Personal. All of these terms refer to 802.11 PSK authentication.

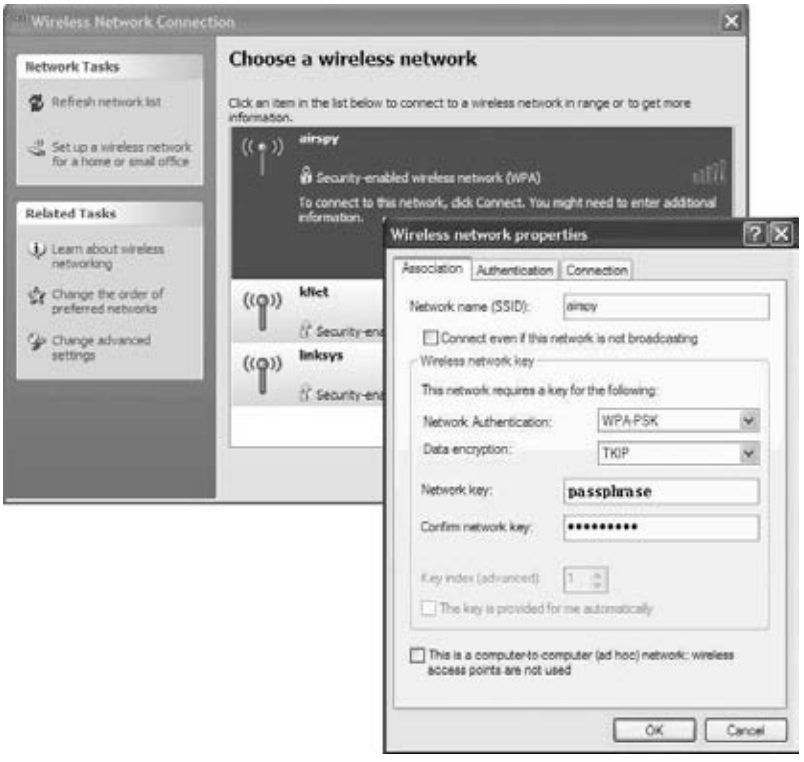
FIGURE 6.1 Vendor terminology example

Preshared Keys (PSK) and Passphrases

A preshared key (PSK) used in a robust security network is 256 bits in length, or 64 characters when expressed in hex. A PSK is a static key that is configured on the access point and on all the clients. The same static PSK is used by all members of the basic service set (BSS). The problem is that the average home user is not comfortable with entering a 64-character hexadecimal PSK on both a SOHO Wi-Fi router and a laptop client utility. Even if home users did enter a 64-character PSK on both ends, they would not be able to remember the PSK and would have to write it down. Most home users are, however, very

comfortable configuring short ASCII passwords or passphrases. As shown in Figure 6.2, the home user enters a *passphrase*, which is an 8 to 63 character string entered into both the client software on the end-user device and also at the access point. The passphrase must match on both ends.

FIGURE 6.2 Client configured with passphrase



As you learned in Chapter 5, a *passphrase-PSK mapping* formula is defined by the 802.11-2007 standard to allow end-users to use a simple ASCII passphrase that is then converted to the 256-bit PSK. Here is a quick review of the formula to convert a passphrase to a PSK:

PSK = PBKDF2(PassPhrase, ssid, ssidLength, 4096, 256)

A simple passphrase is combined with the SSID and hashed 4,096 times to produce a 256-bit (64-character) PSK. Table 6.1 illustrates some examples of how the formula uses both the passphrase and SSID inputs to generate the PSK.

TABLE 6.1 Passphrase-PSK Mapping

Passphrase (8-63 Characters)	SSID	256-Bit /64-Character PSK
carolina	airspy	4725C1AA516B35A61CD91F06394F0D8FA106CEA 049D9E3411AE0EC2EA32B18A9
certification	airspy	5195FFC22CC1F7973168ECA4215A32AC54AB52B 8FD8C09A8646C691CB90A1B65
Victoria	airspy	44D397AE99CF448729D8CBB24550CD6C72E6BD AE0B0CA67224A634B57529ED91

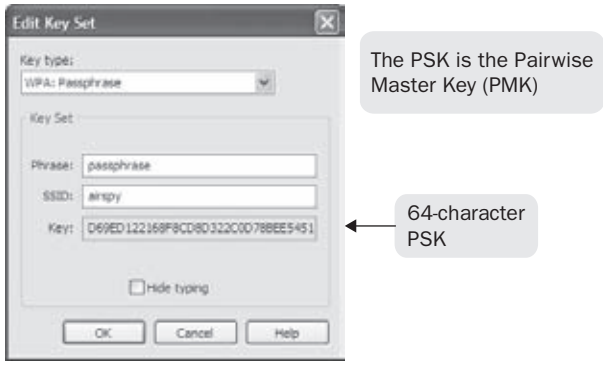
The whole point of the passphrase-PSK mapping formula is to simplify configuration for the average home end-user. Anyone can remember an 8-character passphrase as opposed to a 256-bit PSK.

The 256-bit PSK is also used as the *pairwise master key (PMK)*. The PMK is the seeding material for the 4-Way Handshake that is used to generate dynamic encryption keys. Therefore, the PSK in WPA/WPA2-Personal modes is quite literally the same as the PMK.

Previously, you have learned that the 802.1X/EAP process generates a PMK and that every supplicant has a unique PMK. The same cannot be said when PSK authentication is used. The 256-bit PSK is the PMK. Because every client station uses the same PSK or passphrase that is converted to a PSK, every client station has the same pairwise master key (PMK). This presents a serious security risk.

If a hacker was able to obtain the passphrase maliciously, the hacker could then use the passphrase-PSK mapping formula to re-create the 256-bit PSK. As you can in Figure 6.3, most protocol analyzers are aware of the passphrase-PSK mapping formula and use the SSID and passphrase inputs to re-create the 256-bit PSK. Remember that the PSK is also used as the pairwise master key (PMK).

FIGURE 6.3 Passphrase-PSK mapping



The *4-Way Handshake* uses a pseudo-random function to combine the PMK with the ANonce, SNonce, AA, and SPA to create a pairwise transient key (PTK). As you learned in previous chapters, the PTK is used by the client station and the AP to encrypt/decrypt unicast 802.11 data frames.

The ANonce, SNonce, and the MAC addresses of the client station and the access point are all seen in clear text during the 4-Way Handshake frame exchange. Once the hacker has the PMK derived from the passphrase, the final step is to capture a 4-Way Handshake exchange between a client station and an AP with a protocol analyzer. The attacker now has all the variables needed to duplicate the pairwise transient key (PTK). If the hacker can duplicate the PTK, the hacker can then decrypt any unicast traffic between the AP and the individual client station that performed the 4-Way Handshake.

EXERCISE 6.1

Passphrase-PSK Mapping

In this exercise, you will use a protocol analyzer and passphrase-PSK mapping to regenerate the pairwise master key (PMK). You will then use a capture of a client station's 4-Way Handshake EAPOL-key frames together with the PMK to re-create the temporal keys that are used for encryption.

The following directions should assist you with the installation and use of WildPackets' OmniPeek protocol analyzer demo software. If you have already installed OmniPeek, you can skip steps 1–5.

1. In your web browser, enter the following URL: `www.wildpackets.com/support/downloads`.
2. Under Product Evals, choose OmniPeek Professional. Fill out the OmniPeek evaluation request. A WildPackets representative will send you an email message with a private download URL.
3. Proceed to the private download URL. Download the OmniPeek Professional demo software to your desktop using FTP. This evaluation copy of OmniPeek will be licensed to work for 30 days. Write down the evaluation copy license serial number.
4. Double-click the installation file `omnp602.exe`, and follow the installation prompts. You will need to be connected to the Internet to activate the license. You will be asked to enter the evaluation copy serial number.
5. This exercise will use frame captures that are on the CD that comes with this book. If you would like to use OmniPeek for live captures, you will need to install the proper drivers for your Wi-Fi radio card. Verify that you have a supported Wi-Fi card. Information about the supported drivers can be found at `www.wildpackets.com/support/downloads/drivers`. Review the system requirements and supported operating systems.

6. In Windows, choose Start ➢ Programs ➢ WildPackets OmniPeek, and then click the OmniPeek icon. The OmniPeek application should appear.
7. Click the Open Capture File icon, and browse the book's CD. Open the packet capture file called PASSPHRASE_PSK.pcap.
8. In the left column, click Capture ➢ Packets. Drag the Protocol column so that it can be viewed within the window. Observe the 4-Way Handshake frame exchange in packets #35–#42. Observe that TKIP is used to encrypt the 802.11 data frames that follow.
9. From the Tools menu, select Decrypt WLAN Packets. You will need to create a key set by clicking on the box with the ellipsis, as shown here:

10. Click the Insert button, and create a key set as shown in the following graphic. The passphrase is "certification" and the SSID is "airspy." Click OK three times. Notice that all of the previously encrypted 802.11 data frames are now decrypted. Scroll to packet #57 to view a DHCP response packet.

11. The SSID and passphrase inputs were used to create the pairwise master key (PMK). Combining the PMK along with the ANonce, SNonce, and MAC addresses found in the 4-Way Handshake enabled you to re-create the pairwise transient key (PTK). The PTK was then used to decrypt the unicast 802.11 data frames.

WPA/WPA2-Personal Risks

The risks involved with WPA/WPA2-Personal are basically twofold: network resources can be placed at risk and the encryption keys can be compromised. First, let's discuss how network resources can be placed at risk. WPA/WPA2-Personal uses the weak PSK authentication method that is vulnerable to an offline *brute-force dictionary attack*. WLAN auditing software such as coWPAtty and Aircrack-ng can be used for malicious purposes to obtain weak passphrases using an offline brute-force dictionary attack. We will discuss how to protect against these types of attacks later in this chapter.

More information about WLAN auditing tools, such as coWPAtty and Aircrack-ng, can be found in Chapter 9, "Wireless LAN Security Auditing."

The easier way to obtain a WPA/WPA2 passphrase is through social engineering techniques. Social engineering is the act of manipulating people into performing actions or divulging confidential information. The simplest way to get the passphrase is to just ask someone what it is and they will probably tell you.

As you can see, a hacker can obtain the passphrase using either social engineering skills or using an offline brute-force dictionary attack. Once the passphrase is compromised, the hacker can use any client station to associate with the WPA/WPA2-Personal access point. The hacker is then free to access network resources. This is why PSK authentication was never intended for use in the enterprise and was intended for use as a SOHO security method.

We have already discussed the second risk involved with WPA/WPA2-Personal. If a hacker is able to obtain the passphrase maliciously, the hacker can use the passphrase-PSK mapping formula to re-create the 256-bit PSK and therefore the PMK. The hacker can use the PMK combined with a packet capture of the 4-Way Handshake to re-create the encryption keys. The hacker can then decrypt any unicast traffic between the AP and the individual client station that performed the 4-Way Handshake.

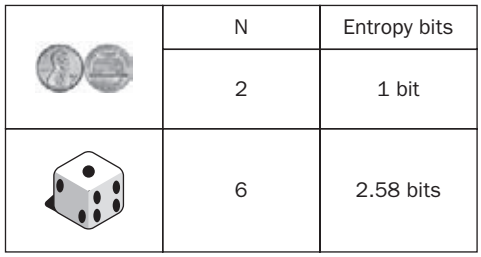
Entropy

In digital communications, *entropy* is a measure of uncertainty associated with a random variable. The complete explanation of the information theory on which entropy is based is well beyond the scope of this book, but we will attempt to explain entropy as it relates to the use of passphrases.

The random act of flipping a coin can be used to visualize entropy. The final result of a coin flip will either be "heads" or "tails," but there is no way to tell what the result will be each time the coin is flipped. The measure of uncertainty associated with the randomness of a coin flip is equal to one bit of entropy. If you roll a single die, it will land on one of

six sides. As shown in Figure 6.4, the measure of uncertainty associated with the random roll of a single die is equal to 2.58 bits of entropy. A random variable has a certain number (N) of outcomes. A coin flip has two possible outcomes while the roll of a die has six possible results. The roll of the die has more uncertainty than a coin flip; therefore, it has more bits of entropy. The more randomness there is to a situation, the more measureable bits of uncertainty exist.

FIGURE 6.4 Entropy bits



A random variable has a certain number (N) of outcomes.

As shown in Table 6.2, entropy bits can also be applied to individual characters in a password or passphrase. For example, if a personal identification number (PIN) was created from the numerical digits, each character of the PIN has 10 possibilities (0–9). Based on complex informational theory, each character created strictly from numerical digits would have 3.3 bits of entropy. If the single-case letters were used in a PIN, each character of the PIN has 26 possibilities (a–z). Based on complex informational theory, each character created strictly from numerical digits would have 4.7 bits of entropy.

TABLE 6.2 Entropy bits

Symbol Set	N of Symbols	Entropy Bits per Character
Numerical digits (0–9)	10	3.32 bits
Single-case letters (a–z)	26	4.7 bits
Single-case letters and digits (a–z, 0–9)	36	5.17 bits
Mixed-case letters and digits (a–z, A–Z, 0–9)	62	5.95 bits
Mixed-case letters, digits, and symbols (Standard U.S. keyboard)	94	6.55 bits

Passwords or passphrases by themselves have an entropy value of zero. It is the method you use to select the passphrase that contains the entropy. When strong passwords or passphrases are created, they should include a combination of uppercase and lowercase letters, numbers, and special symbols. A strong passphrase will have more entropy bits per character than a password created from your name or your phone number. The more entropy (measured in bits) that is contained within the method you use to create your passphrase, the more difficult it will be to guess the passphrase.

Now let's discuss how many entropy bits are contained in a passphrase used in WPA/WPA2-Personal:

> A passphrase typically has about 2.5 bits of security per character, so the passphrase mapping converts an *n* octet password into a key with about $2.5n + 12$ bits of security. Hence, it provides a relatively low level of security, with keys generated from short passwords subject to dictionary attack. Use of the key hash is recommended only where it is impractical to make use of a stronger form of user authentication. A key generated from a passphrase of less than about 20 characters is unlikely to deter attacks.
>
> *802.11i-2004 amendment*

What this quotation means is that each character in a passphrase is worth only 2.5 bits of entropy because most users choose easy-to-remember words as opposed to a mix of alphanumeric and punctuation characters. Therefore, an 8-character passphrase would only contain 20 bits of entropy before the passphrase-to-PSK mapping hash algorithm is calculated. Because the passphrase-to-PSK mapping mixes the SSID with the passphrase, approximately 12 extra bits of entropy are added. Therefore, a typical 8-character passphrase used in a WPA/WPA2-Personal configuration would have a total of 32 bits of entropy.

Please do not confuse entropy security bits with the number of digital bits in a PSK. The passphrase-to-PSK mapping formula will always convert any passphrase of 8 to 63 characters into a 256-bit PSK. Remember that entropy bits are a measure of uncertainty associated with a random variable. The random variable is basically the strength of the passphrase.

The biggest question is the number of bits of entropy needed to protect current data communications. Current information technology security best practices state that 96 bits of entropy should be safe; however, 128 bits might be needed in the future. This all sounds pretty scary if you are using a simple passphrase for your home Wi-Fi router—and you should be scared. As mentioned earlier, the simple passphrases used by most users are susceptible to brute-force offline dictionary attacks. Both the IEEE and the Wi-Fi Alliance recommend a passphrase of 20 characters or more, which would give you at least 62 bits of entropy. The entropy of the passphrase increases significantly if a combination of uppercase and lowercase letters, numbers, and special symbols is used in the passphrase. The entropy of a passphrase also increases with each extra character that is added to the passphrase.

In summary, always use, at a minimum, a 20-character passphrase and mix up the characters for your SOHO Wi-Fi solution. Sadly, most people will use their dog's name or their telephone number for their passphrase. In that case, the bigger risk is a social

engineering attack because the passphrase can be easily guessed. Passphrases were never intended for the enterprise. Enterprise APs and WLAN controllers will usually give you the choice of entering either a passphrase or a 64-character PSK. If, for some reason, PSK authentication must be used in the enterprise, avoid using a passphrase altogether and instead manually configure the full 64-hex character PSK.

Is There an Easy Way to Create a Passphrase with Strong Entropy?

The Gibson Research Corporation maintains a free website that will randomly generate unique cryptographic-strength password strings: `https://www.grc.com/passwords.htm`.

Numerous freeware software tools exist that can be used to assist end-users with creating strong passphrases with increased entropy. These tools can be used to increase the strength of passwords, passphrases, and even the shared secrets that are used between a RADIUS server and an authenticator. One example of such as tool is Juniper Networks' Password Amplifier utility. A free copy of Password Amplifier can be found at `www.juniper.net/customers/support/products/aaa_802/oac_demo.jsp#pa`.

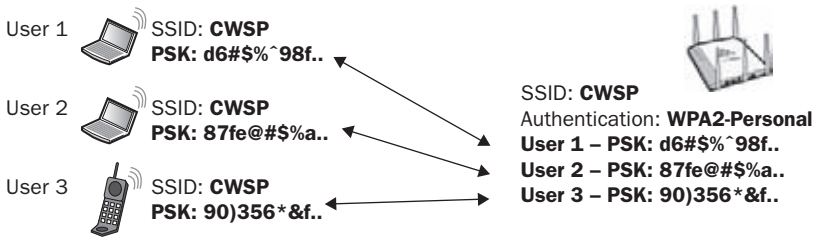
Proprietary PSK

Although the use of passphrases and PSK authentication is intended for use in a SOHO environment, in reality WPA/WPA2-Personal is often still used in the enterprise. For example, even though fast secure roaming (FSR) mechanisms are now possible, many older VoWiFi phones and other handheld devices still do not yet support 802.1X/EAP. As a result, the strongest level of security used with these devices is PSK authentication. Cost issues may also drive a small business to use the simpler WPA/WPA2-Personal solution as opposed to installing and configuring a RADIUS server for 802.1X/EAP.

The biggest problem with using PSK authentication in the enterprise is social engineering. The PSK is the same on all WLAN devices. If end-users accidentally give the PSK to a hacker, WLAN security is compromised. If an employee leaves the company, all the devices have to be reconfigured with a new 64-bit PSK. Because the passphrase or PSK is shared by everyone, a very strict policy should be mandated stating that only the WLAN security administrator is aware of the passphrase or PSK. That, of course, creates another administrative problem because of the work involved in manually configuring each device.

Several enterprise WLAN vendors have come up with a creative solution to using WPA/WPA2-Personal that solves some of the biggest problems using a single passphrase for WLAN access. Each computing device will have its own unique PSK for the WLAN. Therefore, the MAC address of each STA will be mapped to a unique WPA/WPA2-Personal passphrase. A database of the client stations MAC addressees or usernames must be created on an AP or centralized management server. The individual client stations are then assigned individual PSKs that are created either dynamically or manually. As shown in Figure 6.5, the authenticator maintains a database of each individual PSK for each individual client. The PSKs that are generated can also have an expiration date.

FIGURE 6.5 Proprietary PSK



Currently, two WLAN vendors offer *proprietary PSK* solutions, which provide the capability of unique PSKs for each user: Aerohive Networks' Private PSK and Ruckus Wireless' Dynamic PSK. These proprietary PSK solutions prevent social engineering and employee sharing of the passphrase, greatly limit the ability for malicious users to decrypt user traffic, and virtually eliminate the burden for an administrator to limit individual computer access to the WLAN without having to reconfigure each and every WLAN end-user device.

Unfortunately, some WLAN client devices have limited support for 802.1X/EAP. In situations such as these, proprietary PSK solutions may be of benefit for those classes of devices and a vast improvement over standard WPA/WPA2-Personal.

Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS) defines simplified and automatic WPA and WPA2 security configurations for home and small-business users. Users can easily configure a network with security protection by using a personal identification number (PIN) or a button located on the access point and the client device.

WPS was developed by the Wi-Fi Alliance and is a protocol specification that rides over the existing IEEE 802.11-2007 standard. The IEEE does not specify WPS mechanisms. In essence, it is a specification for security *configuration* and network management in the easiest manner possible. The end state provided by using WPS is to prevent unauthorized access and data confidentiality (encryption) of network traffic. While many mechanisms already exist to accomplish this, the manner with which to achieve it is usually too complex and technical for most end-users, especially with small networks.

It is reported by some estimates that 60–70% of wireless networks established have no security enabled, which leaves the network highly vulnerable to attack and eavesdropping. Individual vendors began to create their own security setup mechanisms, which started to cause incompatibility between vendor devices. Furthermore, the Wi-Fi industry as a whole has been plagued with high return rates (20–25% according to Wi-Fi Alliance/Kelton Research in July 2006) and support call volume mostly due to the technical complexity involved with wireless networks.

A white paper from the Wi-Fi Alliance titled "Wi-Fi CERTIFIED for Wi-Fi Protected Setup: Easing the User Experience for Home and Small Office Wi-Fi Networks" is included on the CD that accompanies this book. You will not be tested about WPS in any great detail in the CWSP exam. More detailed information about the Wi-Fi Protected Setup Specification 1.0 can be purchased from `https://www.wi-fi.org/knowledge_center_overview.php?type=4`.

WPS Architecture

Wi-Fi Protected Setup architecture defines three primary and logical roles:

AP An infrastructure-mode 802.11 wireless access point.

Enrollee A device seeking to join the WLAN. Once an enrollee obtains a valid credential, it becomes a member.

Registrar An entity with the authority to issue and revoke access credentials. The registrar issues credentials to Enrollees.

The role of the Registrar may be integrated into an AP, or it may function as a separate device residing behind several APs. When not residing in the AP, it is considered an External Registrar, which can also be a single authority for the entire network (even multiple APs). If the Registrar is external, the APs will need to be configured for the new Registrar running a registration protocol. Because WPS is intended for use in a SOHO environment, the Registrar will usually be integrated within the AP and an External Registrar will not be needed.

The result of adding an AP to a Registrar will include the addition of new Information Elements (IEs) to beacons, probe requests, and probe responses frames. The IEs advertise the WPS capability of the devices. The IEs do not reveal sensitive information but rather provide the details necessary to invoke the WPS process. Part of the flexibility of IEEE 802.11 standard is the ability to provision new IEs without affecting any backward compatibility with legacy or incompatible devices. Devices that are capable of WPS will make use of the WPS IE, but others that are not simply ignore the WPS information.

Security Setup Options

WPS provides consumers several options to set up and enable Wi-Fi security. The two most common security setup options that can be used by WPS are a *personal information number (PIN)* and *push-button configuration (PBC)*. The WPS protocol specification also defines the use of *Near Field Communication (NFC)* tokens and *Universal Serial Bus (USB)* flash drives. All of these methods allow users to configure network names and strong WPA2 data encryption and authentication automatically. The WPS specification

allows for just about any type of Wi-Fi-enabled device to participate in WPS assuming the device supports WPS.

What Is an NFC device?

NFC is a short-range wireless communication technology that operates at 13.56 MHz. Communication between two NFC-compatible devices occurs when they are brought within four centimeters of one another. NFC is mostly used in cell phones and cameras, but could also be used with WLAN devices that support Wi-Fi Protected Setup (WPS).

More information about NFC technology can be found at the NFC Forum website at `www.nfc-forum.org`.

Registration Protocol

The Registration Protocol accomplishes the following purposes:

- It helps to troubleshoot basic connectivity problems with the wireless channel.
- It provides demonstrative identification of the Enrollee to the Registrar and the Registrar to the Enrollee using out-of-band information, enabling the credential configuration function.
- It establishes the roles of each device (AP, Registrar, or Enrollee).
- It securely conveys WLAN settings and other configuration from the Registrar to the Enrollee.
- It establishes an Extended Master Session Key EMSK, which can be used to secure additional application-specific configuration functions.

The *Registration Protocol* is defined to run in-band, out-of-band, or a combination thereof. In the case of in-band configuration, a Diffie-Hellman key exchange is performed to confirm that the Enrollee indeed knows the password. The password itself can be derived from manual user input, USB flash drives, or near-field communication (NFC).

In the case of out-of-band configuration, USB flash drives and NFC are both methods specified by WPS.

The Registration Protocol operates in two phases. The first phase is to exchange public keys and information about the Enrollee and the Registrar. The first phase also enables presence and feature discovery. During the first phase, the Enrollee may be communicating with more than one AP or Registrar, and the user may choose an AP.

If both devices decide to proceed to the second phase, three additional round-trips may be performed to complete the authentication and credential provisioning. The second phase is also designed to establish mutual authentication based on the Enrollee's device password. If there is/are External Registrar(s), the AP will be communicating with both the Enrollee

and the External Registrar(s) during this phase. The Registration Protocol results in WLAN credentials being delivered to the Enrollee.

In-band Configuration Mode

When using in-band configuration mode, a Diffie-Hellman key exchange is performed and authenticated using a shared secret called a device password. The device password is obtained from the Enrollee and is entered into the Registrar using one of the methods described in the "Security Setup Options" section earlier. When you use a physical security setup option, such as a USB or NFC token, you achieve the added security benefit of also exchanging the public key of the Enrollee to the Registrar. This helps to strengthen the mutual authentication trust relationship.

WPS in-band configuration is designed to protect against passive eavesdropping attacks and to also detect and protect against active, brute-force attacks. When the Registrar engages with an Enrollee, it first checks to make sure it knows the password. This is done in the first part of the configuration mode and before enough information is exposed to perform a brute-force attack.

Out-of-Band Configuration Mode

When out-of-band configuration mode is used, there are three options specified by WPS.

The first is with *unencrypted settings* that are stored on out-of-band media like an NFC or USB flash drive. The premise in this method is that the out-of-band media is always in possession (perhaps under lock and key) and is never obtained by a hacker. Of course, should an unauthorized user obtain the media, the security of this method is compromised.

Second, we have *encrypted settings* derived from the Diffie-Hellman public key of the Enrollee first obtained over the in-band channel with the Registrar to encrypt settings for that specific Enrollee.

Lastly, NFC interfaces operating in peer-to-peer mode may be used. NFC is considered not to have any feasible attack methods and is also protected from a 1536-bit Diffie-Hellman exchange. While the NFC communication is protected by this exchange, the WLAN settings are also 128-bit AES encrypted. The Diffie-Hellman public keys and WLAN settings are implicitly authenticated by both the Registrar and the Enrollee because they are received over the NFC interface.

Guidelines and Requirements for PIN Values

The WPS specification does provide some guidance and requirements for PIN values. The minimum recommended length of a numeric PIN is 8 digits. Although PINs less than 8 digits in length technically do not provide enough variance for strong mutual authentication, the Registration Protocol protects the actual PIN against dictionary attacks on fresh PINs.

Furthermore, the standard specifies that PIN values must be randomly generated and not a derivative of any information that can be obtained by an eavesdropper. While that seems like common sense, it is actually called out in the standard and required by manufacturers

to follow. This would include information such as MAC address, model number, serial number, brand name of the company, and so forth. The standard also specifies that, if more than one PIN value is present in the system, they must be cryptographically separate from each other.

Devices may be preconfigured with PINs (and typically should for ease of use) as part of a packaged solution that consumers purchase. The standard does not specify a lifetime to these values, but in the case of too many failed attempts, it is recommended that you invalidate the preconfigured PIN.

Initial WLAN Setup

When setting up an initial WLAN, there are three primary scenarios using WPS. The first and simplest case is when using a standalone AP that has a built-in Registrar. The second is using a legacy (non-WPS capable) AP. In this mode, the AP will not participate in the security setup process and the Enrollee will communicate to an External Registrar. The third case is when a WPS-capable AP has one or more External Registrars and is granted authority by the AP to issue credentials to Enrollees.

There are some security and usability considerations for each mode that we will discuss briefly. In standalone AP mode, the limitations of the user interface and device storage are the primary considerations. The ability to guide a user through the setup process and adequately explain any errors or problems that have been encountered may be an issue on a standalone AP without a visual display.

The consideration with legacy APs is primarily the problem of distributing sufficiently strong keys to the legacy AP. Therefore, the user is likely to create a simpler, and therefore weak, WPA-Personal passphrase that is susceptible to offline dictionary attack.

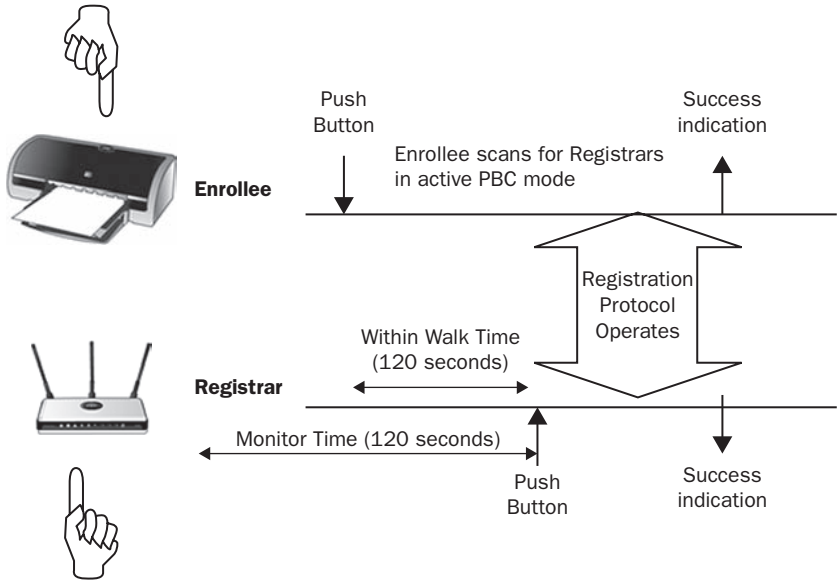
We recommend that APs with External Registrars use the in-band setup for only a limited time. The AP's device password is unlikely to be very strong, and the AP will be more susceptible to attack if it remains in setup mode.

While WPS has been mostly discussed as using WPA/WPA2-Personal modes, the protocol itself can theoretically configure any supported WPA-based security model. Therefore, it is possible to enable an 802.1X/EAP type for subsequent WLAN authentications of member devices.

Example WPS Push-Button Scenario

To help paint the picture of what the real end-user experience should look like, it is best to look at an example use case. The PBC mode seems to have gained the greatest adoption by manufacturers, and the sequences described next are according to the best practices published by the Wi-Fi Alliance. Refer to Figure 6.6 as you follow the PBC sequences. In Figure 6.6, a wireless printer will be the Enrollee and an access point will be the Registrar.

FIGURE 6.6 Wi-Fi Protected Setup—push-button configuration



WPS Push-Button Enrollee Addition

The WPS push-button configuration (PBC) method requires a user to push a button on both the Enrollee and the Registrar within two minutes of each other. This time interval is called the Walk Time. The sequence initiation can be triggered from either end, and the sequence is as follows:

1. The user purchases a new WPS end-user device (Enrollee) and presses a button to trigger an Enrollee addition. While there may not be a physical button on the device, this mode also includes a software-based button, perhaps through a web-based interface. The device may indicate that WPS has been initiated by using a special LED or software message. The device UI should direct the user to trigger the AP/router next.
2. The user initiates WPS on the AP/router (Registrar) with a push-button within two minutes of initiating it on the end-user device. The AP/router should have a designated button on the device that is clearly labeled. To initiate the WPS process, the method should be very simple and clearly convenient for the user.
3. The user walks back to the WPS end-user device to confirm successful completion of the WPS process with a clear visual indication. If any errors were encountered in the process, the cause of the error should be clearly explained on the end-user device. If this is not possible, the device should have a reference sheet that a user can check for a blinking LED sequence.

SOHO Security Best Practices

We have discussed all the technical aspects regarding WPA/WPA2-Personal, which is the security method most often used at home. The following are some simple SOHO security best practices that should be used by average home users to secure their home WLAN:

Default Settings The first and biggest mistake that most home wireless network users make is that they just power up the box and leave all the default configuration settings enabled on the home wireless gateway device. The two most obvious default settings would be the SSID and the administrator login name/password. A simple Google search will generate links to numerous sites that have compiled lists of all the default settings for the products of many wireless vendors. Any individual can also simply download the PDF manual with the same information from the vendor's website. Amateur hackers, wardrivers, and script-kiddies will always target the wide open WLANs first. Using the vendor's default settings is analogous to leaving the front door of your house always open. Do not use the default SSID, and change the device's administrator login name and admin login password. Also, if the device allows, change the default IP address.

SSID Name Do not use a SSID that can clearly identify who you are. Do not use a family surname, your street address, or your dog's name. Choose a network name with no meaning—something such as Rhj18YT89. Please be aware that SSID's are "case sensitive" and must match on both the Wi-Fi home router and the client stations.

SSID Cloaking In Chapter 2, "Legacy 802.11 Security," you learned that anyone with a WLAN protocol analyzer can discover a hidden SSID. You also learned that hiding the SSID in an enterprise environment is not always recommended. Although a cloaked SSID can still be discovered, there is no harm in hiding the SSID in a home network, and it adds another very thin layer of security.

MAC Filters You also learned in Chapter 2 that anyone can spoof a MAC address and bypass a MAC filter. However, using a MAC filter is an extra layer of security. A MAC filter at home does not require much administration because most homes have only two or three devices communicating through the Wi-Fi router.

WPA2-Personal Use CCMP-AES encryption and use a 20-character or longer passphrase. Write down the passphrase and store it in a safe place. More important, do not tell anyone the passphrase.

Summary

After reading this chapter, you should have a better grasp of why WPA/WPA2-Personal is considered a SOHO solution, and you now have some methods to help secure those environments as best as possible. WPA/WPA2-Personal methods have come a long way

from WEP in both end-user configuration convenience and even the security they provide. However, the entropy strength of a passphrase still depends on the complexity used in creating the passphrase.

The Wi-Fi Alliance has gone a step further and has provided the WPS specification to the entire Wi-Fi industry to make the actual configuration process even easier, and it is potentially even more secure for home users. WPS can theoretically scale to multiple APs using redundant External Registrars, thus providing a network large enough for many Wi-Fi users in a small office.

Adoption of WPS capabilities in enterprise-grade WLAN equipment is so far nonexistent, and that is not likely to change anytime soon. The 802.1X/EAP solutions discussed in Chapter 4 should always be used in enterprise environments. WPS should not be used in the enterprise.

Exam Essentials

Explain PSK authentication. PSK authentication is meant to be used in SOHO environments because the stronger enterprise 802.1X authentication solutions are not available. PSK authentication is also known by the more common name of WPA-Personal or WPA2-Personal.

Define entropy and how it relates to PSK authentication. Passwords or passphrases by themselves have an entropy value of zero. Entropy is a measure of uncertainty associated with a random variable. The method you use to select a passphrase can be measured in terms of randomness.

Understand passphrase-to-PSK mapping. Explain how the passphrase-to-PSK formula uses a hash algorithm to mix the SSID with the passphrase. Understand the security weaknesses associated with this method.

Explain the advantages of proprietary PSK solutions. Proprietary PSK solutions prevent social engineering and employee sharing of a passphrase. Proprietary PSK solutions greatly limit the ability of malicious users to decrypt user traffic and simplify administration.

Define WPS architecture and mechanisms. Wi-Fi Protected Setup (WPS) defines simplified and automatic WPA and WPA2 security configurations for home and small-business users. WPS architecture defines three primary roles: AP, Enrollee, and Registrar.

Key Terms

Before you take the exam, be certain you are familiar with the following terms:

4-Way Handshake
AP
brute-force dictionary attack
Enrollee
entropy
Near Field Communication (NFC)
Pairwise Master Key (PMK)
passphrase
passphrase-PSK mapping
personal information number (PIN)
preshared (PSK)
proprietary PSK
push-button configuration (PBC)
Registrar
Registration Protocol
robust security network (RSN)
small office, home office (SOHO)
Universal Serial Bus (USB)
Wi-Fi Protected Access (WPA)
Wi-Fi Protected Setup (WPS)
WPA2-Personal
WPA-Personal

Review Questions

1. What are the main components of the Wi-Fi Protected Setup (WPS) architecture? (Choose all that apply.)
   - **A.** Enrollee
   - **B.** Supplicant
   - **C.** NFC server
   - **D.** Access point
   - **E.** Authentication server
   - **F.** Registrar
   - **G.** Authenticator

2. When configuring an 802.11 client station for WPA2-Personal, what security credentials can be used? (Choose all that apply.)
   - **A.** Server-side certificate
   - **B.** 64-bit PSK
   - **C.** 8-63 character PSK
   - **D.** Token card
   - **E.** Client-side certificate
   - **F.** 64-character passphrase
   - **G.** 8-to-63 character passphrase

3. What inputs are used by passphrase-PSK mapping to create a final 256-bit PSK during 802.11 PSK authentication? (Choose all that apply.)
   - **A.** BSSID
   - **B.** SNonce
   - **C.** SSID
   - **D.** Client MAC address
   - **E.** AP MAC address
   - **F.** Passphrase
   - **G.** ANonce

4. Tammy, the WLAN security engineer, has recommended to management that WPA-Personal security not be deployed within the ACME company's WLAN. What are some of the reasons for Tammy's recommendation? (Choose all that apply.)
   - **A.** Static passphrases and PSKs are susceptible to social engineering attacks.
   - **B.** WPA-Personal is susceptible to brute-force dictionary attacks, but WPA-Personal is not at risk.

C. WPA-Personal uses static encryption keys.

D. WPA-Personal uses weaker TKIP encryption.

E. 802.11 data frames can be decrypted if the passphrase is compromised.

5. When considering the 4-Way Handshake that is used to create dynamic encryption keys, what is the main difference between 802.1X/EAP and PSK authentication? (Choose all that apply.)

A. 802.1X supplicants all use the same PMK.

B. Clients that use PSK authentication all use the same PTK.

C. 802.1X supplicants all use a different PMK.

D. Clients that use PSK authentication all use a different PTK.

E. 802.1X supplicants all use a different PTK.

F. Clients that use PSK authentication all use the same PMK.

6. What is the Wi-Fi Alliance recommendation for the number of characters used in a passphrase for WPA/WPA2-Personal security?

A. 6 characters

B. 8 characters

C. 10 characters

D. 12 characters

E. 20 characters

7. Don has been hired as a consultant to secure the Maxwell Corporation's WLAN infrastructure. Management has asked him to choose a WLAN authentication solution that will best protect the company's branch offices from unauthorized users. The branch offices will use older VoWiFi phones that are not 802.11r-2008 compliant. The company is also looking for the strongest dynamic encryption solution for data privacy reasons. Management is also looking for the cheapest solution as well as a solution that is easy to administer. Which of these WLAN security solutions meets all the objectives required by management? (Choose the best two answers.)

A. WPA-Personal

B. WPA2-Personal

C. WPA-Enterprise

D. WPA2-Enterprise

E. Proprietary PSK

8. Which of these security setup options are available for Wi-Fi Protected Setup (WPS)?

A. NFC

B. PIN

C. USB

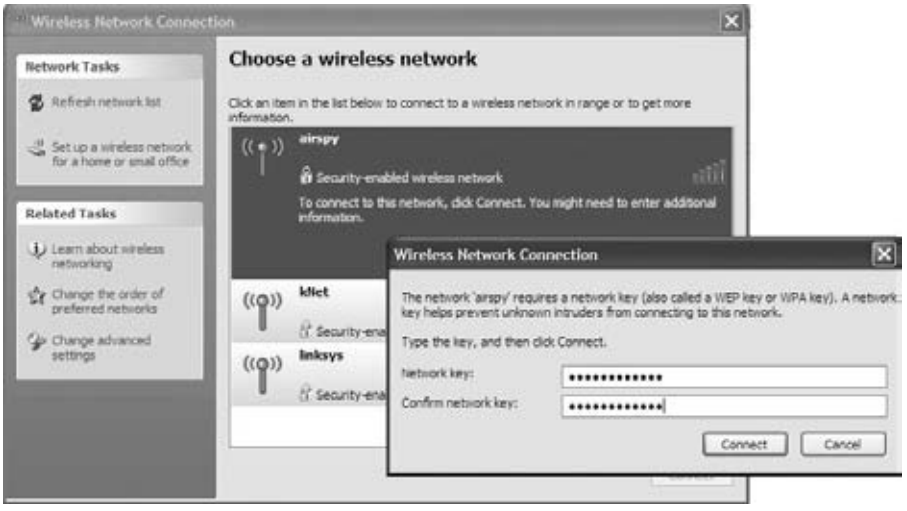
D. PBC

E. All of the above

9. The IEEE 802.11-2007 standard requires an authentication and key management protocol (AKMP) that can be either a preshared (PSK) or an EAP protocol used during 802.1X authentication. What is another name for PSK authentication? (Choose all that apply.)
   - **A.** Wi-Fi Protected Setup
   - **B.** WPA/WPA2-Personal
   - **C.** WPA/WPA2-PSK
   - **D.** WPA/WPA2-Preshared Key
   - **E.** WPA/WPA2-Passphrase

10. Which of these terms best describes a measure of uncertainty associated with a random variable?
   - **A.** Entropy
   - **B.** Encryption
   - **C.** Encapsulation
   - **D.** Encoding

11. After viewing the image shown here, identify the type of WLAN security method being used.



   - **A.** EAP-TLS
   - **B.** CCMP/AES
   - **C.** Dynamic PSK
   - **D.** EAP-TTLS
   - **E.** None of the above

12. Which of these passphrases is the least susceptible to a brute-force offline dictionary attack?

- **A.** 20-character passphrase using numerical digits (0–9)
- **B.** 20-character passphrase using single-case letters (a–z)
- **C.** 20-character passphrase using single-case letters and digits (a–z, 0–9)
- **D.** 20-character passphrase using mixed-case letters and digits (a–z, A–Z, 0–9)

13. Based on the IEEE's estimation of entropy strength for each character used in the average WPA/WPA2 passphrase, how many entropy bits of security would be in an eight-character passphrase?

- **A.** 8 bits
- **B.** 12 bits
- **C.** 20 bits
- **D.** 32 bits
- **E.** 64 bits

14. Which two-phase protocol is used in a Wi-Fi Protected setup communications?

- **A.** Registration Protocol
- **B.** Enrollee protocol
- **C.** EAP-PEAP
- **D.** EAP-TLS
- **E.** EAP-TTLS

15. Name some recommended best practices for securing a home Wi-Fi router. (Choose all that apply.)

- **A.** MAC filter
- **B.** Hidden SSID
- **C.** Change the default settings
- **D.** WPA2-Personal security

16. After viewing the image shown here, what type of credentials can be strengthened with the software application that is depicted? (Choose all that apply.)

A. Passwords

B. Shared secrets

C. Passphrases

D. Pairwise master keys

E. Pairwise transient keys

F. Group temporal keys

17. The ACME company is using WPA2-Personal to secure handheld barcode scanners that are not capable of 802.1X/EAP authentication. Because an employee was recently fired, all the barcode scanners and APs had to be reconfigured with a new static 64-bit PSK. What type of WLAN security solution may have avoided this administrative headache?

A. MAC filter

B. Hidden SSID

C. Change the default settings

D. Proprietary PSK

18. If an 802.1X/EAP solution is not available in the enterprise, which of these security credentials should be used instead?

A. Static 64-character PSK

B. WPA passphrase with 64 bits of entropy

C. WPA2 passphrase with 64 bits of entropy

D. Static WEP key

19. Which of these Wi-Fi Alliance security certifications specify mechanisms not defined by the IEEE-2007 standard?

A. WPA-Personal

B. WPA-Enterprise

C. WPA2-Personal

D. WPA2-Enterprise

E. Wi-Fi Protected Setup

20. The SSID is a logical identifier of a WLAN. Which of these SSIDs would be considered more secure for a home Wi-Fi router?

A. Coleman Family

B. 2436 Peachtree Street

C. Bob's House

D. Rhj18YT89

E. Snoopy

Answers to Review Questions

1. A, D, F. The WPS architecture defines three primary devices: an infrastructure-mode 802.11 wireless access point (AP); an Enrollee, which is a device seeking to join the WLAN; and the Registrar, which is an entity with the authority to issue and revoke access credentials. The Registrar issues credentials to Enrollees. The role of the Registrar may be integrated into an AP, or it may function as a separate device residing behind several APs. Because WPS is intended for use in a SOHO environment, the Registrar will usually be integrated within the AP and an External Registrar will not be needed.

2. B, G. WPA/WPA2-Personal uses PSK authentication. A PSK used in a robust security network is 256 bits in length, or 64 characters when expressed in hex. A preshared key (PSK) is a static key that is configured on the access point and all of the clients. However, in most SOHO environments, an 8-to-63 character passphrase is instead configured on the AP and all of the clients. The passphrase-PSK mapping formula transforms the simple ASCII passphrase to the 256-bit PSK.

3. C, F. The passphrase-PSK mapping formula is defined by the 802.11-2007 standard to allow end-users to use a simple ASCII passphrase that is then converted to the 256-bit PSK. The passphrase is combined with the SSID and hashed 4096 times to produce a 256-bit (64-character) PSK. MAC addresses and nonces are inputs used during the 4-Way Handshake.

4. A, D, E. The risks involved with both WPA-Personal and WPA2-Personal are basically twofold: network resources can be placed at risk and the encryption keys can be compromised. A hacker can obtain the passphrase using either social engineering skills or using an offline brute-force dictionary attack. Once the passphrase is compromised, the hacker can use any client station to associate with the WPA/WPA2-Personal access point. The hacker is then free to access network resources. The hacker can also use the passphrase to re-create encryption keys. The hacker can then decrypt any unicast traffic between the AP and the individual client. WPA-Personal uses TKIP/RC4 encryption and is not necessarily a security risk; however, the stronger CCMP/AES encryption mandated by WPA2-Personal would be preferable.

5. C, F. The 802.1X/EAP process is used to create a pairwise master key (PMK), which is the seeding material for the 4-Way Handshake that is used to create the final temporal encryption keys. Every time a supplicant authenticates within an 802.1X architecture, a unique PMK is created. The same cannot be said when PSK authentication is used. The 256-bit PSK is the PMK. Because every client station uses the same PSK or passphrase that is converted to a PSK, every client station has the same pairwise master key (PMK).

6. E. The simple passphrases used by most users are susceptible to brute-force offline dictionary attacks. Both the IEEE and the Wi-Fi Alliance recommend a passphrase of 20 characters or more. The strength of the passphrase increases significantly if a combination of uppercase and lowercase letters, numbers, and special symbols are used in the passphrase.

7. B, E. Because the Maxwell Corporation is using older VoWiFi phones that are not 802.11r-2009 compliant, they probably will not support fast secure roaming (FSR)

mechanisms that will work with an 802.1X/EAP solution. WPA/WPA2 Enterprise security requires an 802.1X/EAP solution. WPA2-Personal security provides the strongest available CCMP/AES encryption, and it uses simple PSK authentication that can be used with the VoWiFi phones. A Proprietary PSK solution could further enhance security because each individual VoWiFi phone would have a unique PSK.

8. E. The two most common security setup options that can be used by WPS are a personal information number (PIN) and push-button configuration (PBC). The WPS protocol specification also defines the use of Near Field Communication (NFC) cards and Universal Serial Bus (USB) flash drives. All of these methods allow users to configure network names and strong WPA2 data encryption and authentication automatically.

9. B, C, D, E. WPA-Personal and WPA2-Personal both use the PSK authentication method required by the IEEE 802.11-2007 standard. However, WLAN vendors have many names for PSK authentication, including WPA/WPA2-Passphrase, WPA/WPA2-PSK, and WPA/WPA2-Preshared Key. The correct Wi-Fi Alliance terminology is WPA/WPA2-Personal. All of these terms refer to 802.11 PSK authentication.

10. A. In digital communications, entropy is a measure of uncertainty associated with a random variable. The more entropy (measured in bits) that is contained within the method used to create a passphrase, the more difficult it will be to guess the passphrase.

11. E. The image depicts an 802.11 client station being configured with a static key that is used for WEP or possibly a passphrase used for PSK authentication. Client software utilities do not always use the proper terminology. The WPA key referenced in the graphic refers to a passphrase used in WPA-Personal security. WPA-Personal and WPA2-Personal both use the PSK authentication method. WPA-Personal specifies TKIP/RC4 encryption and WPA2-Personal specifies CCMP/AES.

12. D. Passwords or passphrases by themselves have an entropy value of zero. It is the method you use to select the passphrase that contains the entropy. A strong passphrase will have more entropy bits per character than a password created from your name or your phone number. The more entropy (measured in bits) that is contained within the method you use to create your passphrase, the more difficult it will be to guess the passphrase.

13. D. Each character in a passphrase is only worth 2.5 bits of entropy because most users use easy-to-remember words as opposed to a mix of alphanumeric and punctuation characters. Therefore, an 8-character passphrase would only contain about 20-bits of entropy before the passphrase-to-PSK mapping hash algorithm is calculated. Because the passphrase-to-PSK mapping mixes the SSID with the passphrase, approximately 12 extra bits of entropy are added. Therefore, a typical 8-character passphrase used in a WPA/WPA2-Personal configuration would have a total of about 32 bits of entropy.

14. A. The Registration Protocol operates in two phases. The first phase is to exchange public keys and information about the Enrollee and the Registrar. The first phase also enables presence and feature discovery. The second phase is designed to also establish mutual authentication based on the Enrollee's device password. The Registration Protocol results in WLAN credentials being delivered to the Enrollee.

15. A, B, C, D. The most important aspect of SOHO security would be to use a WPA2-Personal solution with CCMP/AES encryption and a 20-character or stronger passphrase. Hiding the SSID and using a MAC filter add extra security even though both methods can be compromised. Default settings should always be changed.

16. A, B, C. Numerous freeware software tools exist that can be used to assist end-users with creating strong passphrases with increased entropy. These tools can be used to increase the strength of passwords, passphrases, and even the shared secrets that are used between a RADIUS server and an authenticator.

17. D. The biggest problem with using PSK authentication in the enterprise is social engineering. The PSK is the same on all WLAN devices. If the end-users accidentally give the PSK to a hacker, WLAN security is compromised. If an employee leaves the company, all the devices have to be reconfigured with a new 64-bit PSK, creating a lot of work for an administrator. Several WLAN vendors offer proprietary PSK solutions where each individual client device will have its own unique PSK. These proprietary PSK solutions prevent social engineering attacks. These proprietary PSK solutions also virtually eliminate the burden for an administrator having to reconfigure each and every WLAN end-user device.

18. A. In the enterprise, using a static 256-bit PSK as opposed to a passphrase is always the preferred method. A PSK used in a robust security network is 256 bits in length, or 64 characters when expressed in hex. A preshared key (PSK) is a static key that can be configured on the access point and all of the clients. Furthermore, do not confuse entropy security bits with the number of digital bits in a PSK. The passphrase-PSK mapping formula will always convert any passphrase of 8 to 63 characters into a 256-bit PSK. Entropy bits are a measure of uncertainty associated with a random variable. The random variable is basically the strength of the passphrase.

19. E. Wi-Fi Protected Setup (WPS) defines simplified and automatic WPA and WPA2 security configurations for home and small-business users. WPS was developed by the Wi-Fi Alliance and is a protocol specification that rides over the existing IEEE 802.11-2007 standard. The IEEE does not specify WPS mechanisms.

20. D. SOHO security best practices dictate that an SSID should not identify who you are. Do not use a family surname, your street address, or your dog's name. Choose a network name with no meaning—something such as Rhj18YT89. Please be aware that SSIDs are case sensitive and must match on both the Wi-Fi home router and the client stations.

Chapter 7

802.11 Fast Secure Roaming

IN THIS CHAPTER, YOU WILL LEARN ABOUT THE FOLLOWING:

- ✓ **History of 802.11 roaming**
  - Client roaming thresholds
  - AP-to-AP handoff
- ✓ **RSNA**
  - PMKSA
  - PMK caching
  - Preauthentication
- ✓ **Opportunistic key caching (OKC)**
- ✓ **Proprietary FSR**
- ✓ **Fast BSS transition (FT)**
  - Information elements
  - FT initial mobility domain association
  - Over-the-air fast BSS transition
  - Over-the-DS fast BSS transition
- ✓ **802.11k**
- ✓ **Voice Personal and Voice Enterprise**
- ✓ **Layer 3 roaming**
- ✓ **Troubleshooting**
- ✓ **SCA roaming**

One of the main reasons that Wi-Fi networks have spread like wildfire is the fact that 802.11 technology provides mobility. In today's world, end-users demand the freedom provided by WLAN mobility. Corporations also realize productivity increases if end-users can access network resources wirelessly. Mobility requires that client stations have the ability to transition from one access point to another while maintaining network connectivity for the upper-layer applications. This ability is known as *roaming*. A perfect analogy is the roaming that occurs when using a cellular telephone. When you are talking on a cell phone to your best friend while riding in a car, your phone will roam between cellular towers to allow for seamless communications and hopefully an uninterrupted conversation. Seamless roaming between access points allows for WLAN mobility, which is the heart and soul of true wireless networking and connectivity. This chapter will cover the history of 802.11 roaming, beginning with legacy autonomous APs and moving on to roaming within WLAN controller environments.

This chapter will also explore the relationship between roaming and security. Although mobility is paramount to any WLAN, maintaining security is just as important. Ideally, all client stations should use WPA2-Enterprise level security when roaming between access points. However, roaming can be especially troublesome for VoWiFi and other time-sensitive applications when using a WPA-Enterprise or WPA2-Enterprise security solution, which involves the use of a RADIUS server. Due the multiple frame exchanges between the authentication server and the supplicant, an 802.1X/EAP authentication often takes 700 milliseconds (ms) or greater for the client to authenticate. VoWiFi requires a handoff of 150 ms or less to avoid a degradation of the quality of the call or, even worse, a loss of connection. Therefore, faster and secure roaming handoffs are required.

This chapter will discuss a variety of methods that allow for *fast secure roaming (FSR)*. The 802.11i security amendment, which is now part of the 802.11-2007 standard, defines two fast secure roaming mechanisms called preauthentication and PMK caching. Most WLAN vendors currently use an enhanced method of FSR called opportunistic PMK caching. Now that the 802.11r-2008 amendment has been ratified, even more complex FSR methods will begin to find their way into the enterprise. As FSR gains broader acceptance, time-sensitive applications, such as voice and video, will use stronger authentication security without a disruption in communications.

History of 802.11 Roaming

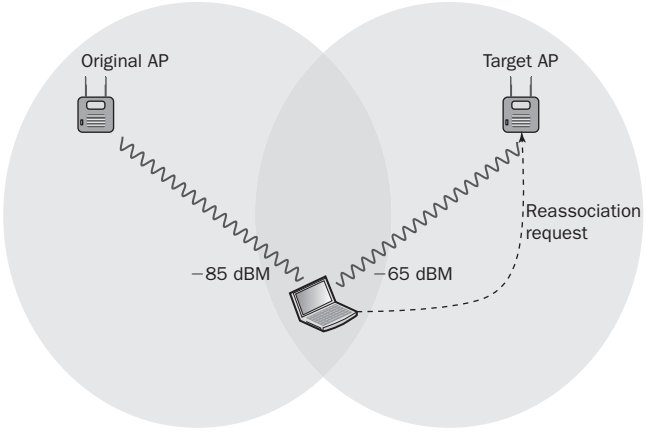
Before we can delve into the relationship between roaming and security, we must first discuss the basics of roaming as well as a little history. The original legacy 802.11

standard, for the most part, only defined roaming as a Layer 2 process known as the reassociation service. The *reassociation service* enables an established association between an access point (AP) and a client station (STA) to be transferred from one AP to another AP. Reassociation allows a client station to move from one basic service set (BSS) to another, and therefore a more technical term used for roaming is *BSS transition*. However, the 802.11-2007 standard does not define two very important processes for BSS transition: client roaming thresholds and AP-to-AP handoff communications.

Client Roaming Thresholds

In standard WLAN environments, client stations always initiate the roaming process known as reassociation. In simpler words, clients make the roaming decision and access points do not tell the client when to roam. What causes the client station to roam is a set of proprietary rules determined by the manufacturer of the wireless card, usually defined by *received signal strength indicator (RSSI)* thresholds. RSSI thresholds usually involve signal strength, noise level, and bit-error rate. As the client station communicates on the network, it continues to look for other access points via probing and will hear received signals from other APs. As shown in Figure 7.1, as the client station moves away from the original access point with which it is associated and the signal drops below a predetermined threshold, the client station will attempt to connect to a new target access point that has a stronger signal. The client sends a frame, called the reassociation request frame, to start the roaming procedure.

FIGURE 7.1 Client roaming decision



Vendors will have different thresholds that kick off the client reassociation process. In other words, two client stations could be associated with the same AP and receiving the same signal strength, yet one of them may roam before the other because they have

different vendor RSSI roaming thresholds. The roaming thresholds in handheld devices tend to encourage roaming more often than the roaming thresholds of WLAN radios found in laptops. The bottom line is that clients make the roaming decision, and all client roaming thresholds are proprietary.

AP-to-AP Handoff

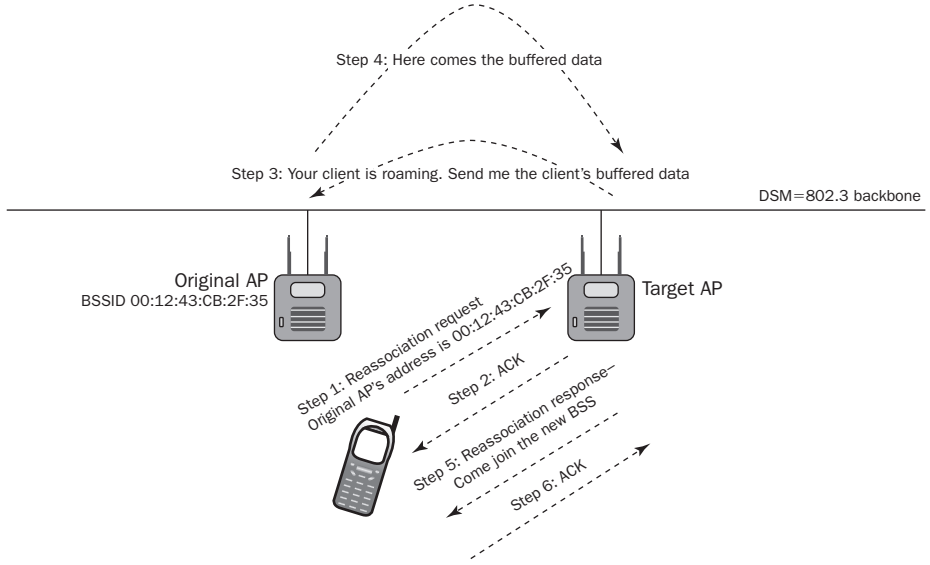
The 802.11-2007 standard also does not define AP-to-AP handoff communications. As the station roams, the original access point and the target access point should communicate with each other across the *distribution system medium (DSM)* and help provide a clean transition between the two APs. The DSM is also simply referred to as the *distribution system (DS)*. The DS is typically an 802.3 wired network. The AP-to-AP handoff communications involves two primary tasks:

- The target AP informs the original AP that the client station is roaming.
- The target AP requests the client's buffered packets from the original AP.

When the 802.11 standard was first ratified, only autonomous APs existed. Let's discuss how roaming works with legacy autonomous APs. As shown in Figure 7.2, roaming occurs after the client and the access point have exchanged reassociation frames, as described in the following steps:

1. In the first step, the client station sends a reassociation request frame to the target access point. The reassociation request frame includes the BSSID (MAC address) of the access point to which it is currently connected (we will refer to this as the original AP).
2. The target access point then replies to the station with an ACK.
3. The target access point attempts to communicate with the original AP by using the distribution system (DS). The target access point attempts to notify the original AP about the roaming client to inform the original AP that the client is leaving the original BSS. The target AP also requests that the original AP forward any buffered data. Please remember that these communications between the APs via the DSM are not defined by the 802.11-2007 standard and are proprietary.
4. If this communication is successful, the original access point will use the distribution system medium to forward any buffered data to the target access point.
5. The target access point then sends a reassociation response frame to the client via the wireless network.
6. The client sends an ACK to the target access point. The client has now joined the BSS of the target AP.
7. If the reassociation is not successful, the client will retain its connection to the original AP and either will continue to communicate with the original AP or attempt to roam to another access point.

FIGURE 7.2 Reassociation



When autonomous APs are used, AP-to-AP roaming handoffs present two problems. First, because the back-end communications are proprietary, different vendors' APs would not effectively talk to each other.

The IEEE initially intended for vendors to have flexibility in implementing proprietary AP-to-AP roaming mechanisms. The IEEE proposed the 802.11F amendment in an attempt to standardize how roaming mechanisms work behind the scenes on the distribution system medium, which is typically an 802.3 Ethernet network using TCP/IP networking protocols. 802.11F addressed "vendor interoperability" for AP-to-AP roaming. The final result was a recommended practice to use the *Inter-Access Point Protocol (IAPP)*. The IAPP protocol uses announcement and handover processes that result in autonomous APs informing other autonomous APs about roaming clients as well as delivery of buffered packets. 802.11F was never ratified and is no longer even a recommended practice. Because most WLAN vendors now use controller-based systems with controller-based access points, IAPP is no longer needed. It should be noted that mixing controller-based solutions from different WLAN vendors is also not advisable.

The second problem with legacy autonomous AP-to-AP roaming handoffs was the latency involved with forwarding the buffered packets between APs. The handoff times with autonomous APs were very slow. In WLAN controller-based solutions, the roaming handoff mechanisms occur within the WLAN controller. The client station packets are also buffered on the centralized WLAN controller and do not have to be forwarded between APs. Therefore, the roaming handoffs that occur within WLAN controllers are much faster than roaming handoffs between legacy autonomous access points.

Now that you have learned the basics of roaming, we will now begin to discuss the relationship between roaming and security.

RSNA

Let's review a few things you already learned in Chapter 5, "802.11 Dynamic Encryption Key Generation." The 802.11i amendment, which was ratified and published as IEEE Std. 802.11i-2004, defined stronger encryption and better authentication methods. The 802.11i security amendment is now part of the 802.11-2007 standard. The 802.11-2007 standard defines what is known as a robust security network (RSN) and robust security network associations (RSNAs).

Keep in mind that a *robust security network association (RSNA)* requires two 802.11 stations (STAs) to establish procedures to authenticate and associate with each other as well as create dynamic encryption keys through the *4-Way Handshake* process. This security association between two stations is referred to as an RSNA. In other words, any two radios must share dynamic encryption keys that are unique between those two radios. CCMP/AES encryption is the mandated encryption method, whereas TKIP/RC4 is an optional encryption method.

Every time a client roams, unique encryption keys must be generated using a 4-Way Handshake process between the access point and the client STA. As you have already learned, either an 802.1X or PSK authentication process is needed to produce the *pairwise master key (PMK)* that seeds the 4-Way Handshake. Therefore, every time a client roams, the client must reauthenticate. An 802.1X framework requires multiple EAPOL frames to be exchanged between the supplicant and the authentication server (AS). If a client station has to reauthenticate using 802.1X/EAP every time, the roaming process will be secure but the delay will be significant. This delay will disrupt the communications of time-sensitive applications such as voice and video. A typical 802.1X/EAP roaming handoff can take 700 ms, which far exceeds the needed handoff time of 150 ms or less for VoWiFi. Secure roaming handoff times will be even worse if the RADIUS server resides across a WAN link. The 802.11i security amendment is now part of the 802.11-2007 standard and defines two fast secure roaming mechanisms called preauthentication and PMK caching, which will be discussed later in this chapter.

PMKSA

Robust security network associations (RSNAs) can be broken down into several subtypes. *A pairwise master key security association (PMKSA)* is the result of a successful IEEE 802.1X authentication exchange between a supplicant and authentication server (AS) or from a preshared key (PSK) authentication. In other words, once the PMK has been created, a bidirectional security association exists between the authenticator and the supplicant. As you learned in Chapter 5, the PMK is the seeding material for the 4-Way

Handshake that creates the *pairwise transient key (PTK),* which is used for encryption and decryption of unicast traffic. Once the 4-Way Handshake creates the final encryption keys, a *pairwise transient key security association (PTKSA)* exists between the authenticator and the supplicant. In Chapter 5, we discussed in great detail how the 4-Way Handshake process results in a PTKSA. In this chapter, we will focus more on pairwise master key security associations (PMKSAs).

RSN security can be identified by a field found in certain 802.11 management frames. This field is known as the *robust security network information element (RSNIE),* which is often referred to simply as the *RSN information element*. An information element is an optional field of variable length that can be found in 802.11 management frames. The RSN information element field is found in four different 802.11 management frames: beacon management frames, probe response frames, association request frames, and reassociation request frames. In Chapter 5, you learned about the authentication key management (AKM) suites and pairwise cipher suites found in the RSN information element. Figure 7.3 shows the entire format of the RSN information element. Notice the PMKID fields within the RSN information element.

FIGURE 7.3 RSN information element format

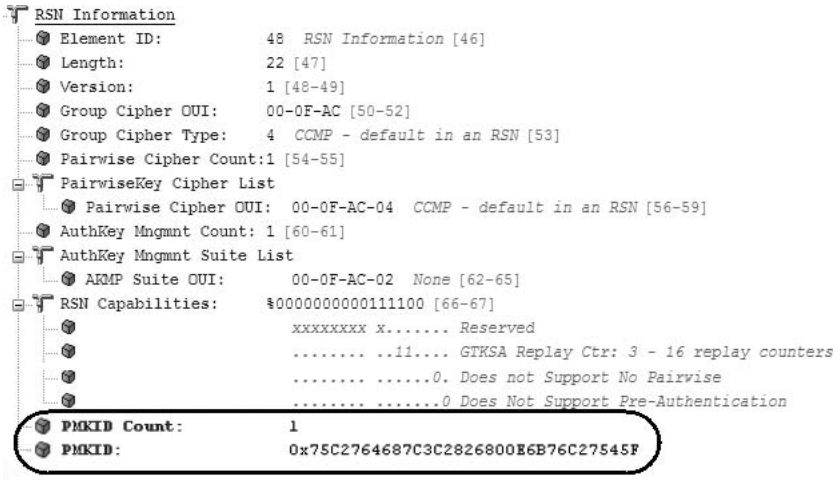
Element ID	Length	Version	Group Cipher Suite	Pairwise Cipher Suite Count	Pairwise Cipher Suite List	AKM Suite Count	AKM Suite List	RSN Capabilities	PMKID Count	PMKID List

A unique identifier is created for each PMKSA that has been established between the authenticator and the supplicant. The *pairwise master key identifier (PMKID)* is a unique identifier that refers to a PMKSA. The PMKID can reference the following types of pairwise master key security associations:

- A PMKSA derived from a PSK for the target AP
- A cached PMKSA from an 802.1X/EAP authentication
- A cached PMKSA that has been obtained through preauthentication with the target AP

We will discuss PMK caching and preauthentication in the next sections of this chapter. The pairwise master key identifier (PMKID) is only found in the RSN information element in association request frames and reassociation request frames that are sent from a client station to an AP. Figure 7.4 shows a protocol analyzer capture of a reassociation request frame's RSN information element and PMKID information. Remember that the PMKID is a unique identifier of an individual PMKSA; however, you will learn that a client station may have established multiple PMKSAs. Therefore, the PMKID Count field specifies the number of PMKIDs in the PMKID List field. The PMKID list contains 0 or more PMKIDs that the STA believes to be valid for a destination AP. The example in Figure 7.4 shows only a single PMKID.

FIGURE 7.4 Pairwise master key identifier (PMKID)



So what exactly comprises a PMKSA? To review, a pairwise master key security association is the result of a successful IEEE 802.1X authentication exchange between a supplicant and authentication server (AS) or from a preshared key (PSK) authentication. A bidirectional security association exists between the authenticator and the supplicant. The components of a PMKSA include the following:

PMK The pairwise master key that was created.

PMKID The unique identifier of the security association.

Authenticator MAC The MAC address of the authenticator.

Lifetime If the key lifetime is not otherwise specified, then the PMK lifetime is infinite.

AKMP The authentication and key management protocol.

Authorization Parameters Any parameters specified by the authentication server or local configuration. This can include parameters such as the STA's authorized SSID.

Although WLAN vendors sometimes use the terms PMK and PMKSA interchangeably, they are two separate entities. The PMK is the key that seeds the 4-Way Handshake, whereas the PMKSA is composed of all the components just listed, including the PMK. You will see that the most important components of the PMKSA are the PMK, the PMKID, and the authenticator's MAC address.

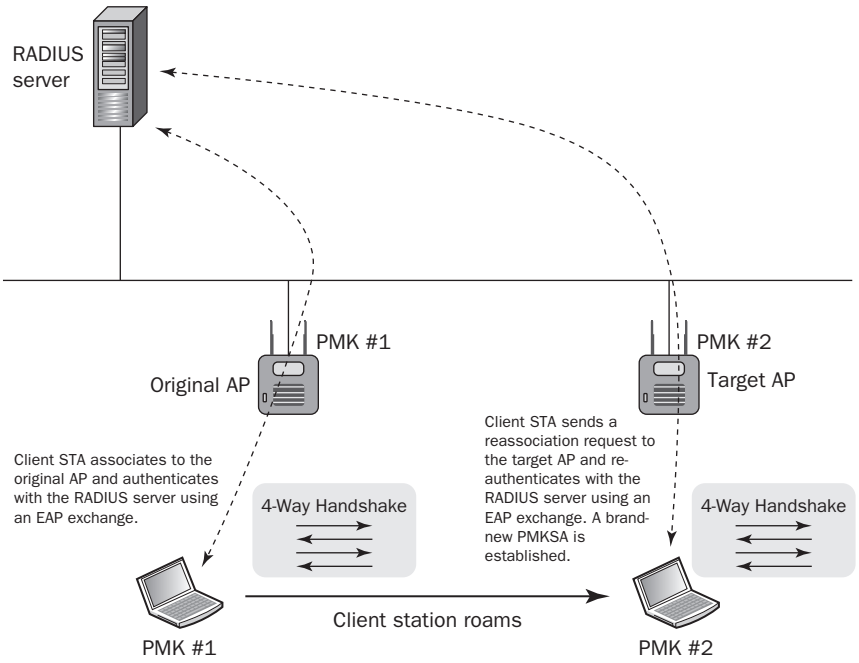
The 802.11-2007 standard states that a client station can establish a new PMKSA during the roaming process with one of four different methods:

- Complete 802.1X/EAP
- PSK authentication
- PMK caching
- Preauthentication

Figure 7.5 depicts the creation of a new PMKSA during reassociation using 802.1X/EAP. PMK #1 is installed on the original AP and the client station. PMK #1 is then used to seed the 4-Way Handshake that is used to create the final keys used for encryption. The client roams to the target AP and reauthenticates with the RADIUS server. The new EAP exchange creates PMK #2 which is installed on the target AP and the client station. PMK #2 is then used to seed the 4-Way Handshake that is used to create the final keys used for encryption in the new BSS.

As you can see, each time the client roams to a new target AP, the client station must reauthenticate with the RADIUS server. Although a new PMKSA is established, the time needed to reauthenticate with the RADIUS server is significant. Many applications will not be affected by the roaming handoff time, but the delay will disrupt the communications of time-sensitive applications such as voice and video. Therefore, the 802.11-2007 standard defines two fast secure roaming mechanisms called preauthentication and PMK caching.

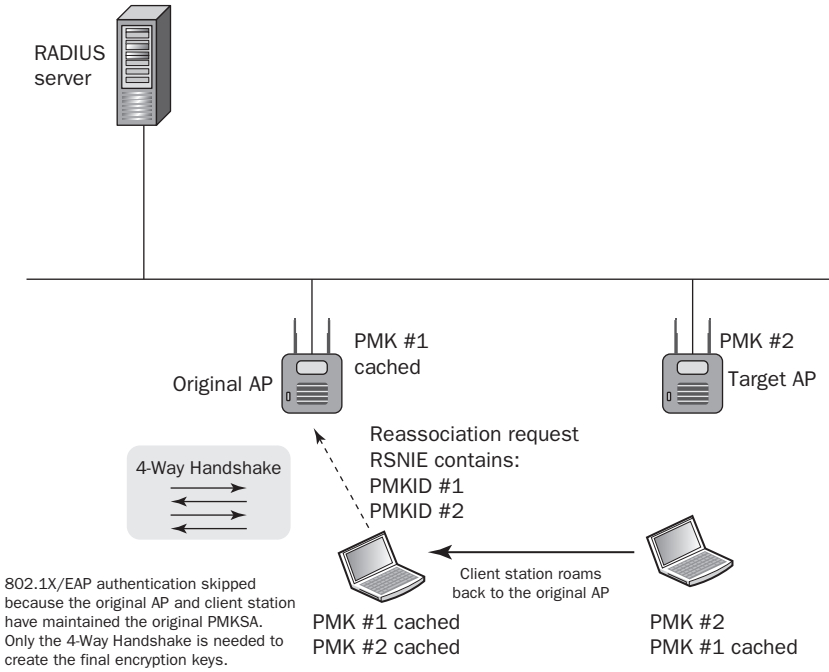
FIGURE 7.5 802.1X/EAP and PMKSA



PMK Caching

PMK caching is a used method by APs and client stations to maintain PMKSAs for a period of time while a client station roams to a target AP and establishes a new PMKSA. An authenticator and a client station can cache multiple PMKs. For example, as shown in Figure 7.6, a client station will associate with an original AP and create an original PMK #1. The client will roam to a target AP and create a new PMK #2; however, the original AP and the client station will both cache PMK #1.

FIGURE 7.6 PMK caching



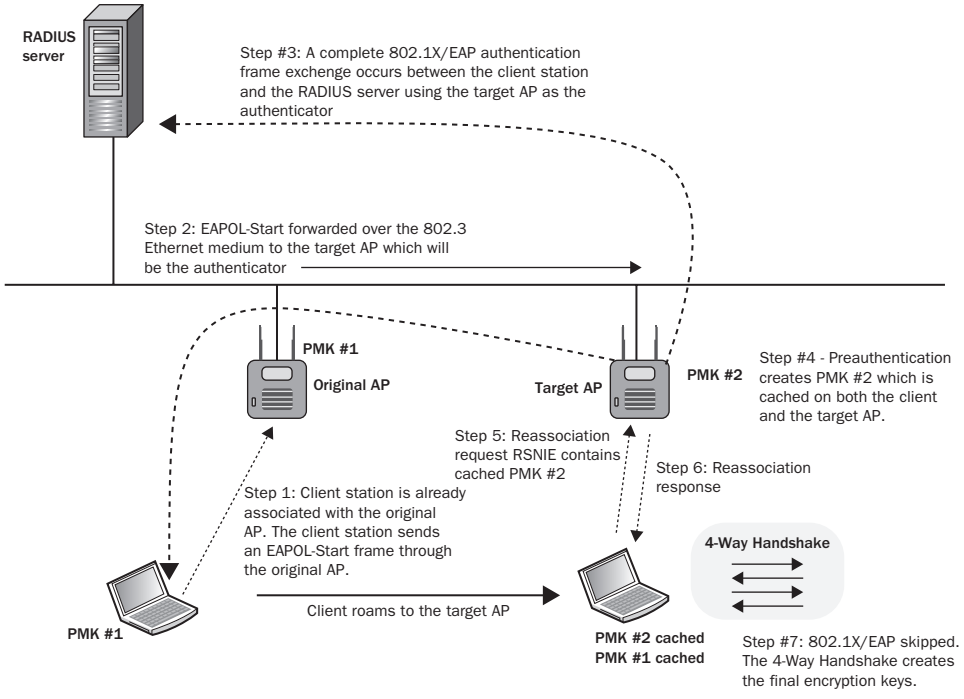
Whenever a client station roams back to the original AP, the client station will send a reassociation request frame that lists multiple PMKIDs in the RSN information element (RSNIE). In other words, the client will be informing the AP about all of the client's cached PMKs. The 802.11-2007 standard states, "An AP whose Authenticator has retained the PMK for one or more of the PMKIDs can skip the IEEE 802.1X authentication and proceed with the 4-Way Handshake." In simpler words, when the client roams back to the original AP, both devices still have the original cached PMK #1 and they can skip the 802.1X/EAP exchange. The client does not need to reauthenticate and create a new PMK because the original PMK still exists. The cached original PMK is then used to seed the 4-Way Handshake.

When a client roams to an AP and the 4-Way Handshake is all that is needed, the roaming handoff is usually below 100 ms, which is fast enough for VoWiFi. Skipping the 802.1X/EAP exchange saves precious time for time-sensitive applications. PMK caching is sometimes called *fast secure roam-back* because the client station is able to roam back to the original AP and skip the 802.1X/EAP exchange. This is great if a client station roams back to an AP where it shares a PMKSA, but how does this speed things up when the client station roams to a new AP? The short answer is there will not be a cached PMK on the target AP unless preauthentication has occurred.

Preauthentication

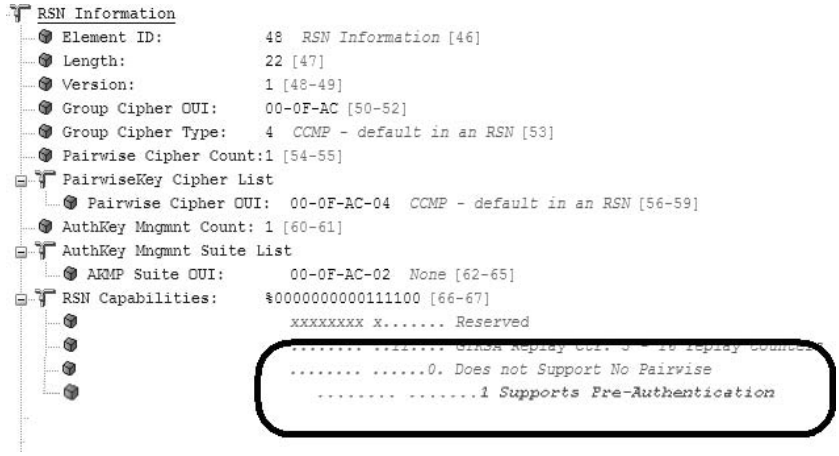
A client station can use *preauthentication* to establish a new PMKSA with an AP prior to roaming to a new target AP. Preauthentication allows a client station to initiate a new 802.1X/EAP exchange with a RADIUS server while associated with the original AP. The purpose of the new 802.1X/EAP authentication is to create a new PMKSA relationship with a new target AP where the client might roam. As Figure 7.7 shows, the client station sends an EAPOL-Start frame through the original AP over the distribution system (DS). An entire 802.1X/EAP exchange occurs between the client station and the RADIUS server; however, the authenticator is the new target AP. Once the client has preauthenticated, a new PMK #2 is created and cached on both the client station and the target AP. If the client station decides to roam to the target AP, the client does not need to reauthenticate and create a new PMK because a precreated cached PMK already exists. The client station roams to the target AP, and the 4-Way Handshake is all that is needed.

FIGURE 7.7 Preauthentication



How do client stations know if they can even learn about APs with which they can preauthenticate? Client stations will discover new APs with both active and passive scanning. As shown in Figure 7.8, an AP can indicate to the client station that the AP is capable of preauthentication in the RSN information element found sent in the AP's probe response or beacon frames.

FIGURE 7.8 Preauthentication-enabled AP



Preauthentication was intended for use with autonomous APs although it can be used with WLAN controller systems as well. It should be noted that preauthentication does not scale very well because it requires all APs to create PMKSAs with all clients that might potentially roam to each AP. Every single client station would need to preauthenticate with every single AP in advance. Preauthentication would therefore place a tremendous load on the backend RADIUS server. PMK caching and preauthentication are simply not very scalable solutions, and therefore the 802.11r task group was formed to define more scalable fast secure transition methods between basic service sets. However, most WLAN vendors did not want to wait for the ratification of the 802.11r-208 amendment, so they implemented a preview of 802.1r mechanisms called opportunistic key caching.

Opportunistic Key Caching (OKC)

So far we have only been discussing roaming as it applies to legacy autonomous APs. WLAN architecture has progressed over the years, and most WLAN vendors now offer a more centralized WLAN controller solution with controller-based APs. Because PMK

caching and preauthentication do not scale well, the majority of the WLAN controller vendors offer a fast secure roaming solution that is an enhancement of PMK caching called *opportunistic key caching (OKC)*. It should be noted that opportunistic key caching is an FSR technique not defined by the 802.11-2007 standard. OKC allows for PMK caching between multiple APs that are under some sort of administrative control. A WLAN controller environment that centrally manages controller-based APs is the perfect environment for opportunistic key caching.

Unlike preauthentication, OKC does not mandate how a PMK arrives at the target AP. OKC instead allows a client station the opportunity to take advantage of a single cached PMK shared among multiple access points.

To understand OKC, let's first discuss the formula for a pairwise master key identifier (PMKID). The 802.11-2007 standard defines a PMK identifier as follows:

PMKID = HMAC-SHA1-128(PMK, "PMK Name" || AA || SPA)

The AA is the authenticator's MAC address, and the SPA is the supplicant's MAC address. This formula shows that a hash function combines the PMK with the access point and client station MAC addresses to create the PMKID.

What Is HMAC?

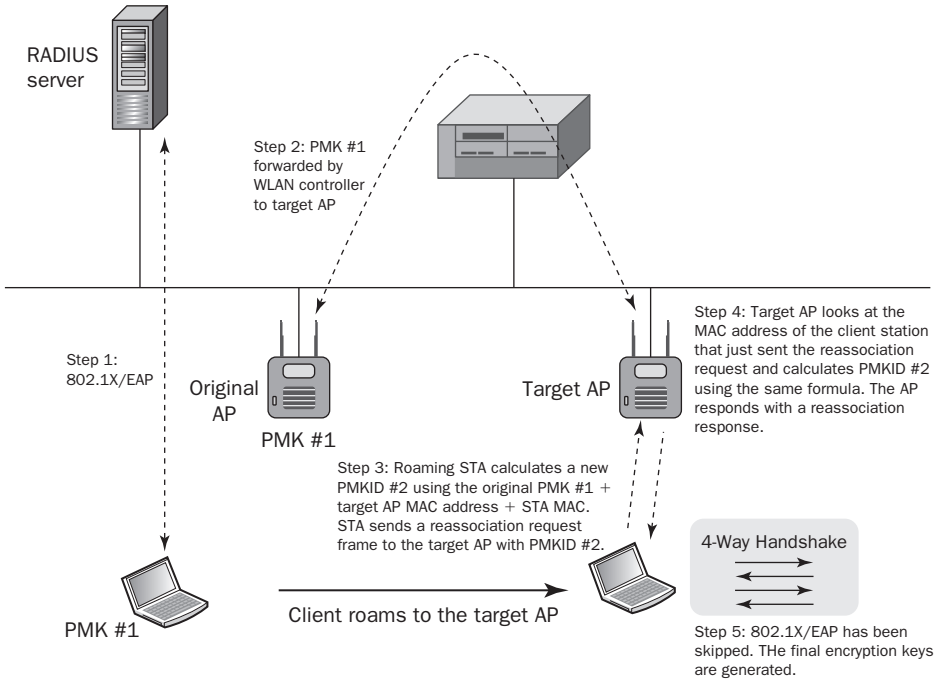
Keyed-Hash Message Authentication Code (HMAC) is a mechanism for message authentication using cryptographic hash functions. HMAC can be used with any iterative cryptographic hash function, such as SHA-1, in combination with a secret shared key. HMAC is defined by IETF RFC 2104, "HMAC: Keyed-Hashing for Message Authentication."

As you can see in Figure 7.9, opportunistic key caching takes advantage of the PMKID formula. A WLAN controller can be used to forward an original PMK and PMKID to multiple access points. Remember that the APs are managed by the WLAN controller and the client traffic is tunneled from the APs to the centralized WLAN controller. Refer to Figure 7.9 when reviewing these steps.

1. The client station uses full 802.1X/EAP authentication and an original PMK #1 and PMKID #1 are created for use by the original AP and the client station. The original AP and the client station perform a 4-Way Handshake.
2. Although, PMK #1 was initially created for the original AP, it is cached on the WLAN controller. The WLAN controller forwards PMK #1 to the target access point.

3. The client station calculates a new PMKID #2 using the original PMK #1 + the target AP MAC address + the client MAC. The client sends a reassociation request frame to the target AP with PMKID #2 in the RSN information element.
4. The target AP looks at the MAC address of the client station that just sent the reassociation request and calculates PMKID #2 using the same formula.
5. Because the PMKID #2 found in the reassociation request frame matches the PMKID #2 calculated by the target AP, reauthentication is not needed. The AP and the client station are still using the original PMK to seed to 4-Way Handshake, however, they are both in possession of the newly calculated PMKID #2, which will allow for a unique security association between the two devices. The AP sends a reassociation response frame and then the 4-Way Handshake is then used to create the final encryption keys shared between the target AP and the client station.

FIGURE 7.9 Opportunistic PMK caching



OKC effectively eliminates the need for client preauthentication, and therefore a more scalable solution is provided. OKC offers several advantages over preauthentication. OKC only requires one initial 802.1X/EAP exchange between the client and the authentication

server. Therefore, OKC reduces the load that is placed on the RADIUS server. Because only a single 802.1X/EAP exchange occurs, only one original PMK is created. The OKC process uses the client station's original PMK as seeding material for all the controller-based APs. The WLAN controller is the authenticator in an 802.1X/EAP solution, and therefore the PMK is cached back on the WLAN controller. How the cached PMK is distributed between the WLAN controller and the controller-based APs is up to the WLAN vendor. OKC will fail if the target AP does not have a newly calculated PMKID that matches the client station's newly calculated PMKID that is sent in a reassociation request frame. In that case, the client station would initiate an 802.1X/EAP exchange and the whole process would start over.

Windows WZC supplicant Registry values that control preauthentication and PMK caching are located at `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EAPOL\Parameters\General\Global`. More information about the Registry values can be found in Appendix A of this book.

The example given in Figure 7.9 depicts OKC with a single WLAN controller. This entire key management process becomes more complex if a client station was to roam to a controller-based AP that tunnels back to a different WLAN controller. Therefore, intercontroller handoff protocols are entirely proprietary. Some WLAN vendors may not support OKC between controllers. In that case, the client station would initiate an 802.1X/EAP exchange and the whole process would start over.

Real World Scenario

How Widely Is Opportunistic Key Caching (OKC) Supported?

Over the last several years, support for OKC has gained wide acceptance. Effectively, OKC is a preview of mechanisms defined by the 802.11r-2008 amendment. Most WLAN controller and infrastructure vendors support OKC. The biggest problem has been client-side support for OKC, which was lacking in the past. The first supplicants to support OKC were the Microsoft Wireless Zero Configuration (WZC) supplicant and Juniper Networks' Odyssey Access Client (OAC). Luckily, more enterprise-grade supplicant solutions have begun to support OKC including some VoWiFi phone manufacturers. For example, Polycom's SpectraLink 8020/8030 VoWiFi phones now support OKC with PEAPv0 (EAP-MSCHAPv2) and EAP-FAST. Client-side support for OKC and 802.11r-2008 mechanisms will grow with the advent of the Wi-Fi Alliance's Voice Enterprise certification.

Proprietary FSR

WLAN vendor Cisco Systems has long offered a proprietary version of fast-securing roaming called Cisco Centralized Key Management (CCKM). Cisco demonstrated market leadership with CCKM; however, CCKM will only work within a Cisco WLAN infrastructure. Now that FSR solutions are becoming standardized, CCKM will likely take a backseat much like the ISL Ethernet switch protocol did with the introduction of IEEE Std. 802.1Q.

CCKM falls within Cisco's licensed CCX program that other vendors may license. The current implementation of CCKM requires Cisco-compatible hardware and works with EAP-LEAP, EAP-FAST, PEAPv1 (EAP-GTC), PEAPv0 (EAP-MSCHAPv2), and EAP-TLS.

CCKM uses a Cisco access point or controller to cache security credentials and effectively takes the place of the RADIUS server when the client stations authenticate. Like all FSR solutions, CCKM shortens the roaming handoff delay.

You will not be tested on CCKM or any other vendor proprietary technologies mentioned in this book. The CWSP exam is a vendor-neutral exam.

Fast BSS Transition (FT)

The recently ratified 802.11r-2008 amendment is known as the *fast basic service set transition (FT)* amendment. Think of the term fast BSS transition as the technical name for standardized fast secure roaming. The main difference between OKC and FT is that the 802.11r-2008 amendment fully defines the key hierarchy used when creating cached keys.

As we have previously stated, OKC key management is a preview of FT, which is also designed for a method of centralized key management. 802.11r mechanisms can be used in an autonomous AP environment; however, a WLAN controller solution with controller-based APs is best suited for an FT solution. Therefore, we will discuss 802.11r within the context of a WLAN controller architecture. 802.11r mechanisms operate within a mobility domain. A *mobility domain* is set of basic service sets (BSSs), within the same extended service set (ESS), that support fast BSS transitions between themselves. In simpler words, a mobility domain is a group of APs that belong to the same ESS where client stations can roam in a fast and secure manner. Some WLAN vendors even refer to their WLAN controllers as the *mobility domain controller (MDC)*. The first time a client station enters a mobility domain, the client will associate with an AP and perform an initial 802.1X authentication. From that point forward, as the client station roams between APs, the

client will be using FT BSS transitions. You will learn later in this chapter that an FT BSS transition can be over-the-air or over-the-DS.

As you learned in Chapter 4, "Enterprise 802.11 Layer 2 Authentication Methods," an 802.1X/EAP exchange creates a *master session key (MSK)* that is used to create a pairwise master key (PMK) for non-FT roaming. FT also uses the 802.1X/EAP exchange to create the master session key, which seeds a centralized, but much more complex, key management solution. After the supplicant and the RADIUS server exchange credentials, the PMK is created from the master session key and sent to the authenticator. The authenticator is the WLAN controller.

802.11r mechanisms introduce multiple layers of PMKs that are cached in different devices. The 802.11r amendment also assigns different roles to different devices. As shown in Table 7.1, each device is assigned a *key holder* role to manage one or more of the multiple keys used in the FT key hierarchy. For now, let's just mention which device is which key holder.

TABLE 7.1 Key holders

Device	Key Holder Role
WLAN controller	Pairwise master key (PMK) R0 key holder (R0KH)
Access point	Pairwise master key (PMK) R1 key holder (R1KH)
Client station	Pairwise master key (PMK) S0 key holder (S0KH)
Client station	Pairwise master key (PMK) S1 key holder (S1KH)

The 802.11r amendment defines a three-level key hierarchy:

Pairwise Master Key R0 (PMK-R0) The first-level key of the FT key hierarchy. This key is derived from the master session key (MSK).

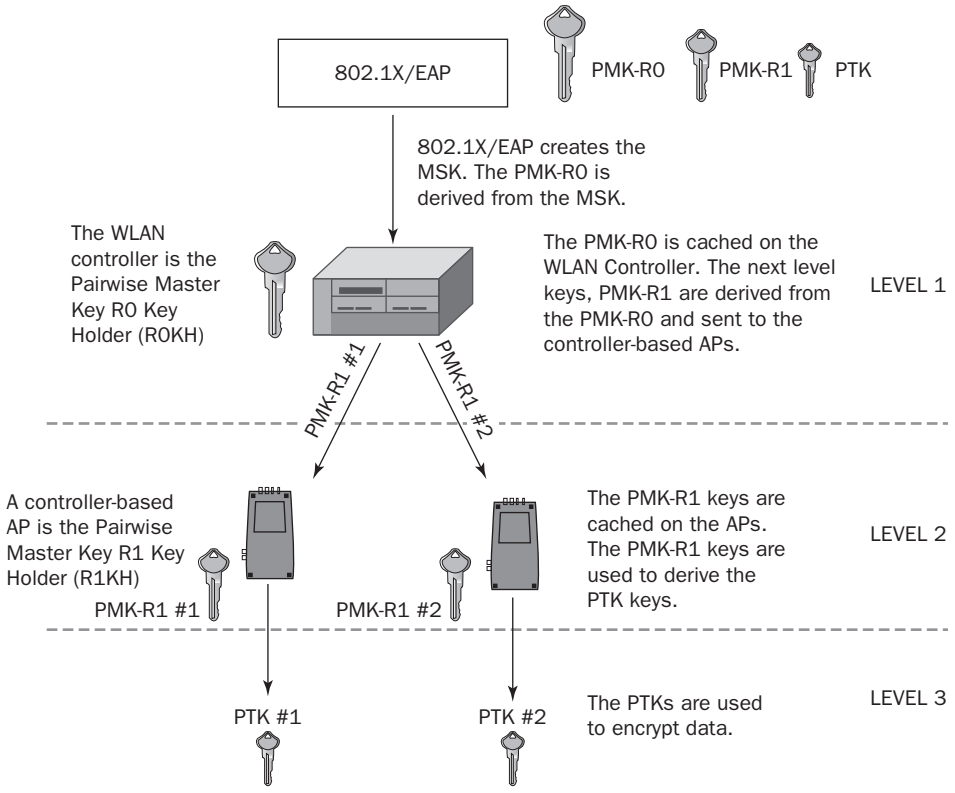
Pairwise Master Key R1 (PMK-R1) The second-level key of the FT key hierarchy.

Pairwise Transient Key (PTK) The third-level key of the FT key hierarchy. The PTK is the final key used to encrypt 802.11 data frames.

As shown in Figure 7.10, the various levels of FT keys are derived and stored in different WLAN devices. 802.1X/EAP creates the master session key (MSK). The MSK is used to create the first-level master key, called a PMK-R0. The PMK-R0 is cached on the WLAN

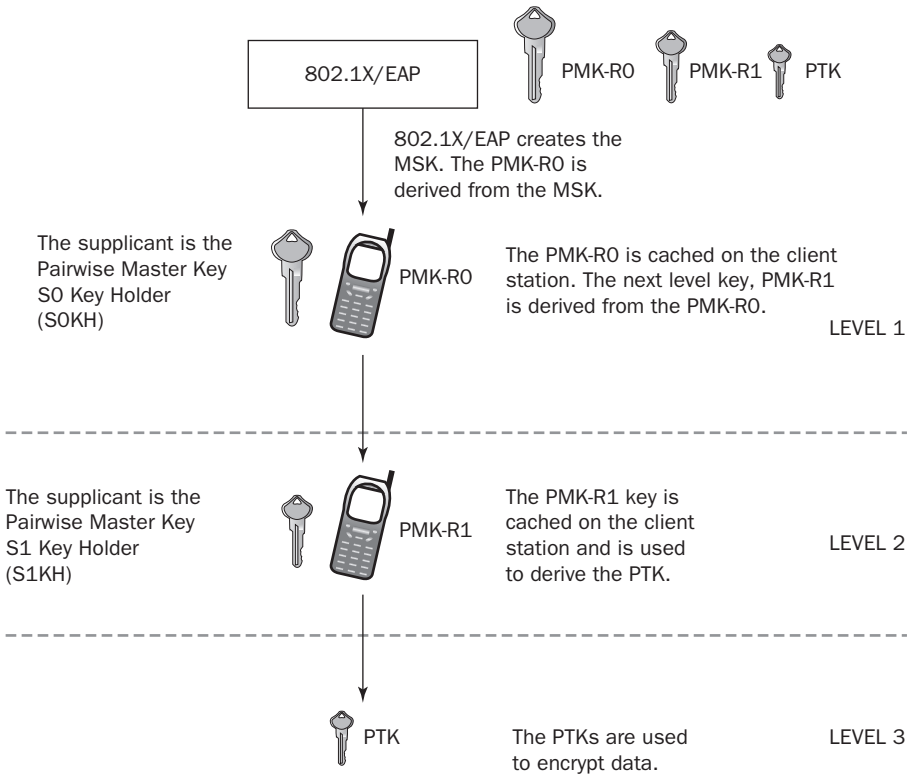
controller. The WLAN controller is the key holder for the first-level key. The second-level key PMK-R1 is derived from the PMK-R0 and sent from the WLAN controller to the controller-based APs. The PMK-R1 keys are cached on the APs. The access points are the key holders for the PMK-R1 keys. The PMK-R1 keys are used to derive the PTKs, which are used to encrypt data.

FIGURE 7.10 FT Key hierarchy—WLAN controller infrastructure



As shown in Figure 7.11, the various levels of FT keys are also derived and stored on the client station. 802.1X/EAP creates the master session key (MSK). The MSK is used to create the first-level master key, called a PMK-R0. The PMK-R0 is cached on the supplicant, which is the client station. The client station is the key holder for the first-level key. The PMK-R0 is cached on the client station. The client station derives the second-level key, PMK-R1, from the PMK-R0. The PMK-R1 key is cached on the client station. The supplicants are the key holders for the PMK-R1 keys. The PMK-R1 keys are used to derive the PTKs, which are used to encrypt data.

FIGURE 7.11 FT key hierarchy—supplicant



To summarize the order of the keys:

MSK > PMK-R0 > PMK-R1 > PTK

It should be noted that the 802.11r-2008 amendment does not specify how the PMK-R1 keys are sent from the WLAN controller to the controller-based APs. If multiple WLAN controllers are used, this becomes even more complex. There is no real definition of how keys should be exchanged between controllers; therefore, intercontroller handoff protocols are entirely proprietary. This also means that it remains highly doubtful that distribution of these keys between WLAN infrastructure devices from different WLAN vendors will be effective.

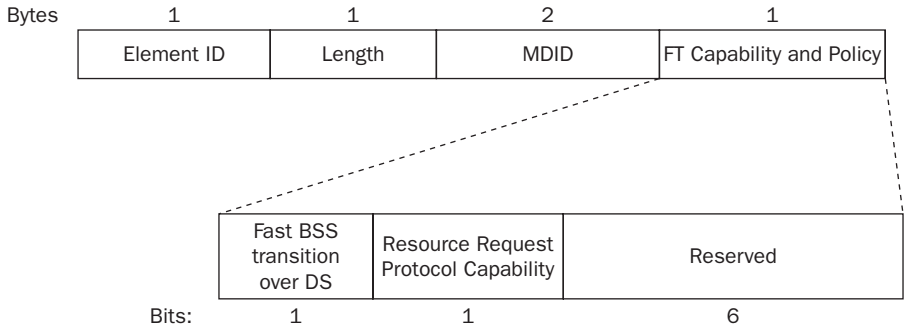
Most WLAN vendors encrypt/decrypt client traffic at the edge of the network using the access points. However, some WLAN vendors perform encryption at the controller level instead of the AP level. End-to-end encryption provides data privacy between the client at the access layer and the WLAN controller that is typically deployed at the core. In that scenario, the WLAN controller functions as both the pairwise master key R0 holder (R0KH) and the pairwise master key R1 holder (R1KH).

Information Elements

To achieve successful fast secure roaming, FT mechanisms still require the use of the RSN information element to indicate the specific authentication key management (AKM) suites and pairwise cipher suites that are being used between the AP and the client station. The 802.11-r-2008 amendment also adds four new information elements. However, we are going to focus on just two of them.

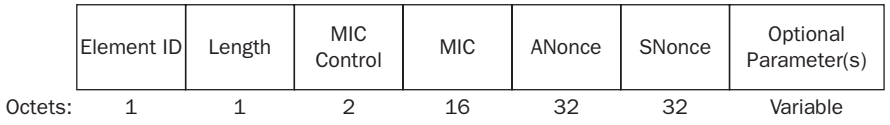
The *mobility domain information element (MDIE)* is used to indicate the existence of a mobility domain as well as the method of fast BSS transition. As shown in Figure 7.12, the *mobility domain identifier (MDID)* field is the unique identifier of the group of APs that constitute a mobility domain. The FT capability and policy field is used to indicate whether over-the-air or over-the-DS fast BSS transition is to be performed. We will discuss the difference between over-the-air and over-the-DS fast BSS transition later in this chapter.

FIGURE 7.12 Mobility domain information element



The *fast BSS transition information element (FTIE)* includes information needed to perform the FT authentication sequence during a fast BSS transition. As shown in Figure 7.13, some of the fields look very similar to the information used during a typical 4-Way Handshake exchange. In the next section, you will see how this information is used in a similar manner during the various FT processes.

FIGURE 7.13 Fast BSS transition information element

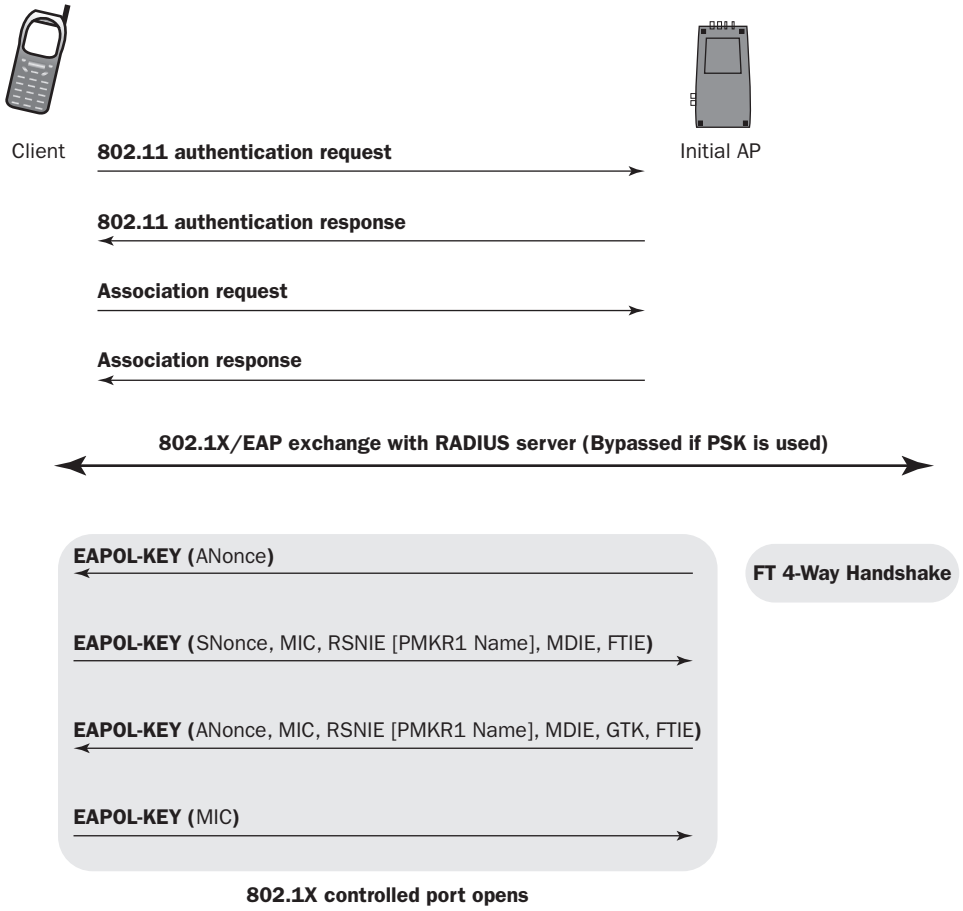


FT Initial Mobility Domain Association

The *FT initial mobility domain association* is the first association in the mobility domain. As shown in Figure 7.14, the client station first exchanges the standard 802.11 Open System authentication request/response frames with the first AP. The client station and AP

then use the MDIE and FTIE information in the association request/response frames to indicate future use of the FT procedures. An original 802.1X/EAP exchange between the client station and the RADIUS server must then occur so seeding material is established for a *FT 4-Way Handshake* that only occurs during the first association. The PTK and GTK encryption keys are created during the FT 4-Way Handshake and the 802.1X controlled port is unblocked. The original 802.1X/EAP exchange also creates the master session key (MSK) that is used for the FT key hierarchy. As you can see, the FT initial mobility domain association is not much different than any initial association used by pre-802.11-r clients. The main difference is that extra information, such as the MDIE and FTIE, is communicated during an FT initial mobility domain association.

FIGURE 7.14 FT initial mobility domain association



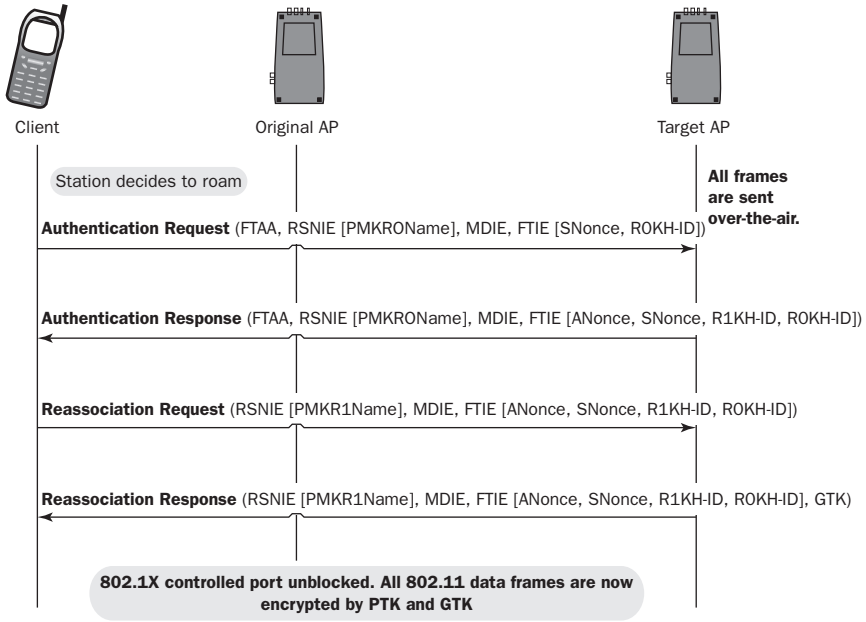
After the initial association, two new methods are defined for a client station to roam from the original AP to a target AP. We will now discuss these two methods of fast BSS transition.

Over-the-Air Fast BSS Transition

Let's consider all the frames that need to be exchanged between a client station and an AP. First, a client has to exchange Open System authentication frames and association frames, as was shown in Figure 7.14. This is a total of four frames, not including the ACKs. Next, a successful 802.1X/EAP exchange between the supplicant and the RADIUS server is needed. The 802.1X/EAP exchange requires many frames. Finally, a 4-Way Handshake exchange is needed between the AP and the client station to create the final dynamic encryption keys. We already know that the purpose of FT and other fast secure roaming mechanisms is to eliminate the need for a new 802.1X/EAP frame exchange every time a client roams. However, the initial four frames of Open System authentication and reassociation are still needed as well as the four frames used during the 4-Way Handshake.

The FT process defines a more efficient method that effectively combines the initial Open System authentication and reassociation frames with the 4-Way Handshake frames. In other words, four less frames are needed when a client roams, thus speeding up the roaming process. As shown in Figure 7.15, an FT protocol frame exchange is used to initiate the roaming exchange and create dynamic encryption keys. Note that the authentication request/response frames and reassociation request/response frames carry an FT authentication algorithm (FTAA) along with nonces and other information needed to create the final dynamic keys. The process shown in Figure 7.15 is known as *over-the-air fast BSS transition*. The client station communicates directly with the target AP using standard 802.11 authentication with the FT authentication algorithm. The PMK-R1 key is the seeding material for the over-the-air fast BSS transition process that creates the final pairwise transient key (PTK).

FIGURE 7.15 Over-the-air fast BSS transition



Over-the-DS Fast BSS Transition

An alternative to the FT method is *over-the-DS fast BSS transition*, which requires the use of *FT Action frames* to complete the PTK creation process. The over-the-DS process uses the FT Action frames over the wired 802.3 infrastructure. As shown in Figure 7.16, the client station sends an FT Action Request frame to the original AP. The FT Action Request frame is forwarded over the distribution system (DS), which is the wired infrastructure. The target AP responds back to the client station over the DS with an FT Action Response frame. The reassociation request and response frames are then sent from the client station to the target AP over the air. The PMK-R1 key is the seeding material for the over-the-DS fast BSS transition exchange that creates the final pairwise transient key (PTK).

FIGURE 7.16 Over-the-DS fast BSS transition

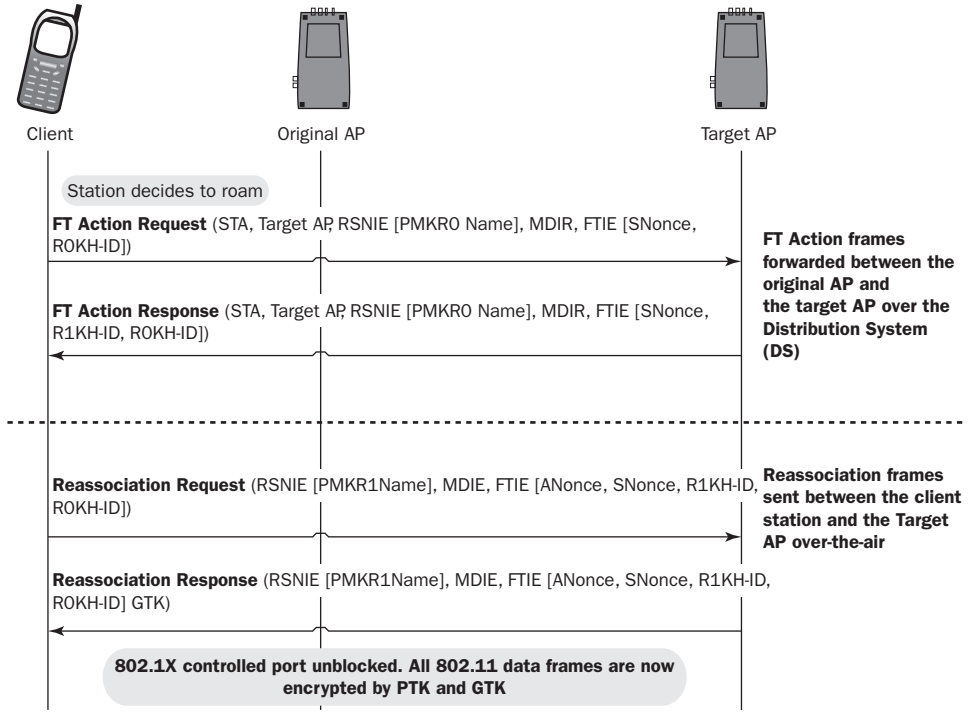
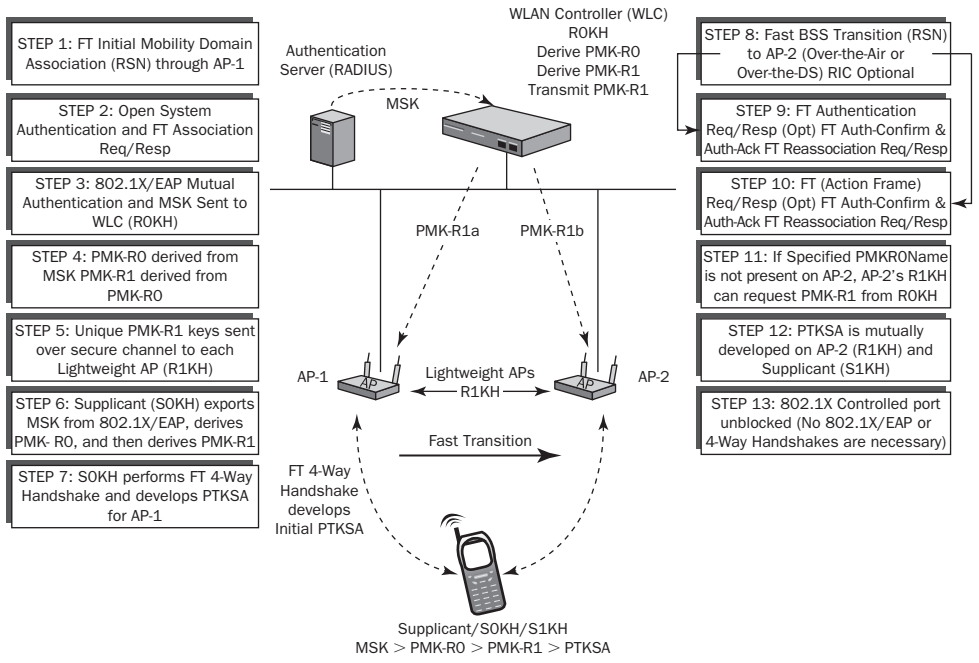


Figure 7.17 shows the multiple steps of the complex fast BSS transition process that has been discussed in this chapter. The process begins with an initial mobility domain association and finally ends with creation of the pairwise transient keys needed for encryption and decryption.

FIGURE 7.17 802.11r fast BSS transition summary



It remains to be seen how many of these FT key mechanisms find their way into WLAN enterprise solutions. Keep in mind that OKC is a preview of many of these FT methods and that OKC is already widely supported. Ultimately, the Wi-Fi Alliance's Voice Enterprise certification will be the main driving force behind any FT mechanisms that are defined by the 802.11r-2008 amendment.

Included on the CD of this book is a white paper titled "Robust Security Network (RSN) fast BSS transition (FT)" authored by Devin Akin, the Chief Wi-Fi Architect of Aerohive Networks. The technical editor of the paper is David Coleman, one of the coauthors of this book. This white paper covers in greater detail all the FSR methods discussed in this chapter. Significant attention is given to the FT architecture. This white paper is recommended extra reading for the CWSP exam.

802.11k

The recently ratified 802.11k-2008 amendment, in conjunction with the recently ratified 802.11r-2008 amendment, together have the potential to improve roaming performance within secure 802.11 WLANs. 802.11k defines *radio resource measurement (RRM)* mechanisms that enable 802.11k-compliant radios to better understand the RF environment in which they exist. If an 802.11 radio is not transmitting, it can evaluate the RF environment and radio link performance while the radio is listening. Radio resource measurements can be made by an AP or a client station. The measurements can be taken locally and can be requested and obtained from another station. RRM data can be made available to upper protocol layers, where it can be used for a range of applications, such as VoIP.

Measurements such as the channel load request/report and the neighbor request/report may be used to collect pre-handoff information, which can drastically speed up handoffs between access points. The whole purpose behind RRM is that client stations and/or APs can make intelligent decisions about the most effective way to utilize the available spectrum, power, and bandwidth for desired WLAN communications.

As defined by 802.11k-2008 amendment, an access point or WLAN controller will request a station to listen for neighboring access points on other channels and gather information. The current AP or WLAN controller will then process that information and generate a *neighbor report* detailing available access points from best to worst. Before a station roams, it may request the neighbor report from the current AP or controller and then decide whether to roam to one of the access points on the neighbor report.

As you learned earlier in this chapter, clients make the roaming decision as opposed to the APs or WLAN controllers. Clients will still look to roam to APs using active and passive scanning, and they will still evaluate locally the RF environment based on RSSI metrics. Client stations will still make the roaming decision; however, the neighbor reports will provide the client stations with additional input so the client stations can make better roaming decisions.

The 802.11k amendment is not part of the 802.11-2007 standard. However, it was ratified in June 2008 and is published as IEEE 802.11k-2008.

Voice Personal and Voice Enterprise

When will 802.11k and 802.11r mechanisms find their way to the client side? The Wi-Fi Alliance is expected to debut a new vendor-interoperability certification called *Voice Enterprise* in 2010. Voice Enterprise will define enhanced support for voice applications in

the enterprise environment. Many aspects of the 802.11r-2008 and 802.11k amendments will probably be tested in Voice Enterprise. Although subject to change, some of the aspects of the Voice Enterprise certification include the following:

Prioritization Support for WMM QoS mechanisms will be mandatory.

Mobility/Roaming A VoWiFi client should be able to maintain a low-latency call while roaming between APs in a secure manner. The proposed AP-handoff time is 50 ms, although 100 ms may be considered acceptable.

Voice Quality Metrics that may be tested include jitter, latency, and packet loss.

Battery Life Support for power management methods such as WMM-PS will be included.

Security WPA2-Enterprise security will be mandatory.

Bandwidth Management A method of call admission control will most likely be defined. The forthcoming WMM-AC certification should define call admission control so traffic does not affect the behavior of active calls.

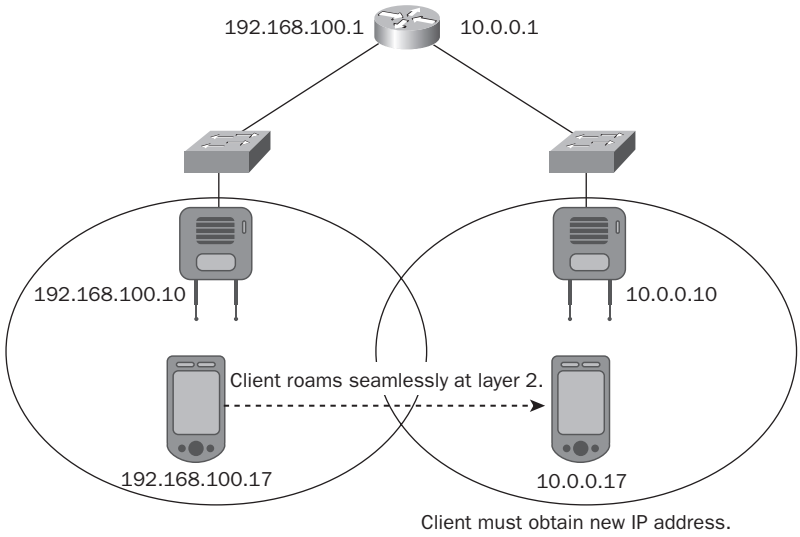
Protocol Adherence and Performance Metrics Adherence guarantees vendor interoperability and performance metrics ensures voice quality.

On June 30, 2008, the Wi-Fi Alliance announced the Wi-Fi CERTIFIED Voice Personal certification program. The Voice Personal certification targets interoperability and performance metrics for VoWiFi in small office/home office (SOHO) environments. Many of the same metrics such as jitter, packet loss, and latency are also tested in Voice Personal. This certification is not intended to validate enterprise solutions and is focused primarily on the home Wi-Fi market. A certified Voice Personal home Wi-Fi router might be capable of handling three active VoWiFi calls.

Layer 3 Roaming

One major consideration when designing a WLAN is what happens when client stations roam across Layer 3 boundaries. In Figure 7.18, the client station is roaming between two access points. The roam is seamless at Layer 2, but a router sits between the two access points, and each access point resides in a separate subnet. In other words, the client station will lose Layer 3 connectivity and must acquire a new IP address. Any connection-oriented applications that are running when the client reestablishes Layer 3 connectivity will have to be restarted. For example, a VoIP phone conversation would disconnect in this scenario, and the call would have to be reestablished.

FIGURE 7.18 Layer 3 roaming boundaries

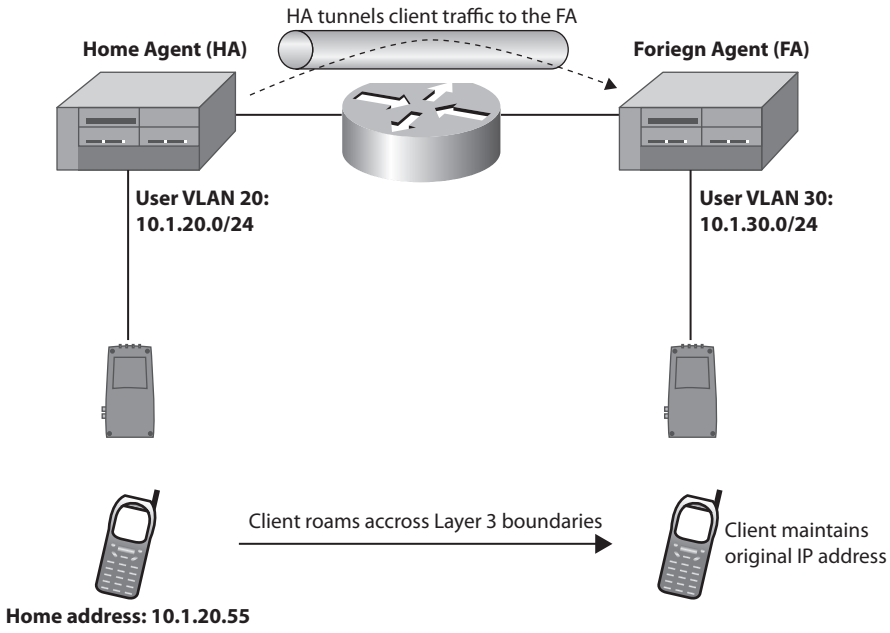


When designing a WLAN, the preferred method is to have overlapping Wi-Fi cells that exist in only the same Layer 3 domains through the use of VLANs. However, because 802.11 wireless networks are usually integrated into preexisting wired topologies, crossing Layer 3 boundaries is often a necessity, especially in large deployments. The only way to maintain upper-layer communications when crossing Layer 3 subnets is to provide either a Mobile IP solution or a proprietary *Layer 3 roaming* solution. *Mobile IP* is an Internet Engineering Task Force (IETF) standard protocol that allows mobile device users to move from one Layer 3 network to another while maintaining their original IP address. Mobile IP is defined in IETF request for comment (RFC) 3344. Mobile IP and proprietary solutions both use some type of tunneling method and IP header encapsulation to allow packets to traverse between separate Layer 3 domains with the goal of maintaining upper-layer communications. It is beyond the scope of this book to fully explain either the standards-based Mobile IP or proprietary Layer 3 roaming solutions. However, most WLAN controllers now support some type of Layer 3 roaming solution as shown in Figure 7.19.

A mobile client receives an IP address also known as a *home address* on a home network. The mobile client must register its home address with a device called a *home agent (HA)*. The original WLAN controller on the client's home network serves as the home agent. The home agent is a single point of contact for a client when it roams across Layer 3 boundaries. The HA shares client MAC/IP database information in a table called a *home agent table (HAT)* with another device called the *foreign agent (FA)*. The foreign agent is another WLAN controller that handles all Mobile IP communications with the home agent on behalf of the client. The foreign agents IP address is known as the *care-of address*. When the client roams across Layer 3 boundaries, the client is roaming to a foreign network where the FA resides. The FA uses the HAT tables to locate the HA of the

mobile client station. The FA contacts the HA and sets up a Mobile IP tunnel. Any traffic that is sent to the client's home address is intercepted by the HA and sent through the Mobile IP tunnel to the FA. The FA then delivers the tunneled traffic to the client and the client is able to maintain connectivity using the original home address.

FIGURE 7.19 Mobile IP



Although maintaining upper-layer connectivity is possible with these Layer 3 roaming solutions, increased latency is often an issue. Additionally, Layer 3 roaming may not be a requirement for your network. Less complex infrastructure often uses a simpler flat Layer 2 design. Even if there are Layer 3 boundaries, your users may not need to roam seamlessly between subnets. Before you go to all the hassle of building a roaming solution, be sure to define your requirements properly.

Troubleshooting

The best way to ensure that seamless roaming will commence is proper design and a thorough site survey. When designing an 802.11 WLAN, most vendors recommend 15 to 25 percent overlap in coverage cells at the lowest desired signal level. The only way to determine whether proper cell overlap is in place is by conducting a coverage analysis site survey. Proper site survey procedures are discussed in detail in the *CWNA: Certified*

Wireless Network Administrator Official Study Guide by author(s) David Coleman and David Westcott (Sybex, 2009).

Changes in the WLAN environment can also cause roaming headaches. RF interference will always affect the performance of a wireless network and can make roaming problematic as well. Very often new construction in a building will affect the coverage of a WLAN and create new dead zones. If the physical environment where the WLAN is deployed changes, the coverage design may have to change as well. It is always a good idea to conduct a coverage survey periodically to monitor changes in coverage patterns.

Troubleshooting roaming by using a protocol analyzer is tricky because the reassociation roaming exchanges occur on multiple channels. To troubleshoot a client roaming between channels 1, 6, and 11, you would need three separate protocol analyzers on three separate laptops that would produce three separate frame captures. CACE Technologies offers a product called AirPcap that is a USB 802.11 radio. As you can see in Figure 7.20, three AirPcap USB radios can be configured to capture frames on channels 1, 6, and 11 simultaneously. All three radios are connected to a USB hub and save the frame captures of all three channels into a single time-stamped capture file. The AirPcap solution allows for multichannel monitoring with a single protocol analyzer.

FIGURE 7.20 AirPcap provides multichannel monitoring and roaming analysis.

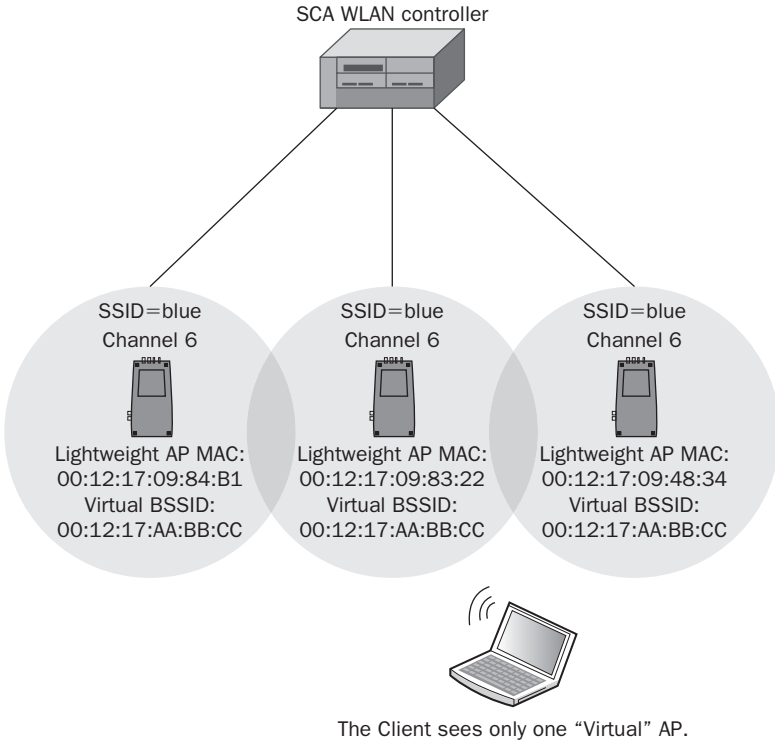
SCA Roaming

At the time of this writing, two vendors, Meru Networks and Extricom, are offering an alternative WLAN channel design solution known as the *single channel architecture (SCA)*. Imagine a WLAN network with multiple access points all transmitting on the same channel and all sharing the same BSSID. A single-channel architecture is exactly what you have just imagined. The client stations see transmissions on only a single channel with one SSID (logical WLAN identifier) and one BSSID (Layer 2 identifier). From the perspective

of the client station, only one access point exists. In this type of WLAN architecture, all access points in the network can be deployed on one channel in 2.4 GHz or 5 GHz frequency bands. Uplink and downlink transmissions are coordinated by a WLAN controller on a single 802.11 channel in such a manner that the effects of co-channel interference are minimized.

Let's first discuss the single BSSID. Single-channel architecture consists of a WLAN controller and multiple lightweight access points. As shown in Figure 7.21, each AP has its own radio card with its own MAC address; however, they all share a *virtual BSSID* that is broadcast from all of the access points.

FIGURE 7.21 Single-channel architecture



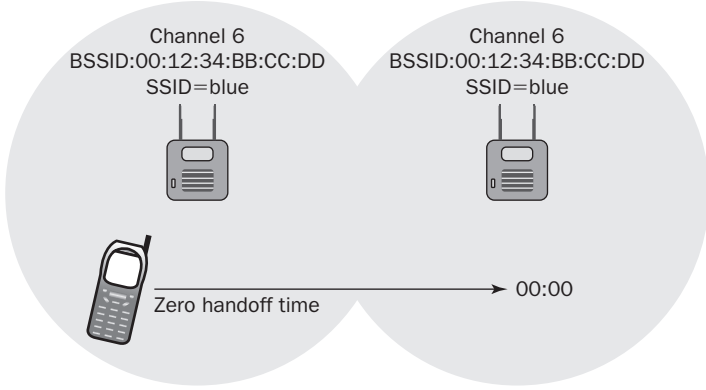
Because the multiple access points advertise only one single virtual MAC address (BSSID), client stations believe they are connected to only a single access point, although they may be roaming across multiple physical APs. In a single-channel architecture (SCA)

system, the clients think they are associated with only one AP, so they never initiate a Layer 2 roaming exchange. In other words, the client stations actually do roam between the physical APs in an SCA environment, but the stations are tricked into thinking they are only associated with one big *virtual AP*.

All of the handoff and management is handled by a central WLAN controller.

As shown in Figure 7.22, the main advantage of an SCA is that clients experience a *zero handoff* time, and the latency issues associated with roaming times are resolved. The virtual AP used by SCA solutions is potentially an excellent marriage for VoWiFi phones and 802.1X/EAP solutions. The virtual BSSID eliminates the need for reauthentication while physically roaming within an SCA and thus a zero handoff time.

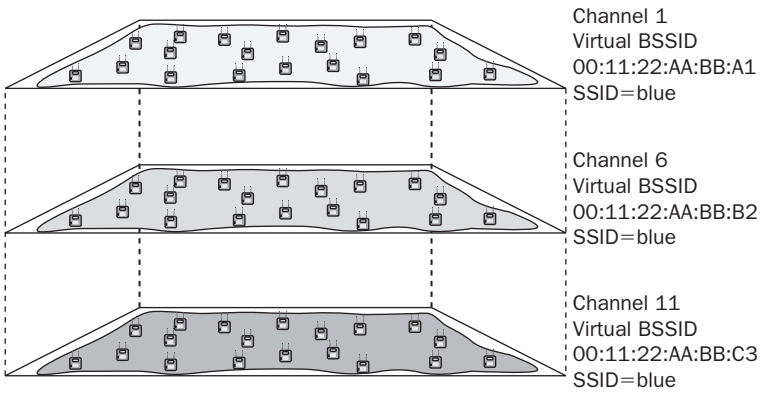
FIGURE 7.22 Zero handoff time



You have learned that client stations make the roaming decision in a typical *multiple-channel architecture (MCA)* environment. However, client stations do not know that they roam in an SCA environment. The clients must still be mobile and transfer Layer 2 communications between physical access points. All the client-roaming mechanisms are now handled back on the WLAN controller, and client-side-roaming decisions have been eliminated.

As you can see in Figure 7.23, in a 2.4 GHz SCA deployment, multiple APs can be co-located by using three channels and three virtual BSSIDs. Co-location design in an SCA is often referred to as *channel stacking*. Each layer of multiple APs on a single channel that use the same virtual BSSID is known as a *channel blanket* or *channel span*.

FIGURE 7.23 2.4 GHz channel stacking—single-channel architecture



In the SCA example shown earlier in Figure 7.23, a client station would see three APs on channels 1, 6, and 11 that had the same logical SSID but three separate virtual BSSIDs. The channel stacks effectively create three virtual APs. A client station might roam between one of the virtual BSSIDs because the client believes there are three separate APs. In this scenario, the clients would initiate a reassociation process when roaming from one virtual BSSID to another. Although the whole point of an SCA architecture is to bypass a complex FSR solution, an FSR solution such as OKC or FT would be needed if there was more than one virtual BSSID.

Exam Essentials

Understand legacy roaming handoff mechanisms. Reassociation is the process clients use to move from one BSS to another. Client roaming thresholds and AP-to-AP handoff communications are proprietary.

Define the operations and limitations of legacy FSR mechanisms. Explain both the PMK caching and preauthentication FSR methods defined by the 802.11-2007 standard.

Explain opportunistic key caching (OKC). Understand how the PMKID is manipulated by OKC to accomplish fast secure roaming.

Explain fast BSS transition (FT). Define all the key hierarchy components and operations defined by the 802.11r-2008 amendment.

Understand the benefits of 802.11k-2008 radio resource measurement (RRM). Describe how RRM enables client stations to make intelligent decisions to improve roaming performance.

Understand the benefits of 802.11k-2008 radio resource measurement (RRM). Describe how RRM enables client stations to make intelligent decisions to improve roaming performance.

Describe single channel architecture (SCA) roaming. Understand how clients roam in an SCA environment using virtual BSSIDs.

Explain the purpose and basics of Mobile IP. Define Mobile IP components and why a Mobile IP solution is needed when clients roam across Layer 3 boundaries.

Key Terms

Before you take the exam, be certain you are familiar with the following terms:

4-Way Handshake

A pairwise master key security association (PMKSA)

BSS transition

care-of address

channel blanket

channel span

channel stacking

distribution system (DS)

distribution system medium (DSM)

fast basic service set transition (FT)

fast secure roam-back

fast secure roaming (FSR)

fast BSS transition (FT)

fast BSS transition information element (FTIE)

foreign agent

FT 4-Way Handshake

home address

home agent

Inter-Access Point Protocol (IAPP)

key holder

Keyed-Hash Message Authentication Code (HMAC)

Layer 3 roaming

master session key (MSK)

Mobile IP

mobility domain

mobility domain controller (MDC)

mobility domain identifier (MDID)

mobility domain information element (MDIE)

multiple channel architecture (MCA)

neighbor report

opportunistic key caching (OKC)

over-the-air fast BSS transition

over-the-DS fast BSS transition

pairwise master key (PMK)

pairwise master key identifier (PMKID)

pairwise master key R0 (PMK-R0)

pairwise master key R1 (PMK-R1)

pairwise transient key (PTK)

pairwise transient key (PTK)

pairwise transient key security association (PTKSA)

PMK caching

preauthentication

radio resource measurement (RRM)

reassociation service

received signal strength indicator (RSSI)

roaming

robust security network association (RSNA)

robust security network information element (RSNIE)

RSN information element

single channel architecture (SCA)

virtual BSSID

Voice Enterprise

Voice Personal

Review Questions

1. What type of solution must be deployed to provide continuous connectivity when a client station roams across Layer 3 boundaries? (Choose all that apply.)
   - **A.** Nomadic roaming solution
   - **B.** Proprietary Layer 3 roaming solution
   - **C.** Seamless roaming solution
   - **D.** Mobile IP solution
   - **E.** Fast secure roaming solution

2. Which pairwise master key security associations (PMKSAs) can be uniquely identified by a PMKID? (Choose all that apply.)
   - **A.** PMKSA derived from a PSK authentication
   - **B.** PMKSA from Open System authentication
   - **C.** Cached PMKSA from an 802.1X/EAP authentication
   - **D.** Cached PMKSA for Mobile IP authentication
   - **E.** Cached PMKSA from preauthentication

3. As defined by the 802.11-2007 standard, which of these methods can be used by a client station to establish a new pairwise master key security association (PMKSA)? (Choose all that apply.)
   - **A.** PSK authentication
   - **B.** Preauthentication
   - **C.** 802.1X/EAP
   - **D.** Postauthentication
   - **E.** PMK caching

4. Which of these methods allows an authenticator and supplicant to skip an entire 802.1X/EAP authentication and proceed with the traditional 4-Way Handshake? (Choose all that apply.)
   - **A.** PMK caching
   - **B.** PTK caching
   - **C.** Opportunistic key caching
   - **D.** fast BSS transition

5. What are some of the variables that an 802.11k-2008–compliant STA can use to initiate reassociation? (Choose all that apply.)
   - **A.** RSSI
   - **B.** Channel load reports
   - **C.** Opportunistic PMK caching

D. Neighbor reports

E. Authentication reports

6. Which of these WLAN design architectures uses a zero handoff time for roaming client stations?

A. MCA

B. OKC

C. Opportunistic PMK caching

D. SCA

E. PMK caching

7. What are some of the components that comprise a PMKID? (Choose all that apply.)

A. Authenticator MAC address

B. Authentication server MAC address

C. PMK

D. MSK

E. Supplicant MAC address

8. Which of these 802.11 management frames contain a PMKID in the RSN information element? (Choose all that apply.)

A. Reassociation request

B. Probe response

C. Reassociation response

D. Beacon

E. Association request

9. Within the three-tier FT key hierarchy defined by 802.11r, which of these keys is cached on a WLAN controller?

A. PMK-R1

B. MSK

C. PTK

D. PMK-R0

E. PMK

10. Within the three-tier FT key hierarchy defined by 802.11r, which of these keys is cached on a controller-based AP?

A. PMK-R1

B. MSK

C. PTK

D. PMK-RO

E. PMK

11. Which of these roaming methods requires the use of FT Action frames?

A. Over-the-air fast BSS transition

B. Over-the-WDS fast BSS transition

C. Over-the-DS fast BSS transition

D. Over-the-WLS fast BSS transition

12. Within the three-tier FT key hierarchy defined by 802.11r, which of these keys is used to encrypt the MSDU payload of an 802.11 data frame?

A. PMK-R1

B. MSK

C. PTK

D. PMK-R0

E. PMK

13. Which of these protocol adherence and performance metrics will most likely be defined by the Wi-Fi Alliance Voice Enterprise certification?

A. Prioritization

B. Mobility

C. Voice quality

D. Battery life

E. Security

F. Access control

G. All of the above

14. Although not defined by the 802.11-2007 standard, which of these methods of fast secure roaming is currently supported by the majority of WLAN vendors?

A. PMK caching

B. Preathentication

C. Opportunistic key caching

D. Over-the-air fast BSS transition

E. Over-the-DS fast BSS transition

15. What aspects of roaming were not defined by the original standard? (Choose all that apply.)

A. Security

B. AP-to-AP handoff

C. PTK

D. RSSI thresholds

E. PMK

16. What is used initially to seed the FT process that is used to create three levels of key hierarchy?

- **A.** PMK-R0
- **B.** PMK-R1
- **C.** PTK
- **D.** MSK
- **E.** PMK

17. Which of these devices serves as a key holder for the PMK-R0 created during a fast BSS transition? (Choose all that apply.)

- **A.** WLAN controller
- **B.** Client stations
- **C.** Controller-based APs
- **D.** RADIUS server
- **E.** Access Layer switch

18. Which of these devices serve as a key holder for the PMK-R1 key created during a fast BSS transition? (Choose all that apply.)

- **A.** WLAN controller
- **B.** Client station
- **C.** Controller-based APs
- **D.** RADIUS server
- **E.** Access Layer switch

19. The ACME Company manufactures two models of WLAN controllers. The standard model uses the controller-based APs to encrypt and decrypt client traffic at the edge of the network. The deluxe model uses end-to-end encryption and the WLAN controller performs encryption/decryption of the client traffic at the core of the network. Which of these statements properly identify the key holder roles? (Choose all that apply.)

- **A.** Standard model: AP is the R0KH
- **B.** Standard model: WLAN controller is the R1KH
- **C.** Deluxe model: WLAN controller is the R0KH
- **D.** Deluxe model: WLAN controller is the R1KH
- **E.** Deluxe model: AP is the R1KH

20. Which key is used to seed both over-the-air and over-the-DS fast BSS transition?

- **A.** MSK
- **B.** PMK-R0
- **C.** PMK-R1
- **D.** PTK
- **E.** GTK

Answers to Review Questions

1. B, D. The only way to maintain upper-layer communications when crossing Layer 3 subnets is to provide either a Mobile IP solution or a proprietary Layer 3 roaming solution.

2. A, C, E. A unique identifier is created for each PMKSA that has been established between the authenticator and the supplicant. The pairwise master key identifier (PMKID) is a unique identifier that refers to a PMKSA. A PMKID can reference PMKSAs derived from a PSK authentication, cached from an 802.1X/EAP authentication, or a PMKSA that has been created through preauthentication with a target AP.

3. A, B, C, E. The 802.11-2007 standard states that a client station can establish a new PMKSA during the roaming process with one of four different methods: PMK caching, preauthentication, complete 802.1X/EAP, and PSK authentication.

4. A, C. The 802.11-2007 standard defines two fast secure roaming mechanisms called preauthentication and PMK caching. Most WLAN vendors currently use an enhanced method of fast secure roaming (FSR) called opportunistic key caching. The 802.11r-2008 amendment defines more complex fast BSS transition (FT) methods of FSR. PMK caching, opportunistic key caching (OKC), and fast BSS transition (FT) all allow for 802.1X/EAP authentication to be skipped when roaming; however, FT does not use the traditional 4-Way Handshake and instead uses either an over-the-air fast BSS transition frame exchange or an over-the-DS fast BSS transition frame exchange.

5. A, C, D. Client stations decide to roam based on proprietary rules determined by the manufacturer of the wireless card, usually defined by received signal strength indicator (RSSI) thresholds. RSSI thresholds usually involve signal strength, noise level, and bit-error rate. 802.11k defines radio resource measurement (RRM) mechanisms that enable 802.11k compliant radios to better understand the RF environment in which they exist. Measurements, such as the channel load request/report and the neighbor request/report, may be used to collect pre-handoff information, which can drastically speed up handoffs between access points.

6. D. The main advantage of a single-channel architecture (SCA) is that clients experience a zero handoff time, and the latency issues associated with roaming times are resolved. Each AP has its own radio card with its own MAC address; however, they all share a virtual BSSID that is broadcast from all the access points. The virtual BSSID eliminates the need for reauthentication while physically roaming within an SCA and thus a zero handoff time.

7. A, C, E. The 802.11-2007 standard defines a PMK identifier with the following formula:

   PMKID = HMAC-SHA1-128(PMK, “PMK Name” || AA || SPA)

   The AA is the authenticator’s MAC address, and the SPA is the supplicant’s MAC address. A hash function combines the PMK with the access point and client station MAC addresses to create the PMKID.

8. A, E. The RSN information element field is found in four different 802.11 management frames: beacon management frames, probe response frames, association request frames, and reassociation request frames. However, the pairwise master key identifier (PMKID) is only found in the RSN information element in association request frames and reassociation request frames that are sent from a client station to an AP. The PMKID is a unique identifier of an individual pairwise master key security association (PMKSA); however, a client station may actually have established multiple PMKSAs and therefore list multiple PMKIDs.

9. D. The 802.11r amendment defines a three-level key hierarchy. The Pairwise Master Key R0 (PMK-R0) is the first-level key of the FT key hierarchy. This key is derived from the master session key (MSK). The PMK-R0 is cached on the WLAN controller.

10. A. The 802.11r amendment defines a three-level key hierarchy. The Pairwise Master Key R1 (PMK-R1) is the second-level key of the fast BSS transition (FT) key hierarchy. The second-level key PMK-R1 is derived from the PMK-R0 and sent to the controller-based APs. The PMK-R1 keys are cached on the APs. The access points are the key holders for the PMK-R1 keys.

11. C. Over-the-DS fast BSS transition requires the use of FT Action frames to complete the PTK creation process. A client stations sends an FT Action Request frame to the associated AP. The FT Action Request frame is forwarded over the distribution system (DS), which is the wired infrastructure. The target AP responds back to the client station over the DS with an FT Action Response frame. The reassociation request and response frames are then sent from the client station to the target AP over-the-air.

12. C. The pairwise transient key (PTK) is the third-level key of the FT key hierarchy. The PTK is the final key used to encrypt 802.11 data frames. The PTK is created during either an over-the-air fast BSS transition frame exchange or over-the-DS fast BSS transition frame exchange. In any 802.11 robust security network (RSN), the PTK is used to encrypt the MSDU payload of an 802.11 unicast data frame.

13. G. Although subject to change, a variety of protocols and metrics will be tested by the Voice Enterprise certification. Support for WMM QoS mechanisms will be mandatory. VoWiFi clients should be able to maintain a low-latency call while roaming between APs in a secure manner. The proposed AP-handoff time is 50 ms although 100 ms may be considered acceptable. Voice quality metrics that may be tested include jitter, latency, and packet loss. Battery life will be protected with support for power management methods such as WMM-PS. WPA2-Enterprise security will be mandatory. A method of call admission control will most likely also be defined. The forthcoming WMM-AC certification should define call admission control so traffic does not affect the behavior of active calls. Many aspects of the 802.11r-2008 and 802.11k amendments will probably be tested in Voice Enterprise.

14. C. Fast BSS transition mechanisms are defined by the 802.11r amendment; however, they are not yet widely and fully supported. PMK caching and preauthentication are supported by most WLAN vendors, and they are both defined by the 802.11-2007 standard. Because PMK caching does not scale well, the majority of the WLAN controller vendors offer a fast secure roaming solution that is an enhancement of PMK caching called opportunistic

key caching (OKC). Note that OKC is an FSR technique not defined by the 802.11-2007 standard. OKC allows for PMK caching between multiple APs that are under some sort of administrative control. A WLAN controller environment that centrally manages controller-based APs is the perfect environment for opportunistic key caching. Unlike preauthentication, OKC does not mandate how a PMK arrives at the target AP. OKC instead allows a client station the opportunity to take advantage of a cached PMK shared among multiple access points. Effectively, OKC is a preview of mechanisms defined by the 802.11r-2008 amendment.

15. B, D. The original legacy 802.11 standard, for the most part, only defined roaming as a Layer 2 process known as the reassociation service. However, the 802.11-2007 standard does not define two very important processes for BSS transition: client roaming thresholds and AP-to-AP handoff communications. Client roaming thresholds are usually based on RSSI.

16. D. An 802.1X/EAP exchange creates a master session key (MSK), which is used to create a pairwise master key (PMK) for non-FT systems. FT also uses the 802.1X/EAP exchange to create the master session key that seeds a centralized but much more complex key management solution. The supplicant and the RADIUS server exchange credentials, and the PMK is created from the master session key and sent to the authenticator. The authenticator is typically a WLAN controller or an autonomous AP.

17. A, B. The PMK-R0 is cached on the WLAN controller. The WLAN controller is the key holder for the first level key. The various levels of FT keys are also derived and stored on the supplicant. 802.1X/EAP creates the master session key (MSK). The MSK is used to create the first level master key called a PMK-R0. The PMK-R0 is cached on the supplicant, which is the client station. The client station is the key holder for the first-level key. The PMK-R0 is also cached on the client station.

18. B, C. The second-level key PMK-R1 is derived from the PMK-R0 and sent to the controller-based APs. The PMK-R1 keys are cached on the APs. The access points are the key holders for the PMK-R1 keys. The client station derives the second-level key PMK-R1 from the PMK-R0. The PMK-R1 key is cached on the client station. The supplicants are the key holders for the PMK-R1 keys.

19. C, D. Most WLAN vendors encrypt/decrypt client traffic at the edge of the network using the access points. In this model the WLAN controller functions as the Pairwise Master Key R0 Holder (R0KH) while the AP functions as the Pairwise Master Key R1 Holder (R1KH). However, some WLAN vendors perform encryption at the WLAN controller level instead of at the AP level. End-to-end encryption provides data privacy between the client at the access layer and the WLAN controller that is typically deployed at the core. In that scenario, the WLAN controller functions as both the Pairwise Master Key R0 Holder (R0KH) and the Pairwise Master Key R1 Holder (R1KH).

20. C. During both methods of fast BSS transition, four frames carry an FT authentication algorithm (FTAA) along with nonces and other information needed to create the final dynamic keys. The PMK-R1 key is the seeding material for both over-the-air and over-the-DS fast BSS transition frame exchanges that create the final pairwise transient key (PTK).

Chapter 8

Wireless Security Risks

IN THIS CHAPTER, YOU WILL LEARN ABOUT THE FOLLOWING:

- ✓ **Unauthorized rogue access**
  - Rogue devices
  - Rogue risks
  - Rogue prevention
- ✓ **Eavesdropping**
  - Casual eavesdropping
  - Malicious eavesdropping
  - Eavesdropping risks
  - Eavesdropping prevention
- ✓ **Authentication attacks**
- ✓ **Denial of Service (DoS) attacks**
  - Layer 1 DoS
  - Layer 2 DoS
- ✓ **MAC spoofing**
- ✓ **Wireless hijacking**
- ✓ **Encryption cracking**
- ✓ **Peer-to-Peer attacks**
- ✓ **Management interface exploits**
- ✓ **Vendor proprietary attacks**
- ✓ **Social engineering**
- ✓ **Physical damage and theft**
- ✓ **Public use and WLAN hotspots**

802.11 wireless networking is inherently insecure due to the use of a shared and unbounded medium—radio frequency (RF) signals. Unlike traditional bounded, or wired, networks, the medium used by wireless networks extends beyond the confines of your office or home and even beyond your campus and property as far as the signal can propagate. Essentially, your network is shared with not only the computers and other devices on your cables but also with any other 802.11 devices on the same frequency channel. 802.11 transmissions can be monitored by any third party not participating in the WLAN conversations. This lack of signal containment makes wireless networking inherently insecure. 802.11 WLANs have become expected in many locations such as office buildings, hotels, airports, coffee shops, restaurants, and now even in airplanes. New networks are increasingly wireless by default and wired by exception. Access points and client devices have become less expensive and are sold by popular retail outlets and even in vending machines. The increased use of 802.11 wireless technology has made it easier for workers to be more productive in the office and on the road. As the popularity of WLANs continues to grow, so does the potential for WLAN attacks and security risks. In this chapter, we will examine the risks involved with the use of 802.11 wireless networking and discuss some of the ways to mitigate these risks.

Unauthorized Rogue Access

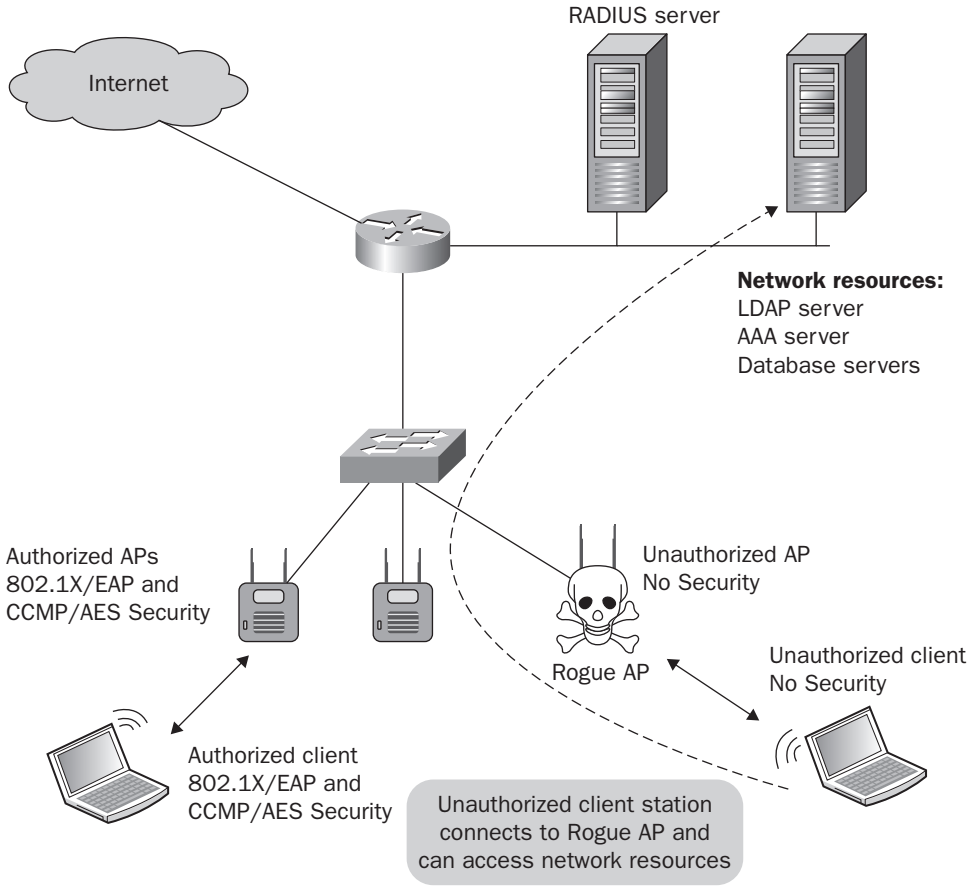
The corporate WLAN is an authorized wireless portal to network resources. In Chapter 4, "Enterprise 802.11 Layer 2 Authentication Methods," we discussed the proper 802.1X/EAP mechanisms that should be used to authenticate users before they are authorized through the corporate WLAN portal. However, what is there to prevent an individual from installing their own unauthorized wireless portal onto the network backbone? The big buzz phrase in Wi-Fi security has always been the *rogue access point* or *rogue device*. A rogue access device is any WLAN radio that is connected to the wired infrastructure but is not under the management of proper network administrators. A rogue device is any unauthorized WLAN portal to network resources.

Rogue Devices

It is not uncommon for a company to have a wireless network installed and not even know about its existence. The individuals usually responsible for installing rogue access points (APs) are not hackers; they are employees not realizing the consequences of their actions. According to some statistics, well over 80 percent of home users have wireless access at home and have become accustomed to the convenience and mobility that Wi-Fi offers. As

a result, employees often install their own wireless devices in the workplace because the company they work for has yet to deploy an enterprise wireless network or they are not aware of the corporate policy forbidding installation of WLAN devices. The problem is that, while these self-installed access points might provide the wireless access that the employees desire, they are rarely secured. Any $75 SOHO Wi-Fi access point or router can be plugged into a live data port. The rogue access point is a potential open and unsecured gateway straight into the wired infrastructure that the company wants to protect (see Figure 8.1).

FIGURE 8.1 Rogue access point



While it is true that in some industries, corporate espionage exists and in some government deployments dedicated attackers can be found, the vast majority of rogue devices are not installed for these malicious purposes. The majority of rogue devices are placed on networks by approved network users, employees, contractors, and visitors. Employees, contractors, and visitors are granted physical access to the buildings on a daily

basis, something a dedicated attacker is not given. These "trusted" individuals rarely place rogue devices for malicious purposes. They place them to extend their wireless coverage or provide wireless coverage in areas that they feel it should exist without organizational permission. Some of the "trusted" individuals do not know that they are doing anything wrong due to the lack of an enforced security policy covering the use of wireless devices. They are simply uninformed about the risks of such device use.

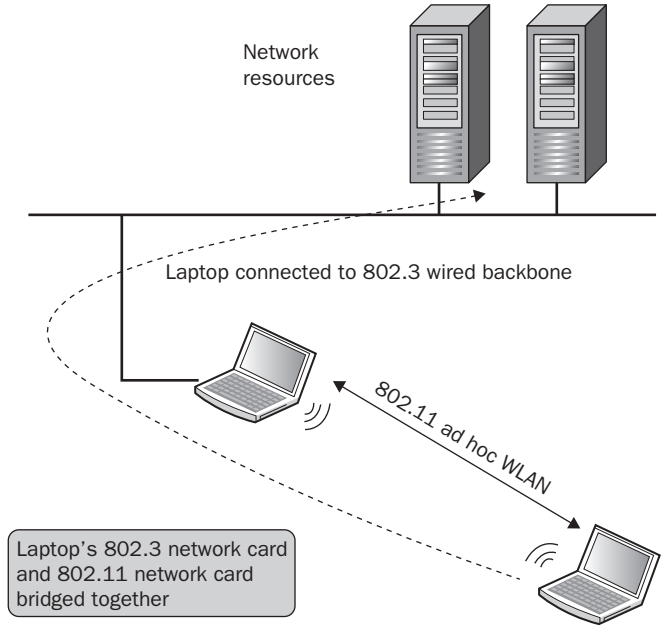
Other members of this "trusted" group know that what they are doing is against policy but believe their need for wireless networking is more important than written policy. This subgroup will often take measures to hide the rogue access points or laptops under their desks, in boxes, or behind furniture. Rogue devices are even found in server rooms, having been placed there by the IT staff against policy. Although only a single open portal is needed to expose network resources, many large companies have discovered literally dozens of rogue access points installed by employees and/or contractors. Most of the rogue devices that are installed by employees are actually not access points but are instead SOHO 802.11 wireless routers that can be purchased for under $75.

Don't Have Wi-Fi at Work? Surprise!

A United States WLAN services company, Netrepid, performed a wireless survey for a hospital in 2007 that was found to have over 75 rogue access points throughout the main building. The IT department was certain that, prior to the survey, there were no rogue devices in the building. The rogue devices were almost exclusively SOHO wireless routers.

Probably the most overlooked rogue device is the ad hoc wireless network. The technical term for an 802.11 ad hoc WLAN is an *independent basic service set (IBSS)*. The 802.11 radios communicating within an IBSS network consist solely of client stations, and no access point is deployed. An IBSS network that consists of just two stations (STAs) is analogous to a wired crossover cable. An IBSS, however, can have multiple client stations in one physical area communicating in an ad hoc fashion. Unfortunately, ad hoc networks also have the potential of providing rogue access into the corporate network. Very often an employee will have a laptop or desktop plugged into the wired network via an Ethernet network card. On that same computer, the employee has a Wi-Fi radio and has set up an ad hoc Wi-Fi connection with another employee. As shown in Figure 8.2, the Ethernet connection and the Wi-Fi card can be bridged together—an intruder might access the ad hoc wireless network and then potentially route their way to the Ethernet connection and get onto the wired network.

FIGURE 8.2 Bridged ad hoc WLAN



Another emerging rogue type is the wireless printer. Many printers now have 802.11 radios with ad hoc mode. Attackers can connect to these printers using the printer manufacturer's administrative tools, downloadable from the company's website. Then using these tools, attackers can upload their own firmware to your printer, thus allowing them to bridge the wired and wireless connections of your printer to gain access to your wired network, without the use of an access point. Many wireless camera security systems can be breached in a similar manner.

As we have already mentioned, the individuals usually responsible for installing rogue access points are not hackers but instead are employees. The employees leave an open wireless portal for anyone to pass through. Because rogue devices are unauthorized WLAN portals, all of your network resources are potentially exposed. If network resources are exposed, the following risks exist:

Data Theft Corporate data on database servers can be compromised. Credit card information, corporate trade secrets, personnel information, and medical data can all be stolen if exposed via a rogue device. Any data stored on network servers or desktop workstations is entirely at risk. Data theft is usually the most common risk associated with rogue access. Here are some additional risks:

Data Destruction Destruction of data can also occur. Databases can be erased and drives can be reformatted.

Loss of Services Network services can also be disabled. Even if no data was stolen or destroyed, imagine the loss of productivity and the potential losses if email services were disabled by an attacker through a rogue AP.

Malicious Data Insertion An attacker can use the unauthorized portal to upload viruses and pornography. Remote control applications and keystroke loggers can also be uploaded to network resources and used to gather information at a later date. Attackers have been known to upload illegally copied software and set up illegal FTP servers to distribute the illegal software.

Third-Party Attacks Once an attacker has accomplished rogue access, your wired network can be used as a launching pad for third-party attacks against other networks across the Internet. Distributed denial-of-service (DDoS) attacks against other corporate networks can be launched from your network infrastructure. Spammers long ago figured out that they can use a rogue AP as the originating source to send spam.

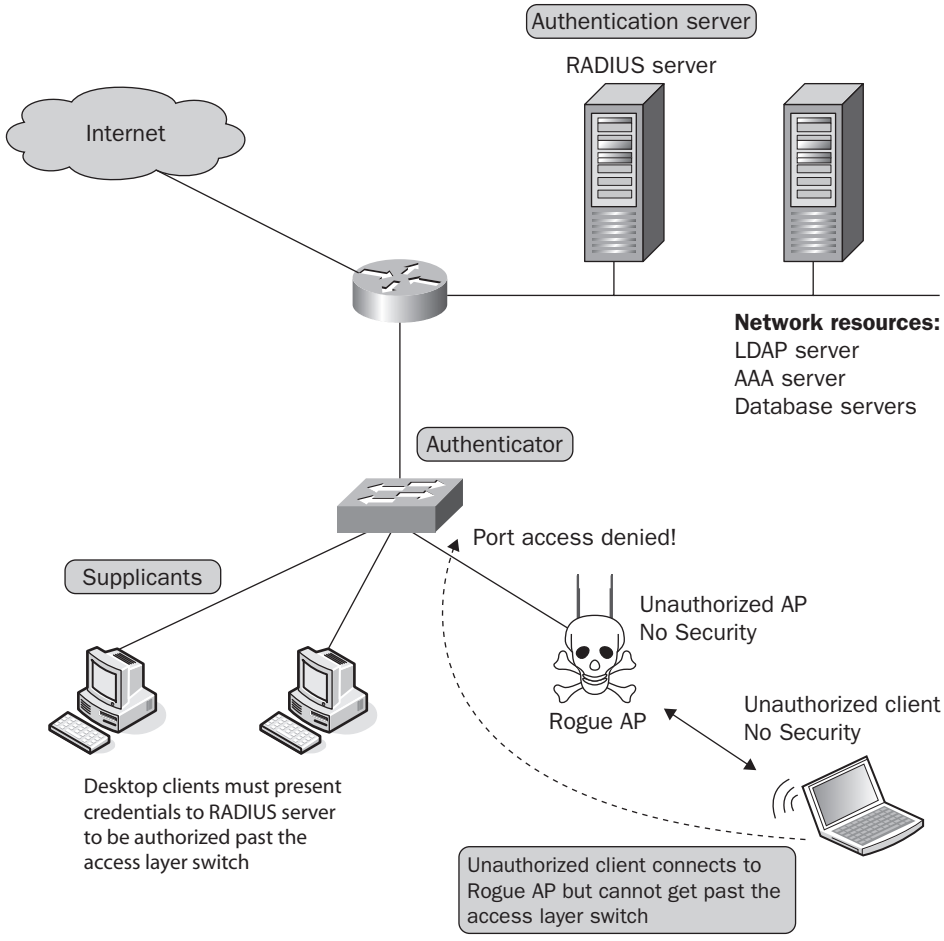
Rogue Prevention

In Chapter 13, "Wireless Security Policies," we will discuss corporate policies that ban employees from installing unauthorized APs. Additionally, many government agencies and corporations ban the use of ad hoc networks. The ability to configure an ad hoc network can be disabled on most enterprise client devices. Endpoint WLAN security software can also be installed on WLAN client devices to prevent bridging between 802.11 client radios and 802.3 Ethernet radios.

Policy is a great start. However, beyond physical security or wired port control, there is nothing to prevent an intruder from connecting their own rogue AP via an Ethernet cable into any live data port provided in a wall plate.

The best way of preventing rogue access is wired port control. The main focus of Chapter 4 was how 802.1X/EAP security is used for authentication and authorization via the WLAN. It should be noted that 802.1X/EAP can also be used to authorize access through wired ports on an access layer switch. EAP-MD5 and EAP-TLS can be used for wired 802.1X/EAP authentication to control wired side access. As depicted in Figure 8.3, unless proper credentials are presented at Layer 2, upper-layer communications are not possible through the wired port. A rogue device cannot act as a wireless portal to network resources if the rogue device is plugged into a managed port that is blocking upper-layer traffic. Therefore, a wired 802.1X/EAP solution is an excellent method for preventing rogue access.

FIGURE 8.3 Wired 802.1X/EAP prevents rogue access.



It should be noted that most businesses do not use a wired 802.1X/EAP solution for wired port control. Therefore a WLAN monitoring solution known as a *wireless intrusion detection system (WIDS)* is always needed to detect potential rogue devices. Most WIDS vendors prefer to call their products a *wireless intrusion prevention system (WIPS)*. The reason that they refer to their products as prevention systems is that they are all now capable of mitigating attacks from rogue access points and rogue clients.

In Chapter 10, "Wireless Security Monitoring," you will be introduced to the concept of *classification*, which is used by wireless intrusion detection systems (WIDS) to differentiate between authorized devices and rogue devices. A more detailed discussion of methods of rogue detection, classification, and mitigation is also found in that chapter.

WIPS solutions use several methods to effectively terminate, suppress, and contain communications from rogue devices. The most common method of rogue containment uses a known Layer 2 DoS attack against the rogue device as a countermeasure. Rogue APs and ad hoc clients can be effectively contained until they are located and removed. Another method of rogue mitigation uses the Simple Network Management Protocol (SNMP). Most WIPSs can determine that the rogue AP is connected to the wired infrastructure and may be able to use SNMP to disable the managed switch port that is connected to the rogue AP. If the switch port is closed, the attacker cannot attack network resources that are behind the rogue AP. This method of rogue AP mitigation is known as *port suppression*.

Real World Scenario

Will a WIPS Protect Against All Known Devices?

The simple answer is "no." Although wireless intrusion prevention systems are outstanding products that can mitigate most rogue attacks, some rogue devices will go undetected. The radio cards inside the WIPS sensors typically monitor the 2.4 GHz ISM band and the 5 GHz UNII frequencies. Older legacy wireless networking equipment exists that transmits in the 900 MHz ISM band, and these devices will not be detected. The radio cards inside the WIPS sensors also use only *direct sequencing spread spectrum (DSSS)* and *orthogonal frequency division multiplexing (OFDM)* technologies. Wireless networking equipment exists that uses *frequency hopping spread spectrum (FHSS)* transmissions in the 2.4 GHz ISM band and will go undetected. The only tool that will detect with 100 percent certainty either a 900 MHz or a frequency hopping rogue AP is a spectrum analyzer capable of operating in those frequencies. Some WIPSs are beginning to offer *Distributed Spectrum Analysis Systems (DSAS)*. A more detailed discussion of DSAS can be found in Chapter 10.

Eavesdropping

Just as human conversations can be overheard by any third party within hearing range of the speakers' voices, WLAN communications between two 802.11 radios can be overheard by any third-party 802.11 station on the same frequency channel. Because the RF medium is half-duplex, and therefore a shared medium, only one 802.11 station can transmit at any given time. However, any 802.11 radio within listening range can monitor any active 802.11 transmissions. WLAN communications can be monitored via two eavesdropping methods: *casual eavesdropping* and *malicious eavesdropping*.

Casual Eavesdropping

Casual eavesdropping is sometimes referred to as WLAN discovery. Casual eavesdropping is accomplished by simply exploiting the 802.11 frame exchange methods that are clearly

defined in the 802.11-2007 standard. As we discussed in Chapter 2, "Legacy 802.11 Security," in order for an 802.11 client station to be able to connect to an access point, it must first discover the access point. A station discovers an access point by either listening for an AP (passive scanning) or searching for an AP (active scanning). In *passive scanning*, the client station listens for 802.11 beacon management frames that are continuously sent by the access points.

A casual eavesdropper can simply use any 802.11 client radio to listen for 802.11 beacon management frames and to discover Layer 2 information about the WLAN. Some of the information found in beacon frames includes the service set identifier (SSID), MAC addressing, supported data rates, and other basic service set (BSS) capabilities. All of this Layer 2 information is in cleartext and can be seen by any 802.11 radio.

In addition to scanning passively for APs, client stations can actively scan for them. In *active scanning*, the client station transmits management frames known as probe requests. The access point then answers back with a probe response frame that basically contains all of the same Layer 2 information that can be found in a beacon frame. A probe request without the SSID information is known as a *null probe request*. If a directed probe request is sent, all APs that support that specific SSID and hear the request should reply by sending a probe response. If a null probe request is heard, all APs, regardless of their SSID, should reply with a probe response.

Most casual eavesdroppers will discover 802.11 networks using software tools that send null probe requests. Casual eavesdropping is typically considered harmless and is also often referred to as wardriving. Wardriving is strictly the act of looking for wireless networks, usually while in a moving vehicle. The term wardriving was derived from *wardialing* from the 1983 film *WarGames*. Wardialing is old technique used by hackers using computer modems to scan thousands of telephone numbers automatically to search for other computers with which they can connect. Wardriving software utilities known as *WLAN discovery tools* exist for the purpose of finding open WLAN networks. The most common wardriving WLAN discovery tool is a freeware program called *NetStumbler* (see Figure 8.4).

FIGURE 8.4 NetStumbler

NetStumbler and other WLAN discovery tools send out null probe requests across all license-free 802.11 channels with the hope of receiving probe response frames containing wireless network information, such as SSID, channel, encryption, and so on. By design,

the very nature of 802.11 passive and active scanning is to provide the identifying network information that is accessible to anyone with an 802.11 radio card. Because this is an inherent and necessary function of 802.11, wardriving is not a crime. However, the goal of many wardrivers is to find open 802.11 wireless networks that can provide free gateway access to the Internet. Although the legality of using an open wireless gateway to the Internet remains unclear in most countries, the majority of wardrivers are not hackers intending harm but rather simply wireless users wanting temporary, free Internet access. The legality of using someone else's wireless network without permission is often unclear, but be warned that people have been arrested and prosecuted as a result of these actions.

We do not encourage or support the efforts of using wireless networks that you are not authorized to use. We recommend that you connect only to 802.11 wireless networks that you are authorized to access.

Real World Scenario

What Tools Are Needed for Wardriving?

Companies sell what they call wardriving kits. These kits normally consist of an antenna, pigtail, and PCMCIA card. The kit allows the user to detect devices from a greater range using integrated wireless cards or standard PCMCIA cards.

To get started wardriving, you will need an 802.11 client card, a software WLAN discovery application, and an automobile! Numerous freeware-based discovery tools exist, including NetStumbler for Windows, MiniStumbler for Windows CE, MacStumbler for Macintosh, and Kismet for Linux. A copy of NetStumbler is included on the CD that accompanies this book and can also be downloaded at `www.netstumbler.com`. Another, optional tool is a high-gain external antenna that can be connected to your wireless card via a pigtail connector. Many wardrivers also use global positioning system (GPS) devices in conjunction with NetStumbler to pinpoint the longitude and latitude coordinates of the signal from access points that they discover. Wardriving capture files with GPS coordinates can be uploaded to large dynamic mapping databases on the Internet. One such database, called the Wireless Geographic Logging Engine (WIGLE), maintains a searchable database of more than 5 million access points. Go to `www.wigle.net` and type in your address to see whether any wireless access points have already been discovered in your neighborhood.

Malicious Eavesdropping

Malicious eavesdropping is the unauthorized use of protocol analyzers to capture wireless communications and is typically considered illegal. Most countries have some type of wiretapping law that makes it a crime to listen in on someone else's phone conversation.

Additionally, most countries have laws making it illegal to listen in on any type of electromagnetic communications, including 802.11 wireless transmissions. Protocol analysis and packet analysis are used to diagnose problems in network communications, identify traffic patterns, and find bottlenecks. Many commercial and freeware 802.11 protocol analyzers exist that allow wireless network administrators to capture 802.11 traffic for the purpose of analyzing and troubleshooting their own wireless networks. In earlier chapters, you used a WLAN protocol analyzer in several exercises to look at 802.11 frame transmissions. A *protocol analyzer* is a passive device that operates in an RF monitoring mode to capture any 802.11 frame transmissions within their range. However, a protocol analyzer can also be used as a malicious listening device for unauthorized monitoring of 802.11 frame exchanges.

Eavesdropping Risks

Because malicious eavesdropping is a passive attack, it should be understood that a WIDS/WIPS solution will not be able to detect a protocol analyzer because it is not a transmitting device. The WLAN protocol analyzer is a listening device and will go undetected. Because protocol analyzers capture 802.11 frames passively, a wireless intrusion detection system (WIDS) cannot detect malicious eavesdropping, and the attacker cannot be located.

802.11 frames can be passively monitored and data can be captured from great distances well beyond the limits of corporate buildings and property lines. An attacker does not need physical access to buildings or property to perform malicious eavesdropping. WLANs cannot be hidden from the outside world when the RF signal propagates beyond property lines. Even if a strong RF signal does not propagate from beyond your own walls, an eavesdropper could use a high gain antenna to amplify a weak signal and still be able to monitor 802.11 frame transmissions passively from locations beyond your physical control. 802.11 frames can be passively captured with a protocol analyzer from a distance of many miles if the attacker has line of sight, and the attacker will remain undetected.

Postal Analogy

Think of WLAN communications as sending postcards, letters, or any other package. If someone sees the package in transit, they can always see its origin and destination as well as the means by which it is being conveyed—mail, courier, express delivery service, freight, and so on. Despite the fact that the package is well wrapped or in an envelope, the addressing is still exposed. In wireless terms, no matter how the information is encrypted, Layers 1 and 2 are exposed to allow proper transmission and reception. Therefore, all Layer 2 information, such as MAC addresses, will always be exposed in a WLAN environment. When a postcard is sent, not only will the addressing and means of conveyance be seen, but the actual postcard message can also be read by anyone while the postcard is in transit. If no encryption is used in a WLAN environment, the Layer 3–7 data payload is exposed to anyone who happens to be listening.

Many people believe that if their data is encrypted, they have nothing else that an attacker may wish to collect. That belief brings with it a false sense of security. All Layer 2 information is still seen in cleartext, and this information can be gathered passively using a WLAN protocol analyzer. MAC addresses and Layer 2 discovery protocols can be seen in the clear.

As discussed in Chapter 2, a legacy security measure is MAC filtering. MAC filtering is the blocking of all MAC addresses from connecting unless they are specifically allowed or, alternately, allowing all MAC addresses unless they are specifically denied access. As stated earlier, the MAC addresses of WLAN devices are visible each time a device transmits any type of frame. Since the MAC addresses can be seen by any device on the same channel, an attacker can document their use. Anyone with a WLAN protocol analyzer can capture 802.11 frame exchanges between an AP and a client and see the MAC addressing that is used for the Layer 2 communications. Simply put, MAC filters do not offer any real measure of security for wireless transmissions.

Wired leakage is also a security risk and a type of information that an attacker can use to gain access to your network or data. Wired leakage often occurs when wired stations, servers, or infrastructure devices use a broadcast protocol to communicate or to find other devices with which to replicate. Access points may forward broadcast and multicast traffic from the wired infrastructure. Layer 2 discovery protocols, such as the *Cisco Discovery Protocol (CDP),* will reveal information about the wired network as well as what can be seen wirelessly. Again, passively using protocol and packet analysis will not deter a potential attacker from gaining valuable information about your infrastructure.

If encryption is not being used, the Layer 3–7 payload of any 802.11 data frame will also be exposed. Any cleartext communications such as email and Telnet passwords can be captured if no encryption is provided. Furthermore, any unencrypted 802.11 frame transmissions can be reassembled at the upper layers of the OSI model. For example, email messages can be reassembled and therefore read by an eavesdropper. Web pages and instant messages can also be reassembled. VoIP packets can be reassembled and saved as a WAV sound file. Malicious eavesdropping of this nature is highly illegal. Because of the passive and undetectable nature of this attack, encryption must always be implemented to provide data privacy.

Eavesdropping Prevention

How can you stop attackers and others from gaining access to your exposed information? The easiest and most important method of protection against malicious eavesdropping attacks is to use encryption. Encryption provides the data privacy necessary to protect the *MAC Service Data Unit (MSDU)* upper layer payload of 802.11 data frames. A strong, dynamic encryption solution—such as TKIP/RC4 or, even better, CCMP/AES—is a mandatory requirement to protect the Layer 3–7 payload.

To prevent anyone other than intended recipients from hearing your transmissions, you can use RF shielding to stop transmissions from exiting or entering your building.

Mylar films can be placed on all of your windows, stopping signals from escaping through them. Special paint or wallpapers can be used to do the same for your walls, essentially making your building a *Faraday cage*. A Faraday cage, also known as a Faraday shield, is an enclosure made of a wired mesh or other conductive material to contain electric fields such as RF signals. Faraday shields can be built into the walls of buildings, but the construction costs are very high. Usually only well-funded and extremely security-conscious organizations, such as government offices and military institutions, go through the time and expense and take these measures to contain RF transmissions from exposure to the outside world.

The bottom line is that because 802.11 technology operates at Layers 1 and 2 of the OSI model, there is virtually no way to protect those two layers from eavesdropping. To prevent some Layer 2 wired leakage, we highly recommended that you disable Layer 2 discovery protocols such as CDP.

However, the number one priority should always be to protect the MAC Service Data Unit (MSDU) upper layer payload of 802.11 data frames. Strong, dynamic encryption solutions, such as TKIP/RC4 or even better CCMP/AES, should always be considered mandatory requirement to protect the Layer 3–7 payload and provide data privacy.

Authentication Attacks

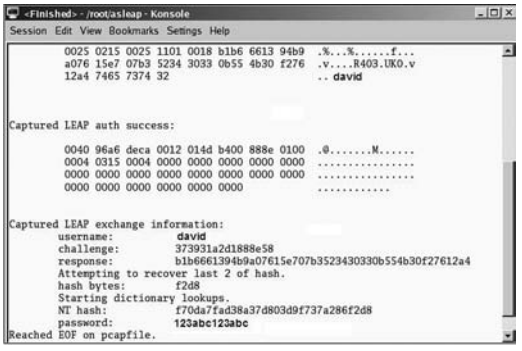
As you learned earlier, the usual purpose of an 802.11 wireless network is to act as a portal into an 802.3 wired network. It is therefore necessary to protect that portal with very strong authentication methods so that only legitimate users with the proper credentials will be authorized to access network resources.

Authentication is the method of verifying the presented identity and credentials. Once the method of authentication has been determined by an attacker, they can begin to try to break the authentication process. Some forms of authentication are stronger than others. There are some forms of authentication that are very easy to break and should not be used in secure environments. There are others that are very complex, which are better suited to more secure environments. The type of authentication used is often dictated by things other than the security requirements of the transmissions and environments, such as ease of use, cost, device types, firmware used, regulations policy, and legacy deployments.

In Chapter 2, you learned about Open System authentication, which essentially validates all clients. As you have also already learned, stronger authorization to access network resources can be achieved by either an 802.1X/EAP authentication solution or the use PSK authentication. The 802.11-2007 standard does not define which type of EAP authentication method to use, and all flavors of EAP are not equal. Some types of EAP authentication methods are more secure than others. As a matter of fact, Cisco's *Lightweight Extensible Authentication Protocol (LEAP)*, once one of the most commonly deployed 802.1X/EAP solutions, is susceptible to an *offline dictionary attack*. The hashed password response during the LEAP authentication process is crackable. An attacker merely has to capture a frame exchange when a LEAP user authenticates and then run the capture file through an offline dictionary attack tool, as shown in Figure 8.5. The password can

be derived in a matter of seconds. The username is also seen in cleartext during the LEAP authentication process. After the attacker gets the username and password, they are free to impersonate the user by authenticating onto the WLAN and then accessing any network resources that are available to that user. It should be noted that weaker VPN solutions such as PPTP using MS-CHAPv2 authentication are also susceptible to offline dictionary attacks. Stronger EAP authentication protocols that use "tunneled authentication" are not susceptible to offline dictionary attacks.

FIGURE 8.5 Offline dictionary attack



The biggest risk with any authentication attack is that all network resources become vulnerable if the authentication credentials are compromised. The risks of authentication attacks are similar to rogue access points. If an authorized WLAN portal can be compromised and the authentication credentials can be obtained, the following risks also apply:

- Data theft
- Data destruction
- Loss of services
- Malicious data
- Third-party attacks

Because of these severe risks, it is therefore necessary to secure the corporate WLAN infrastructure properly with an 802.1X/EAP solution that uses a RADIUS server and the tunneled authentication EAP protocols discussed in Chapter 4. Multifactor authentication, also known as two-factor authentication, also increases the difficulty of cracking security immensely by adding another set of required credentials. WPA-Enterprise and WPA2-Enterprise certified solutions are almost always a necessity for the strong authentication security that is required in the workplace.

Because most home users do not have a RADIUS server in their house, weaker WPA/WPA2-Personal authentication methods are normally used. Until fast secure roaming

mechanisms become more commonplace, expect WPA/WPA2-Personal authentication to still be widely used for VoWiFi phones in the enterprise.

WPA/WPA2-Personal, using *preshared keys*, is a weak authentication method that is vulnerable to an offline *brute-force dictionary attack*. Shared keys or passphrases are also easily obtained through social engineering techniques. Social engineering is the act of manipulating people into performing actions or divulging confidential information. Hacking utilities are available that can derive the WPA/WPA2 passphrase by using an offline brute-force dictionary attack. An attacker who obtains the passphrase can associate with the WPA/WPA2 access point and access network resources. The biggest risk with any authentication attack is that all network resources could become vulnerable if the authentication credentials are compromised.

Even worse is that after obtaining the passphrase, the hacker can begin to decrypt the dynamically generated TKIP/RC4 or CCMP/AES encryption key. In Chapter 6, "SOHO 802.11 Security," you learned that the passphrase is used to derive the Pairwise Master Key (PMK), which is used with the 4-Way Handshake to create the final dynamic encryption keys. If a hacker has the passphrase and captures the 4-Way Handshake, they can re-create the dynamic encryption keys and decrypt traffic. WPA/WPA2-Personal is not considered a strong security solution for the enterprise because if the passphrase is compromised, the attacker can not only access network resources, they can also decrypt traffic. In situations where there is no RADIUS server or the client devices do not support 802.1X/EAP authentication, a WPA/WPA2-Personal deployment may be necessary.

A policy mandating very strong passphrases of 20 characters or more should always be in place whenever a WPA/WPA2-Personal solution is deployed. Furthermore, because passphrases are static, they are susceptible to social engineering attacks. To prevent social engineering attacks, policy must dictate that only the administrator have knowledge of any static passphrases and that the passphrases are never shared with end users.

Denial-of-Service Attacks

Denial-of-service (DoS) attacks are not by themselves an attempt to gain access to your information or data. A DoS attack against a WLAN is an attack that effectively disables the WLAN. With the proper tools, any individual with ill intent can temporarily disable a Wi-Fi network by preventing legitimate users from accessing network resources. For mission-critical systems, this is a serious security concern. If the WLAN goes down, any application or network resource being accessed through the WLAN is no longer available. The wireless VoIP phone conversation comes to an abrupt end, communications with your database server are no longer possible, and wireless access to an Internet gateway has been closed. DoS attacks can be either malicious attempts to disrupt your WLAN or of an accidental nature. DoS attacks can also be used to jump-start other attacks such as wireless hijacking and Wi-Fi phishing. The good news is that monitoring systems exist that can detect and identify DoS attacks immediately. The bad news is that usually nothing can

be done to prevent DoS attacks other than locating and removing the source of the attack. DoS attacks can be targeted against the entire WLAN or can be targeted against individual access points or individual WLAN clients.

Layer 1 DoS Attacks

A DoS attack to a WLAN is most easily accomplished at Layer 1 in the RF environment. Layer 1 DoS attacks are a result of radio frequency interference. What can cause Layer 1 DoS? Layer 1 DoS can be a result from either intentional interference or unintentional interference.

Denial of service at Layer 1 usually occurs as an unintentional result of transmissions from non-802.11 devices. All sorts of devices transmit in the very crowded 2.4 GHz ISM band. RF video cameras, baby monitors, cordless phones, and microwave ovens are all potential sources of interference. The whole point of a spectrum analysis site survey is to identify and eliminate these sources of interference. But what if an employee forgets about corporate policy and employs a leaky microwave oven or a 2.4 GHz cordless phone after the original site survey was performed? Microwave ovens typically operate at 800 to 1,000 watts. Although microwave ovens are shielded, they can become leaky over time. A received signal of –60 dBm is about 1 millionth of 1 milliwatt and is considered a very strong signal for normal 802.11 communications. If a 1,000 watt microwave oven is even 0.000000001 percent leaky, the oven will interfere with the 802.11 radio.

Unintentional interference may cause continuous DoS; however, the disruption of service is often sporadic. This disruption of service will upset the performance of Wi-Fi networks used for data applications and can completely disrupt VoWiFi communications within a WLAN. At the very least, unintentional interference will result in retransmissions that negatively affect WLAN performance. The majority of unintentional interfering devices transmit in the 2.4 GHz ISM frequency band, and 2.4 GHz cordless phones, Bluetooth devices, medical equipment, and many other devices can cause unintentional interference in the 2.4 GHz ISM band. The 5 GHz UNII bands are less susceptible to unintentional interference. 5 GHz cordless phones often cause interference with the four channels of the 5 GHz UNII-3 band.

Now let's examine deliberate attempts to disrupt wireless networking at Layer 1. If the RF medium can be accidentally interfered with, it can also be purposely jammed at Layer 1. *Intentional interference* can be accomplished using a wide-band jamming device or narrow-band jamming device. A wide-band jammer transmits a signal that raises the noise floor for most of the entire frequency band and therefore disrupts communications across multiple channels. As shown in Figure 8.6, there are companies that sell wide-band jammers as security tools for enforcing no Wi-Fi zones. Most of these jamming devices transmit in the 2.4 GHz frequency range, but 5 GHz jammers exist as well. The use of such devices is usually illegal in most countries.

FIGURE 8.6 RF jamming device

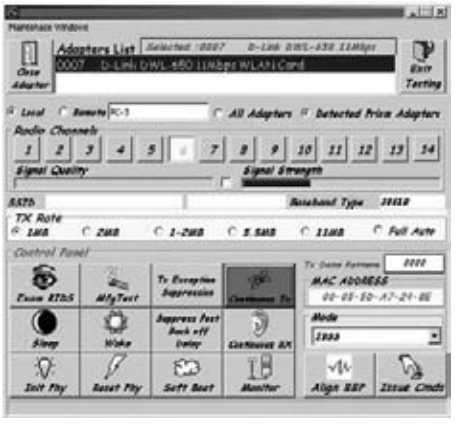
Narrow-band or single-channel jamming can also be done with commercially available devices. Figure 8.7 shows a signal generator that is normally used for legitimate testing purposes, such as to provide a power source to measure coax loss with a wattmeter. However, what is to prevent a villainous individual from transmitting a 1 watt (+30 dBm) signal via an ordinary antenna? The signal generator would then be transformed into a jamming device that will overtake most 802.11 radio cards that transmit at a maximum of 100 mw (+20 dBm). Higher-gain antennas can be combined with the signal generator to achieve more radiated power and extend the range of the DoS attack. Unidirectional antennas can be used to focus a Layer 1 DoS jamming attack.

FIGURE 8.7 RF signal generator and wattmeter

For much less money, an attacker could use the *Queensland Attack* to disrupt an 802.11 WLAN. What if an 802.11 radio card could be placed in a "continuous transmit" state? In this scenario, the radio card would not actually be sending data or modulating data, but would be sending out a constant RF signal much like a narrow-band signal generator. Other 802.11 radios never get to access the medium because whenever they perform a clear channel assessment, the medium is occupied by the continuous transmitter. Researchers at Queensland University in Australia discovered this attack is indeed feasible. As shown in Figure 8.8, a major chipset manufacturer of 802.11b radio cards produced a software utility that placed the radios in a continuous transmit state for testing purposes. This utility can also be used for malicious purposes and is often referred to as the Queensland Attack.

An 802.11b radio operating in continuous transmit state at 30 mW may not be as large as threat as a 1 watt jammer; however, any 802.11b/g cards within range of the malicious radio will be affected.

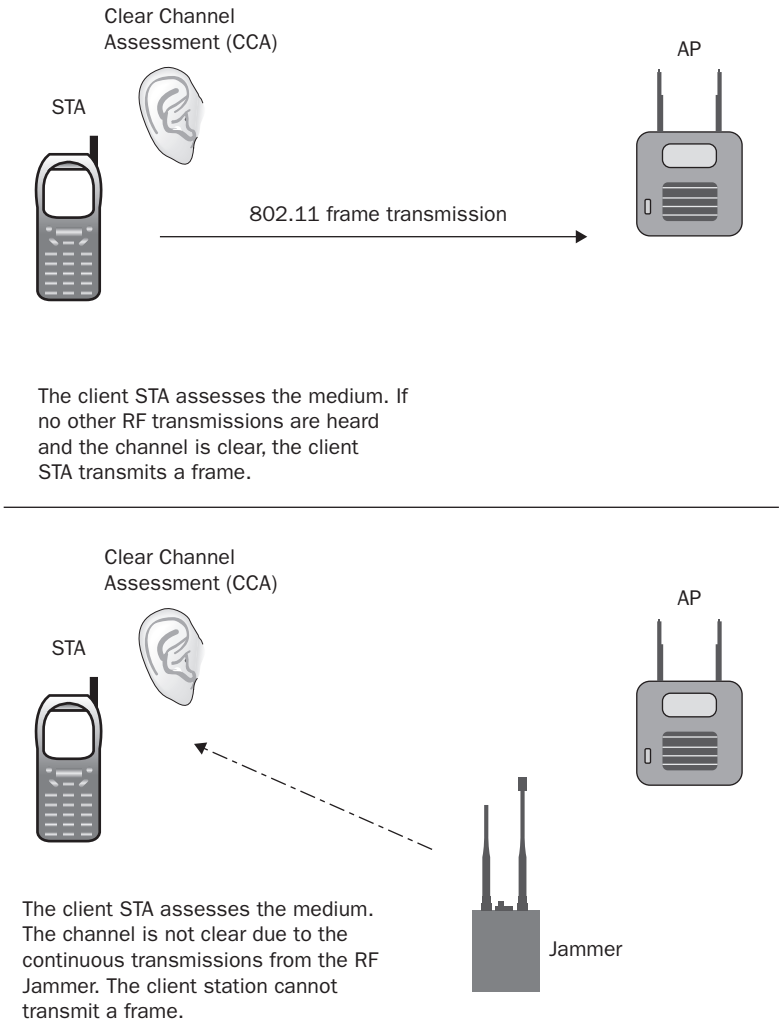
FIGURE 8.8 Testing utility used for Queensland Attack



Why do jamming attacks, both accidental and intentional, cause a denial of service? Because of the half-duplex nature of the RF medium, it is necessary to ensure that at any given time only one radio card has control of the medium. *Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)* is a process used to ensure that only one radio card is transmitting at a time on the medium. One major component of the CSMA/CA method of medium contention is *physical carrier sense*.

Physical carrier-sensing is performed constantly by all stations that are not transmitting or receiving. When a station performs a physical carrier sense, it is actually listening to the channel to see whether any other transmitters are taking up the channel. Physical carrier sense has two purposes. The first purpose is to determine whether a frame transmission is inbound for a station to receive. If the medium is busy, the radio will attempt to synchronize with the transmission. The second purpose is to determine whether the medium is busy before transmitting. This is known as the *clear channel assessment (CCA)*. As shown in Figure 8.9, the CCA involves listening for 802.11 RF transmissions at the Physical layer. The medium must be clear before a station can transmit. However, if the medium is not clear (based on sensing RF transmissions that exceed predefined energy thresholds), the 802.11 radio will defer for a defined amount of time and then perform the CCA once again to listen for a clear medium before transmitting. However, if there is a "continuous" RF transmission that is constantly heard during the CCA intervals, 802.11 transmissions will completely cease until the signal is no longer present. If 802.11 transmissions cease due to an interfering RF signal, the result is a denial of service to the WLAN.

FIGURE 8.9 Clear channel assessment (CCA)



Whether intentional or unintentional, a Layer 1 attack may also result in a partial DoS attack. Every time an 802.11 radio transmits a unicast frame, if the frame is received properly, the 802.11 radio that received the frame will reply with an acknowledgment (ACK) frame. If the ACK is received, the original station knows that the frame transfer was successful. All unicast 802.11 frames must be acknowledged. Broadcast and multicast frames do not require an acknowledgment. If any portion of a unicast frame is corrupted, the cyclic redundancy check (CRC) will fail and the receiving 802.11 radio will not send an ACK frame to the transmitting 802.11 radio. If an ACK frame is not received by

the original transmitting radio, the unicast frame is not acknowledged and will have to be retransmitted. RF devices that just transmit intermittently can disrupt with 802.11 transmissions. The intermittent RF interferer will cause corruption of 802.11 unicast frames that are being transmitted and result in Layer 2 retransmissions. An increase in Layer 2 retransmissions will result in decreased throughput and increased latency. While this might not be as traumatic as a continuous transmitting device causing a complete denial of service, the WLAN performance is still adversely affected.

Taking out the entire band or a single channel for only a few seconds breaks all the communications of any upper-layer applications being used over the WLAN. When the attack is stopped, client stations must locate the AP again, authenticate/associate, get an IP address, and reestablish the application session.

Jamming attacks are often used to kick-start other types of attacks. Jamming can force client stations to reauthenticate. A protocol analyzer can then be used to capture the authentication process of clients using a weak method of authentication, such as LEAP or WPA/WPA2-Personal. The information needed to proceed with an offline dictionary attack has been captured. Narrow-band jamming can also be used to jump-start wireless hijacking, man-in-the-middle, and Wi-Fi phishing attacks described later in this chapter.

If you suspect that sources of interference are causing problems for your network, you can find them using a *spectrum analyzer*. A spectrum analyzer is a frequency domain measurement and troubleshooting tool. A spectrum analyzer can help identify and locate an interfering transmitter. Spectrum analyzers will be discussed in greater detail in Chapter 10, "Wireless Security Monitoring."

A white paper titled "Protecting Wi-Fi Networks from Hidden Layer 1 Security Threats," authored by David Coleman of AirSpy Training and Neil Diener of Cisco Systems, is included on the CD that you received with this book. This white paper is highly recommended reading when you're preparing for the CWSP exam.

Layer 2 DoS Attacks

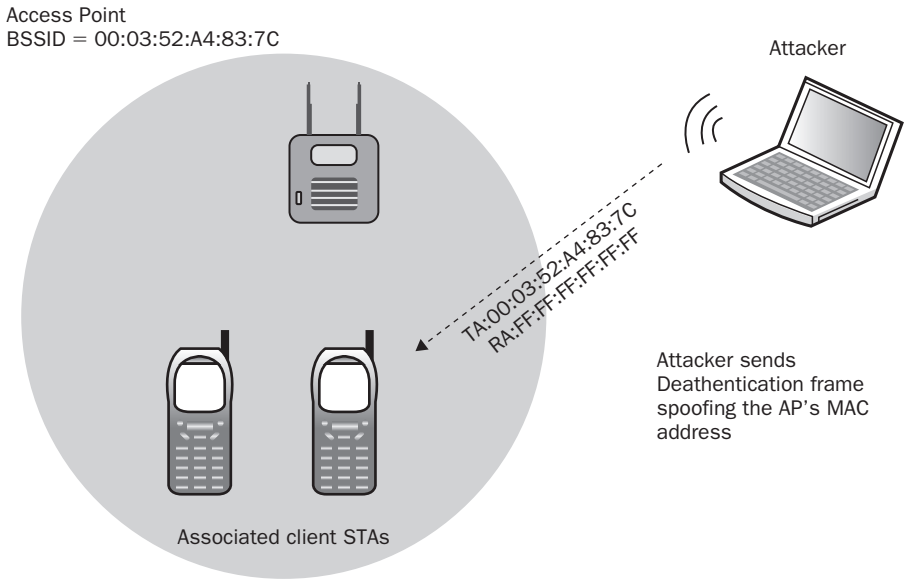
The more common type of DoS attacks that originate from hackers are Layer 2 DoS attacks. A wide variety of Layer 2 DoS attacks exist that are a result of tampering with 802.11 frames and retransmitting them into the air. The most common involves spoofing *disassociation* or *deauthentication* management frames. Let's examine some of the more common Layer 2 intentional DoS attacks.

Many of the intentional DoS attacks found here at Layer 2 use combinations of basic wireless networking requirements and the manipulation of what is required by wireless transmissions for them to succeed. For a client STA to pass data within the basic service set (BSS), it must be authenticated and associated. Without authentication, there is neither association nor Layer 2 connection.

An 802.11 management frame, called a deauthentication frame, is sometimes used by client stations and APs to sever communications at Layer 2. An 802.11 deauthentication frame is a notification and not a request. If a station wants to deauthenticate from an AP, or an AP wants to deauthenticate from stations, either device can send a deauthentication frame. Because authentication is a prerequisite for association, a deauthentication frame will automatically cause a disassociation to occur.

Sadly, deauthentication frames can easily be spoofed, and a deauthentication attack can be launched against a single device or the entire BSS. An attacker simply observes the MAC addresses of client stations and access points using a protocol analyzer. The attacker then uses a hex editor to edit a previously captured deauthentication frame. As shown in Figure 8.10, the attacker can edit the 802.11 header and spoof the MAC address of an access point or a client in either the transmitter address (TA) field or the receiver address (RA) field. The attacker then retransmits the spoofed deauthentication frame repeatedly. The station that receives the spoofed deauthentication frame thinks it is coming from another legitimate station and disconnects at Layer 2. Unicast deauthentication frames can be used as an attack against a single client or multiple clients can be deauthenticated if the destination address is a broadcast address.

FIGURE 8.10 Deauthentication attack



Disassociation attacks work in the same manner and are equally effective for the attacker. Just like deauthentication, disassociation is a notification, not a negotiation. Disassociation management frames can also be spoofed and thereby accomplish the same result as a deauthentication attack.

802.11w Amendment

The 802.11w-2009 amendment is intended to help stop some DoS attacks that use spoofed management frames. Many more types of Layer 2 DoS attacks exist, including association floods, reassociation floods, authentication floods, EAPOL floods, PS-Poll floods, and virtual carrier attacks. Luckily, any good wireless intrusion detection system will be able to alert an administrator immediately to a Layer 2 DoS attack. The 802.11w draft amendment is the proposed *management frame protection (MFP)* amendment with a goal of delivering certain types of management frames in a secure manner. The end result will hopefully prevent some of the Layer 2 DoS attacks that currently exist, but many Layer 2 DoS attacks will never be circumvented. More information about 802.11w-2009 amendment can be found in Chapter 10.

Let's discuss some other Layer 2 DoS attacks that can be accomplished by simply editing 802.11 frames and retransmitting them into the air. Once such attack is called *illegal channel beaconing*. This attack uses a spoofed beacon frame transmitted on the same real channel as the legitimate AP, so that the associated client stations will hear the spoofed beacon. The spoofed beacon uses the same SSID, but the channel field has been edited to display a nonexistent, or illegal, channel. For example, there are 14 channels available for use in the 2.4 GHz range, none of which are used in the spoofed beacon. The attacker's beacon could be telling the client STAs that the AP is on channel 0 or channel 432 or some other unused channel number, when in reality the attacker is beaconing on the same real channel used by the legitimate devices. The drivers of some WLAN vendor radios cannot interpret the illegal channel, and a denial of service is the result.

Probe requests and responses are management frames and can be spoofed just as beacons can be spoofed to disrupt network connectivity. If an attacker sends probe response frames to a victim station, even if it is already associated with a real AP, that station will assume that it should try to connect to that AP. The stations that fall victim to this attack did not send a probe request frame looking for this AP but will try to connect to it anyway. This attack is called a *probe response flood*.

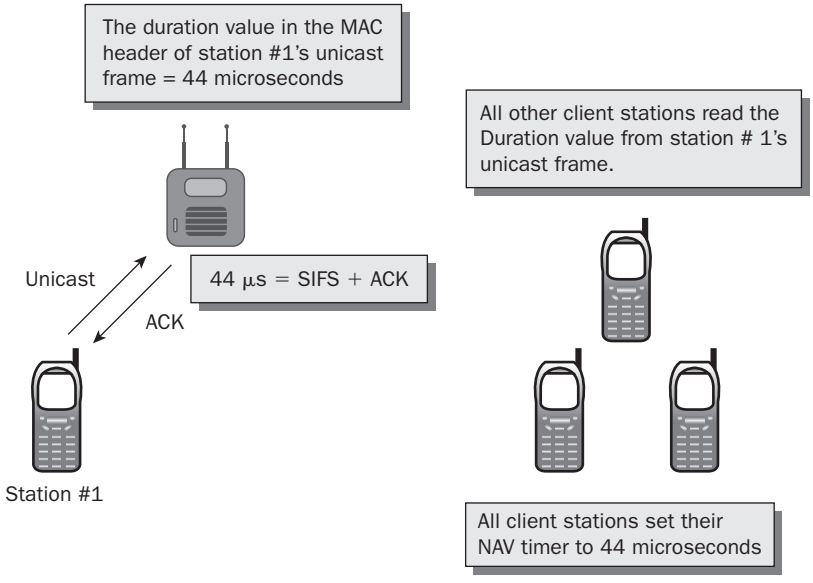
Many Layer 2 DoS attacks are flooding attacks that use management or control frames to overwhelm an access point or client station. An example of a Layer 2 flooding involves an attack on an AP's association table. The 802.11-2007 standard defines the maximum number of client associations to an access point as 2,007. In reality, no access point would ever want 2,007 clients associations, but in theory it is possible. Most vendors offer settings on APs or WLAN controllers to limit the number of active client associations to an AP for capacity purposes. For example, an administrator might set the maximum number of client associations to 20 per access point. An attacker can flood an AP with bogus association request frames and fill up the AP's association table. Then, when any legitimate client attempts to associate, the legitimate clients are denied association because the maximum has already been reached. This attack is called an *association flood*.

Another Layer 2 DoS attack is called *FakeAP*. This software tool generates thousands of counterfeit management advertising fake SSID and BSSIDS. The original intent was to

hide a real access point in plain sight among all the fake APs to confuse any wardrivers, NetStumblers, script kiddies, and other undesirables. The problem is that the FakeAP tool can also be used for a DoS attack. Legitimate client stations may spend time attempting to associate to the APs that do not exist.

As mentioned earlier is this chapter, Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is the process used to ensure that only one radio card is transmitting at a time on the medium. Another major component of the CSMA/CA method of medium contention is *virtual carrier sense*. Virtual carrier sense uses a timer mechanism known as the *network allocation vector (NAV)* or the NAV timer. The network allocation vector (NAV) timer maintains a prediction of future traffic on the medium based on Duration value information seen in a previous frame transmission. When an 802.11 radio is not transmitting, it is listening. As shown in Figure 8.11, when the listening radio hears a frame transmission from another station, it looks at the Layer 2 header of the frame and determines whether the *Duration/ID* field contains a Duration value or an ID value. If the field contains a Duration value, the listening station will set its NAV timer to this value. The listening station will then use the NAV as a countdown timer, knowing that the RF medium should be busy until the countdown reaches 0. This process essentially allows the transmitting 802.11 radio to notify the other stations that the medium will be busy for a period of time (the Duration/ID value). The stations that are not transmitting listen and hear the Duration/ID value, set a countdown timer (NAV), and wait until their timer hits 0 before they can contend for the medium and eventually transmit on the medium. A station cannot contend for the medium until its NAV timer is 0, nor can a station transmit on the medium if the NAV timer is set to a nonzero value.

FIGURE 8.11 Virtual carrier-sense



The Duration value can be set from 0 to 32767. Most frames do not approach the limit. If an attacker is not contending for the medium but simply transmitting frames with spoofed Duration/ID field values set near the upper limit, an attack known as the *virtual-carrier attack* will disrupt the WLAN. By selecting a value near the limit such as 29000, the attacker knows that stations are not likely to ignore the spoofed frame. Some stations will ignore values over 30000. The high value used by the attacker will cause stations in the area hearing it to set their NAV timer to that high number. The victims then must count down from that number to zero. Once they reach zero, the stations listen to the medium again, and they hear another spoofed frame from the attacker and reset their NAV timers, thus starting the process all over. In this case, the victim stations would never be allowed access to the medium. The attacker is simply winning the contention for the medium by using spoofed Duration values and causing everyone else to remain idle during the attacker's transmissions.

Most Layer 2 DoS attacks are not doing anything "special." The attackers are merely exploiting the way that 802.11 communications function at Layer 2 to disrupt legitimate traffic. As mentioned earlier, numerous Layer 2 DoS attacks exist such as association floods, reassociation floods, authentication floods, EAPOL floods, and PS-Poll floods. All of these attacks are accomplished by simply editing 802.11 frames and retransmitting them to disrupt Layer 2 communications.

MAC Spoofing

All 802.11 wireless network cards have a physical address known as a *MAC address*. This address is a 12-digit hexadecimal number that is seen in cleartext in the Layer 2 header of 802.11 frames. Wi-Fi vendors provide MAC filtering capabilities on their access points and WLAN controllers. Usually, MAC filters are configured to apply restrictions that will allow traffic only from specific client stations to pass through. These restrictions are based on their unique MAC addresses. All other client stations whose MAC addresses are not on the allowed list will not be able to pass traffic through the virtual port of the access point and onto the distribution system medium.

As you learned in Chapter 2, "Legacy 802.11 Security," MAC addresses can be spoofed, or impersonated, and any amateur hacker can easily bypass any MAC filter by spoofing an allowed client station's address. MAC spoofing can often be achieved in the Windows operating system by simply editing the wireless card's MAC address in Device Manager or by performing a simple edit in the Registry. Third-party software utilities, such as SMAC (described in a moment), can also be used to accomplish MAC spoofing. MAC spoofing renders MAC filters useless as a form of security on wireless networks, since MAC addresses are always visible to anyone on the same channel and in the same area.

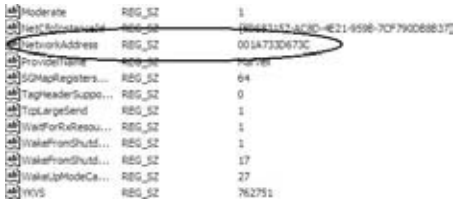
No two devices should ever have the same MAC address configured on them from the manufacturer. The organizationally unique identifier (OUI) address is the first three octets of the MAC address that identifies the manufacturer of the card. The remaining octets of the MAC address are unique and are used to identify the individual card. The existence of two cards with the same MAC address should not happen because vendors are very careful to

avoid this in the manufacturing process, to prevent address conflicts. Attackers, on the other hand, use duplicate MAC addressing to their advantage. By cloning a MAC address an attacker can bypass MAC filters. The filter cannot distinguish between a legitimate device and a spoofed device, thereby allowing them access to spoofed devices. The MAC filter has no way of knowing that more than one device is using the same addressing. Frames from either device—the real one or the attackers—are accepted by the network. Traffic leaving the network bound for either device is transmitted into the air. Both devices receive the frames but only the one expecting it processes the data. This happens because the devices are using different sockets. If the attacker is in close proximity to the cloned device, the attack may go undetected by some WIPS solutions that only use sensor location to trigger a MAC spoof–based alarm. To be able to detect spoofing more efficiently, better WIPS products also look at the sequence numbers of the frames being transmitted by the devices. If they are out of sequence, an alarm can be triggered, alerting a WLAN administrator to the MAC spoofing attack.

One place where a MAC spoofing attack is still used with great effect is at public-access WLAN hotspots. A *MAC piggy-backing* attack is used to circumvent the hotspot captive portal login requirements. The attacker is not trying to break into a network to steal data but rather to exploit the way the hotspot's *captive portal* works to gain free Internet access. Captive portal authentication solutions are usually the only security provided for public-access WLANs and hotspots. Once a station connects to the hotspot SSID and gets an IP address, the user opens their browser. Rather than going to their normal home page, the user is redirected to the captive portal web login page. This page may have a simple terms terms-of-use agreement or may require credentials to access the Internet beyond the captive portal page. The required credentials could be a username and password or credit card information. When the captive portal is satisfied that the user has the correct information to gain Internet access—password, credit card, and so on—the captive portal authentication allows the user access to a gateway to the Internet. The only security beyond this point is a common MAC filter allowing access for users who have authenticated via the captive portal login page. An attacker uses a WLAN protocol analyzer to determine which stations are passing data frames through the AP, indicating the captive portal has approved their MAC addresses to do so. Then the attacker clones the MAC address of a station passing data through the AP onto their wireless card. The attacker can then connect to the AP and pass data as well because the AP and its captive portal believe the attacker is an approved device. MAC piggy-backing is not normally considered a malicious attack, but the attack could be considered as theft of services if the hotspot requires payment for access.

If MAC addresses are designated by the manufacturer of the cards and no two MAC addresses should ever be the same, how are attackers able to change them? Attackers and users alike can change MAC addresses very easily using utilities within the operating system or programs designed to allow this change. As shown in Figure 8.12, changing the MAC address through the OS can be done by directly editing the Registry value for the card's MAC address and rebooting the system. When the system comes back up, the card will be using the new cloned MAC address.

FIGURE 8.12 MAC address Registry settings

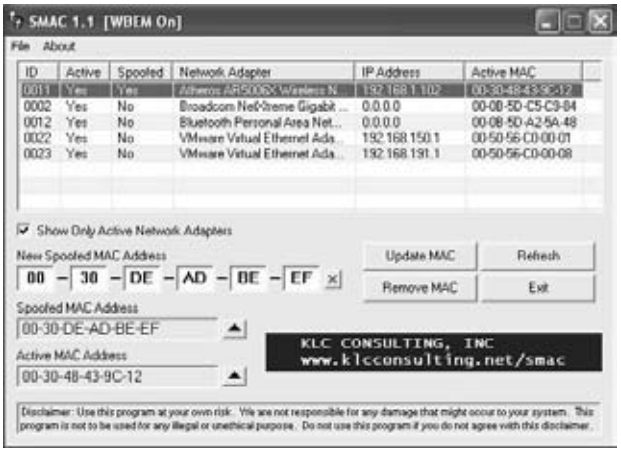


As shown in Figure 8.13, many WLAN cards will allow a change of the MAC address to be made in the GUI without a system reboot. This option is typically found in the Advanced settings of the networking properties of the card's MAC address.

FIGURE 8.13 MAC address: networking settings

If the attacker does not wish to edit the Registry directly and the card they are using does not have the option to configure a locally assigned MAC address, programs are available that will allow the user to change the MAC address despite the other limitations. One such program is SMAC from KLC Consulting. As shown in Figure 8.14, SMAC has the ability to set specific MAC addresses as well as the ability to generate MAC addresses based on known OUI structures from several vendors. It also keeps track of recently used MAC addresses for future use.

FIGURE 8.14 SMAC



Because of spoofing and because of all the administrative work that is involved with setting up MAC filters, MAC filtering is not considered a reliable means of security for wireless enterprise networks and should be implemented only if stronger security is not available.

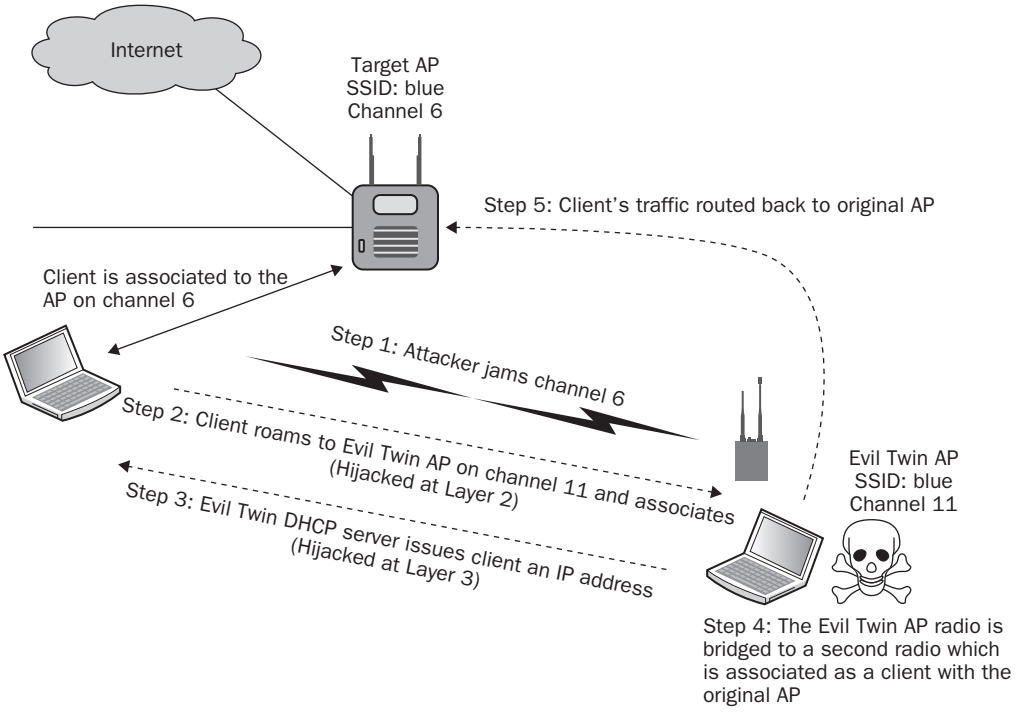
Wireless Hijacking

An attack that often generates a lot of press is *wireless hijacking*, also known as the *evil twin attack*. The attacker configures access point software on a laptop, effectively turning a Wi-Fi client card into an access point. Some small Wi-Fi USB devices also have the ability to operate as an AP. The access point software on the attacker's laptop is configured with the same SSID that is used by a public-access hotspot. The attacker's access point is now functioning as an evil twin AP with the same SSID but is transmitting on a different channel. The attacker then sends spoofed disassociation or deauthentication frames, forcing client stations associated with the hotspot access point to roam to the evil twin access point. At this point, the attacker has effectively hijacked wireless clients at Layer 2 from the original access point. Although deauthentication frames are usually used as one way to start a hijacking attack, RF jammers can also be used to force any clients to roam to an evil twin AP.

The evil twin AP will typically be configured with a Dynamic Host Configuration Protocol (DHCP) server available to issue IP addresses to the clients. At this point, the attacker will have hijacked the client stations at Layer 3. The attacker has a private WLAN network and is free to perform peer-to-peer attacks on any of the hijacked clients. The user's computer could, during the process of connecting to the evil twin, fall victim to the DHCP attack, an attack that exploits the DHCP process to dump root kits or other malware onto the victim's computer in addition to giving them an IP address as expected.

The attacker may also be using a second wireless card with their laptop to execute what is known as a *man-in-the-middle attack*, as shown in Figure 8.15. The second WLAN card is associated with the original access point as a client. In operating systems, networking cards can be bridged together to provide routing. The attacker has bridged together their second wireless card with the Wi-Fi card that is being used as the evil twin access point. After the attacker hijacks the users from the original AP, the traffic is then routed from the evil twin access point through the second Wi-Fi card, right back to the original access point from which the users have just been hijacked. The result is that the users remain hijacked; however, they still have a route back through the gateway to their original network, so they never know they have been hijacked. The attacker can therefore sit in the middle and execute peer-to-peer attacks indefinitely while remaining completely unnoticed.

FIGURE 8.15 Wireless hijacking/man-in-the-middle attack



These attacks can take another form in what is known as the *Wi-Fi phishing attack*. The attacker may also have web server software and captive portal software. After the users have been hijacked to the evil twin access point, they will be redirected to a login web page that looks exactly like the hotspot's login page. Then the attacker's fake login page may request a credit card number from the hijacked user. Phishing attacks are common on the Internet and are now appearing at your local hotspot.

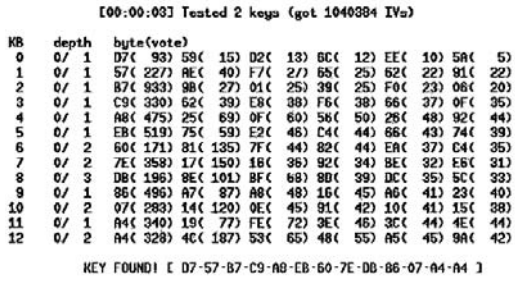
The only way to prevent a hijacking, man-in-the-middle, or Wi-Fi phishing attack is to use a mutual authentication solution. Mutual authentication solutions not only validate the user connecting to the network, but also validate the network to which the user is connecting. 802.1X/EAP authentication solutions require that mutual authentication credentials be exchanged before a user can be authorized. A user cannot get an IP address unless authorized; therefore, users cannot be hijacked.

Encryption Cracking

Encrypting transmitted information is extremely important in wireless communications, since the medium is shared and unbounded. If any degree of data privacy is to be expected, some form of encryption should be used—the stronger, the better. Earlier wireless networks used no encryption at all or they used Wired Equivalent Privacy (WEP) to encrypt the transmissions. As you learned in Chapter 2, WEP is a Layer 2 encryption method that does indeed provide data privacy when encrypting the Layer 3–7 data payload known as the MAC Service Data Unit (MSDU). Unfortunately, WEP has been cracked, and software tools exist that can derive the static WEP key from 802.11 data frame traffic that has been captured using a protocol analyzer. Older WEP cracking software could take days to run because the number of Initialization Vectors (IVs) needed to crack the key is relatively high. WEP uses either a 40-bit secret key or a 104-bit secret key to protect the data. No matter which secret key length is used, 40 bit or 104 bit, WEP only uses a 24-bit IV. If an attacker gathers enough IVs they can crack 64-bit and 128-bit WEP in minutes. An attacker would need to capture about 500,000 IVs to be able to crack the WEP key. In a SOHO environment, this could take weeks of captures. In an enterprise, with a larger traffic volume than SOHO networks, this could still take days.

As shown in Figure 8.16, modern freeware cracking tools can now break through WEP protected frames in a matter of minutes and obtain the static WEP key. Modern cracking tools now use an injection attack that forces devices to generate the IVs much faster than regular traffic requires. The injection attacks often use Address Resolution Protocol (ARP) flooding to force this to happen. Now cracking 128-bit WEP keys can be done in a few minutes versus the days and weeks of older tools that employed large capture files and brute-force attacks. Once an attacker has obtained the WEP key, they can connect to the WLAN and decode the data captured offline or decode data frames in real time.

FIGURE 8.16 Cracked WEP key



Network managers abandoned WEP for newer, more secure dynamic encryption methods. To improve on the security offered by WEP, the Temporal Key Integrity Protocol (TKIP) was developed. TKIP uses 48-bit IVs, time-bound keys, and the RC4 algorithm for an improvement over the security offered by WEP. Although the TKIP encryption method has not yet been cracked, TKIP is not considered a strong means of encryption due to the use of the weaker RC4 algorithm. A better encryption method is dynamic CCMP encryption, which uses the AES algorithm.

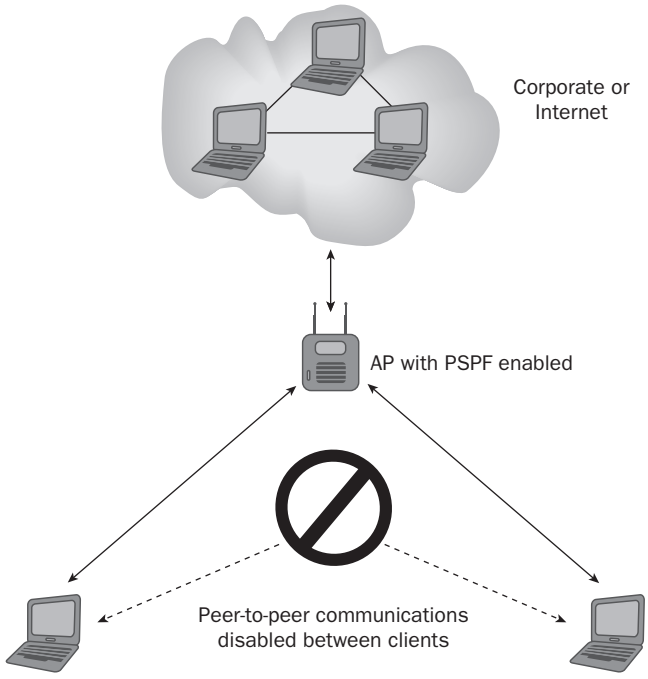
Peer-to-Peer Attacks

A commonly overlooked risk is the *peer-to-peer attack*. As you learned in earlier chapters, an 802.11 client station can be configured in either infrastructure mode or ad hoc mode. When configured in ad hoc mode, the wireless network is known as an independent basic service set (IBSS) and all communications are peer-to-peer without the need for an access point. Because an IBSS is by nature a peer-to-peer connection, any user who can connect wirelessly with another user can gain access to any resource available on either computer. A common use of ad hoc networks is to share files on the fly. If shared access is provided, files and other assets can accidentally be exposed. A personal firewall is often used to mitigate peer-to peer attacks. Some client devices can also disable this feature so that the device will connect only to certain networks and will not associate to a peer-to-peer without approval.

Users that are associated with the same access point are typically just as vulnerable to peer-to-peer attacks as IBSS users. Properly securing your wireless network often involves protecting authorized users from each other, because hacking at companies is often performed internally by employees. Any users associated with the same access point that are members of the same basic service set (BSS), and are in the same VLAN, are susceptible to peer-to-peer attacks because they reside in the same Layer 2 and possibly Layer 3 domains. In most WLAN deployments, Wi-Fi clients communicate only with devices on the wired network, such as email or web servers, and peer-to-peer communications are not needed. Therefore, most vendors provide some proprietary method of preventing users from inadvertently sharing files with other users. If connections are required to other wireless peers, the traffic is routed through a Layer 3 switch or other network device prior to passing to the desired destination station.

Public Secure Packet Forwarding (PSPF) is a feature that can be enabled on WLAN access points or controllers to block wireless clients from communicating with other wireless clients on the same wireless VLAN. This isolates each user on the wireless network to ensure that an 802.11 station cannot be used to gain Layer 2 or Layer 3 access to another 802.11 station. With PSPF enabled, client devices cannot communicate directly with other client devices on the wireless network, as shown in Figure 8.17.

FIGURE 8.17 Peer-to-peer connectivity disabled



Although PSPF is a proprietary term most commonly used by Cisco, other vendors offer similar capabilities under different names such as *peer blocking*. It should be noted that some applications require peer-to-peer connectivity. Many VoWiFi phones offer "push-to-talk" capabilities that use multicasting. VoWiFi phones are typically segmented in a separate wireless VLAN from the rest of wireless data clients. Peer-to-peer blocking should not be enabled in the voice VLAN if push-to-talk multicasting is required.

Management Interface Exploits

One of the main goals of attackers is to gain access to administrative accounts or root privilege. Once they gain that access, they can run several attacks against networks and individual devices. On wired networks these attacks are launched against firewalls, servers, and infrastructure devices. In wireless attacks, these are first launched against access points or WLAN controllers and subsequently against the same targets as in wired attacks. Wireless infrastructure hardware such as autonomous access points and WLAN controllers

can be managed by administrators via a variety of interfaces, much like managing wired infrastructure hardware. Devices can typically be accessed via a web interface, a command-line interface, a serial port, a console connection, and/or Simple Network Management Protocol (SNMP). It is imperative that these interfaces be protected. Interfaces that are not used should be disabled. Strong passwords should be used, and encrypted login capabilities such as Hypertext Transfer Protocol Secure (HTTPS) should be utilized if available.

Lists of all the default settings of every major manufacturer's access points exist on the Internet and are often used for security exploits by hackers. It is not uncommon for intruders to use security holes left in management interfaces to reconfigure access points. Legitimate users and administrators can find themselves locked out of their own wireless networking equipment. After gaining access via a management interface, an attacker might even be able to initiate a firmware upgrade of the wireless hardware and, while the upgrade is being performed, power off the equipment. This attack could likely render the hardware useless, requiring it to be returned to the manufacturer for repair.

Many WLAN devices often have settings that allow for remote administration via the Internet. Although these settings are intended for legitimate administrators, an attacker may use remote access to management interfaces to perform the same attacks just described. Remote access should either be turned off or locked down tight.

Policy should dictate that all WLAN infrastructure devices be configured from only the wired side of the network. If an administrator attempts to configure a WLAN device while connected wirelessly, the administrator could lose connectivity due to configuration changes being made.

Vendor Proprietary Attacks

Hackers often find holes in the firmware code used by specific WLAN autonomous access points and WLAN controller vendors. Most of these vendor-specific exploits are in the form of buffer overflow attacks. When these vendor-specific attacks become known, the WLAN vendor usually makes a firmware fix available in a timely manner. These attacks can be best avoided by staying informed through your WLAN vendor's support services.

New WLAN vulnerabilities and attacks are discovered on a regular basis including vendor proprietary attacks. For example, WLAN security company, AirMagnet, recently discovered a vulnerability with Cisco Networks' Over-The-Air-Provisioning (OTAP) protocol. OTAP allows newly deployed Cisco APs to listen for multicast traffic from other nearby Cisco APs and use the information to find a Cisco WLAN controller. The newly deployed AP could potentially hear multicast traffic from a neighboring WLAN and incorrectly attach to an incorrect controller. An attacker could also intentionally hijack an AP. *SkyJack* is the name given to this over-the-air exploit by AirMagnet. Although the SkyJack exploit of Cisco's OTAP protocol has received a lot of press, it should be understood that vulnerabilities are discovered in all WLAN vendors' solutions. Once the exploits are discovered, the affected WLAN vendor will make safeguard recommendations on how to avoid the exploit. In most cases the WLAN vendor will release a patch that can fix the problem. More information about the SkyJack exploit can be found at `www.airmagnet.com/assets/AM_Technote_SkyJack_082509`. Cisco's safeguard

recommendations for the SkyJack exploit can be found at `http://tools.cisco.com/security/center/viewAlert.x?alertId=18919`.

Physical Damage and Theft

An important aspect of the installation of wireless equipment is the "pretty factor." The majority of businesses prefer that all wireless hardware remain completely out of sight. Aesthetics is extremely important in retail environments and in the hospitality industry (restaurants and hotels). Any business that is dealing with the public will require that the Wi-Fi hardware be hidden or at least secured. Many vendors are designing more aesthetic-looking access points and antennas. Some vendors have even camouflaged access points to resemble smoke detectors. Indoor enclosures that mounted in place of ceiling tiles are also often used to conceal access points. It should also be noted that most enclosure units can be locked to help prevent physical damage or theft of expensive Wi-Fi hardware.

Client devices such as VoWiFi phones and WLAN barcode scanners are often easily stolen. Several companies such as AeroScout and Ekahau provide a WLAN *real-time location system (RTLS)*, which can track the location of any 802.11 radio device as well as active Wi-Fi RFID tags with great accuracy. The components of an overlay WLAN RTLS solution include the preexisting WLAN infrastructure, preexisting WLAN clients, Wi-Fi RFID tags, and an RTLS server. Additional RTLS WLAN sensors can also be added to supplement the preexisting WLAN APs.

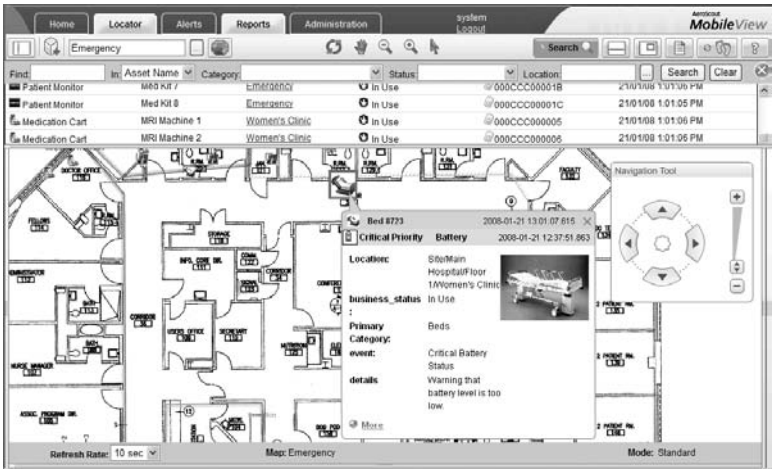
Active RFID tags and/or standard Wi-Fi devices transmit a brief signal at a regular interval, adding status or sensor data if appropriate. Figure 8.18 shows an active RFID tag attached to a hospital IV pump. The signal is received by standard wireless APs (or RTLS sensors), without any infrastructure changes needed, and is sent to a processing engine that resides in the RTLS server at the core of the network. The RTLS server uses signal strength and/or time-of-arrival algorithms to determine location coordinates.

FIGURE 8.18 Active 802.11 RFID tag

Courtesy of AeroScout

As pictured in Figure 8.19, a software application interface is then used to see location and status data on a display map of the building's floor plan. The RTLS application can be used to define zones on the floor plan that will trigger alarms if client devices or RFID tags leave a certain area or zone. An RTLS solution can greatly reduce theft of WLAN devices as well as any company assets with an attached RFID tag.

FIGURE 8.19 RTLS application



Courtesy of AeroScout

Social Engineering

Social engineering or "hacking the user" is a very real threat to all networks. Social engineering involves getting users to reveal information without knowing they have done so. It also may involve gaining information from public sources such as the target's website or corporate reports. Another effective social engineering attack is dumpster diving—going through the target's trash looking for information. This once was a big problem for credit cards. Retailers used carbon papers and physical imprints of the customer's card as part of the transaction. The carbon papers would be discarded by the clerks and later deposited in common garbage dumpsters. People wanting to use the credit card numbers of others would go through the trash in the dumpster to find the carbon papers and thus the credit card numbers.

Phishing is also a social engineering attack. Phishing is a criminal process used to acquire sensitive information fraudulently, such as usernames, passwords, and credit card information, by masquerading as a valid authority during electronic communication. Many of us have gotten the infamous email "I am in another country and need help getting my millions out, and I will share the money with you for your help." Perhaps you received the email from a bank or government office asking for your personal information or bank

account numbers. Why do these obvious junk emails, phone calls, and letters continue to be sent? These scams continue because some unfortunate people respond to them, giving the criminals the information or money they desire. The Wi-Fi phishing attack discussed earlier in this chapter uses wireless hijacking techniques and a bogus captive portal to perpetrate a similar scam.

Computer network users sometimes are even more careless with corporate information and device security. People are often more concerned with ease of use than they are with security. Users will often keep the same simple passwords for months or years. Their passwords can be found written on sticky notes under their keyboards or stuck to their monitors. No matter how much money is spent on security equipment and software or even on security guards, users still may carelessly or unwittingly give attackers information that will compromise security measures. For example, a call can be placed to users stating that the caller is from the IT security team. The caller may tell the user that some unapproved software or freeware that is not allowed has been detected on their machine. The caller tells the user they want to help the user become compliant with corporate policy and, that by giving them their username and password, the caller will be able to remove the suspicious software from their machine without the caller having to report it as a policy violation to the user's manager. Desperate to avoid trouble, users usually comply with the attacker's requests.

Users cannot all be trained security professionals. How can we train our users to be more security conscious as they travel with company laptops? We can train them to make sure their personal firewalls are always on and that their antivirus software is up to date and running, and to recognize social engineering attacks and report them to corporate security teams as soon as possible.

A variant of these attacks is called reverse social engineering. This is a process by which an attacker poses as someone in authority and gives the user bogus information rather than trying to get information from the user. The users are almost always the weakest link in network security.

Real World Scenario

Social Engineering and Chocolate

In 2004 a survey was conducted in London in the Liverpool Street Station. The survey (`http://news.bbc.co.uk/2/hi/technology/3639679.stm`) found that commuters were willing to share their passwords with strangers conducting the survey in exchange for a piece of candy. A whopping 34 percent revealed their passwords when asked if it had something to do with a pet or child's name. A second survey revealed that 79 percent of those questioned gave away personal information without even knowing what they were exposing when questioned by "survey takers."

Public Access and WLAN Hotspots

When you are using the WLAN at an Internet cafe, coffee shop, airport, hotel, and other public WLAN hotspots, you are not as protected as you are as when you are using your organization's WLAN where security measures have been taken to protect your wireless communications. Hotspots are often breeding grounds for peer-to-peer attacks, viruses, hijacking, data theft or manipulation, eavesdropping attacks, and other malicious events.

So what makes these convenient connections so vulnerable to attacks? There is no real security provided by the hotspot's host. The hotspots may be using a captive portal requiring users to agree to the terms of use statement prior to granting the connection. Captive portal authentication is considered to be a weak authentication method but is normally adequate for simply authorizing users to access a gateway to the Internet. However, public-access WLANs do not offer an encryption solution. All 802.11 data frames are therefore unencrypted and susceptible to malicious eavesdropping attacks. The hotspots may have been set up by a contractor that doesn't monitor it after installation.

Hotspots do not deploy wireless intrusion prevention systems (WIPS) to protect users either. Thus there is also no security monitoring of the insecure WLAN connectivity. The vast majority of hotspots users are not security conscious as they travel, making them vulnerable to attack as well.

Knowing that hotspots are the "wild west of Wi-Fi," we can implement a remote access policy for all corporate employees who access hotspots and other noncorporate Wi-Fi networks. End users will be taking their laptops and handheld devices off site and away from company grounds. Most users will likely use wireless networks at home and at wireless hotspots to access the Internet. By design, many of these remote wireless networks have absolutely no security in place, and it is imperative that a remote access WLAN policy be strictly enforced. This policy should include the required use of an IPsec VPN solution to provide device authentication, user authentication, and strong encryption of all wireless data traffic. Hotspots are prime targets for malicious eavesdropping attacks.

Personal firewalls should also be installed on all remote computers to prevent peer-to-peer attacks. Personal firewalls will not prevent hijacking attacks or peer-to-peer attacks, but will prevent attackers from accessing most critical information. Endpoint WLAN policy enforcement software solutions exist that force end users to use VPN and firewall security when accessing any wireless network other than the corporate WLAN. The remote access policy is mandatory because the most likely and vulnerable location for an attack to occur is at a public-access hotspots.

Summary

Due to the unbounded functionality of wireless networking exposing Layers 1 and 2 to anyone within listening range and on the same frequency, there are many more risks involved in its use than found in traditional bounded networking. Strong security measures exist for WLAN communications that should be employed to mitigate the risks involved in 802.11 communications. WLAN administrators should have a thorough understanding of all of the WLAN security risks and potential attacks. Thorough comprehension of all WLAN threats will ultimately result in the better decisions when choosing 802.11 security solutions for the enterprise.

Exam Essentials

Understand the risk of the rogue access point. Be able to explain why the rogue AP and other rogue devices provide a portal into network resources. Understand that hackers are usually not the source of rogue devices.

Define peer-to-peer attacks. Understand that peer-to-peer attacks can happen via an AP or through an ad hoc network. Explain how to defend against the attack.

Know the risks of eavesdropping. Explain the difference between casual and malicious eavesdropping. Explain why encryption is needed for protection.

Define authentication and hijacking attacks. Explain the risks behind these attacks. Understand that a strong 802.1X/EAP solution is needed to mitigate these attacks.

Explain wireless denial of service attacks. Know the difference between Layer 1 and Layer 2 DoS attacks. Explain why these attacks cannot be mitigated and can only be monitored.

Understand management interface exploits. Explain the reasons for hardening the WLAN infrastructure for authorized and secure administration only.

Understand the concept of social engineering. Know that end users are always the weakest link in WLAN security. Explain why end users need to be trained to recognize social engineering attacks. Understand that any type of static password, passphrase, or shared encryption key is always susceptible to a social engineering attack.

Key Terms

Before you take the exam, be certain you are familiar with the following terms:

active scanning

association flood

brute force dictionary attack

captive portal

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

casual eavesdropping

Cisco Discovery Protocol (CDP)

classification

deauthentication

Denial of service (DoS)

direct sequencing spread spectrum (DSSS)

disassociation

Distributed Spectrum Analysis System (DSAS)

Duration/ID

evil twin attack

FakeAP

Faraday cage

frequency hopping spread spectrum (FHSS)

illegal channel beaconing

independent basic service set (IBSS)

injection attack

Intentional interference

Lightweight Extensible Authentication Protocol (LEAP)

MAC piggy-backing

MAC Service Data Unit (MSDU)

malicious eavesdropping

management frame protection (MFP)

man-in-the-middle attack

NetStumbler

network allocation vector (NAV)

null probe request

offline dictionary attack

orthogonal frequency division multiplexing (OFDM)

passive scanning

peer blocking

peer-to-peer attack

port suppression

preshared keys

probe response flood

protocol analyzer

Public Secure Packet Forwarding (PSPF)

Queensland Attack

rogue access point

rogue containment

rogue device

Simple Network Management Protocol (SNMP)

spectrum analyzer

Unintentional interference

virtual carrier sense

virtual-carrier attack

wardialing

Wi-Fi phishing attack

Wired leakage

wireless hijacking

wireless intrusion detection system (WIDS)

wireless intrusion prevention system (WIPS

WLAN discovery tools

Review Questions

1. When an attacker passively captures and examines wireless frames from a victim's network, what type of attack is taking place?
   - **A.** Injection
   - **B.** Data destruction
   - **C.** Frame manipulation
   - **D.** Man in the middle
   - **E.** Eavesdropping

2. Which of these attacks are considered denial-of-service attacks? (Choose all that apply.)
   - **A.** Man-in-the-middle
   - **B.** Jamming
   - **C.** Deauthentication spoofing
   - **D.** MAC spoofing
   - **E.** Peer-to-peer

3. The majority of rogue devices are placed by whom? (Choose all that apply.)
   - **A.** Attackers
   - **B.** Wardrivers
   - **C.** Employees
   - **D.** Contractors
   - **E.** Visitors

4. Which of these attacks would be typically associated with malicious eavesdropping? (Choose all that apply.)
   - **A.** NetStumbler
   - **B.** Peer-to-peer
   - **C.** Protocol analyzer capture
   - **D.** Packet reconstruction
   - **E.** PS polling attack

5. What are some of the risks if a rogue device goes undetected?
   - **A.** Data theft
   - **B.** Data destruction
   - **C.** Loss of network services
   - **D.** Data insertion
   - **E.** Third-party attacks
   - **F.** All of the above

6. Which of these can cause unintentional RF jamming attacks against an 802.11 wireless network? (Choose all that apply.)
   - **A.** Microwave oven
   - **B.** Signal generator
   - **C.** 2.4 GHz cordless phones
   - **D.** 900 MHz cordless phones
   - **E.** Deauthentication transmitter

7. Which of these attacks are wireless users susceptible to at a public-access hotspot? (Choose all that apply.)
   - **A.** Wi-Fi phishing
   - **B.** Happy AP attack
   - **C.** Peer-to-peer attack
   - **D.** Malicious eavesdropping
   - **E.** 802.11 reverse ARP attack
   - **F.** Man-in-the-middle
   - **G.** Wireless hijacking

8. Which of these encryption technologies have been cracked? (Choose all that apply.)
   - **A.** 64-bit WEP
   - **B.** TKIP/RC4
   - **C.** CCMP/AES
   - **D.** 128-bit WEP
   - **E.** Wired Equivalent Privacy

9. Which of these attacks are considered Layer 2 denial-of-service attacks? (Choose all that apply.)
   - **A.** Deauthentication spoofing
   - **B.** Jamming
   - **C.** Virtual carrier attacks
   - **D.** PS-Poll floods
   - **E.** Authentication floods

10. What type of security solution can be used to prevent rogue WLAN devices from becoming an unauthorized portal to a wired network infrastructure? (Choose all that apply.)
    - **A.** 802.1X/EAP
    - **B.** Port control
    - **C.** WIPS
    - **D.** TKIP/RC4
    - **E.** WINS

11. What can happen when an intruder compromises the preshared key used during WPA/WPA2-Personal authentication? (Choose all that apply.)

- **A.** Decryption
- **B.** Eavesdropping
- **C.** Spoofing
- **D.** Encryption cracking
- **E.** Access to network resources

12. What is another name for a wireless hijacking attack?

- **A.** Wi-Fi phishing
- **B.** Man-in-the-middle
- **C.** Fake AP
- **D.** Evil twin
- **E.** AirSpy

13. Tammy has been brought in as a consultant to design a WLAN. The customer is concerned that the users will try to hack into each other's laptops over the WLAN. The customer also requires strong security and will be using a VoWiFi solution. What are some of the recommendations that Tammy should make to meet the customers concerns and requirements? (Choose all that apply.)

- **A.** Create a WLAN profile and separate VLAN for the laptops using WPA2-Enterprise security and another WLAN profile for the VoWiFi phones using WPA2-Personal security.
- **B.** Enable station-to-station traffic blocking for all WLAN profiles and VLANs.
- **C.** Enable station-to-station traffic blocking only for the laptop WLAN profile and VLAN.
- **D.** Enable station-to-station traffic blocking only for the VoWiFi phone WLAN profile and VLAN.
- **E.** Create a WLAN profile and separate VLAN for the VoWiFi phones using WPA2-Enterprise security and another WLAN profile for the laptops using WPA2-Personal security.

14. Which components of Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) can be compromised by a denial-of-service attack? (Choose all that apply.)

- **A.** NAV timer
- **B.** Interframe spacing
- **C.** Clear channel assessment
- **D.** Random backoff timer

15. What security can be used to stop attackers from seeing the MAC addresses used by your legitimate 802.11 WLAN devices?

- **A.** MAC spoofing
- **B.** VPN tunneling
- **C.** CCMP/AES encryption
- **D.** Use 802.1X authentication
- **E.** None of the above

16. Wired leakage occurs under which of the following circumstances?
    A. When weak wireless encryption is used
    B. When weak wireless authentication is used
    C. When wired broadcast traffic is passed through an AP
    D. When wired unicast traffic is passed through an AP
    E. When the protection mode is disabled on an AP

17. Which of these attacks can be mitigated with a mutual authentication solution? (Choose all that apply.)
    A. Malicious eavesdropping
    B. Deauthentication
    C. Man-in-the-middle
    D. Wireless hijacking
    E. Authentication flood

18. Wireless intrusion prevention systems (WIPSs) are unable to detect which of the following attacks?
    A. Association flood
    B. Malicious eavesdropping
    C. Management frame fuzzing
    D. Injection attacks
    E. Null probe attacks

19. Name two types of rogue devices that cannot be detected by a Layer 2 wireless intrusion prevention system (WIPS).
    A. 900 MHz radio
    B. 802.11h-compliant device
    C. FHSS radio
    D. 802.11b routers
    E. 802.11g mixed-mode device

20. What type of solution can be used to perform countermeasures against a rogue access point?
    A. WPA-Enterprise
    B. 802.1X/EAP
    C. WIPS
    D. TKIP/RC4
    E. WINS

Answers to Review Questions

1. E. Eavesdropping is unauthorized passive capturing of data, often conducted with packet analyzing software. The other attacks listed are active attacks that would be detectable and may interrupt traffic flow. Because eavesdropping is a passive attack, it will be undetected by a WIDS/WIPS solution.

2. B, C. DoS attacks can occur at either Layer 1 or Layer 2 of the OSI model. Layer 1 attacks are known as RF jamming attacks. A wide variety of Layer 2 DoS attacks exist that are a result of tampering with 802.11 frames, including the spoofing of deauthentication frames.

3. C, D, E. The majority of unauthorized devices placed on networks, rogues, are placed there by people with access to the building. This means that they are more often placed by people you trust: employees, contractors, and visitors. Wardrivers and attackers are not usually allowed physical access.

4. C, D. Malicious eavesdropping is achieved with the unauthorized use of protocol analyzers to capture wireless communications. Any unencrypted 802.11 frame transmission can be reassembled at the upper layers of the OSI model.

5. F. Because rogue devices are unauthorized WLAN portals, all of your network resources are potentially exposed. Any data stored on network servers or desktop workstations is entirely at risk. Data theft is usually the most common risk associated with rogue access. Destruction of data can also occur. Databases can be erased and drives can be reformatted. Network services can also be disabled. An attacker can use the unauthorized portal for malicious data insertion and upload viruses and pornography. Remote control applications and keystroke loggers can also be uploaded to network resources and used to gather information at a later date. Attackers have been known to upload illegally copied software and set up illegal FTP servers to distribute the illegal software. Once an attacker has accomplished rogue access, a wired network can be used as a launching pad for third-party attacks against other networks across the Internet.

6. A, C. Microwave ovens operate in the 2.4 GHz ISM band and are often a source of unintentional interference. 2.4 GHz cordless phones can also cause unintentional jamming. A signal generator is typically going to be used as a jamming device, which would be considered intentional jamming. 900 MHz cordless phones will not interfere with 802.11 equipment that operates in either the 2.4 GHz ISM band or the 5 GHz UNII bands. There is no such thing as a deauthentication transmitter.

7. A, C, D, F, G. Currently, there is no such thing as a Happy AP attack or an 802.11 reverse ARP attack. Wireless users are especially vulnerable to attacks at public-use hotspot because there is no security. Because no encryption is used, the wireless users are vulnerable to malicious eavesdropping. Because no mutual authentication solution is in place, they are vulnerable to hijacking, man-in-the-middle, and phishing attacks. The hotspot access point might also be allowing peer-to-peer communications, making the users vulnerable to peer-to-peer attacks. Every company should have a remote-access wireless security policy to protect their end users when they leave company grounds.

8. A, D, E. Wired Equivalent Privacy (WEP) encryption has been cracked, and currently available tools may be able to derive the secret key within a matter of minutes. The size of the key makes no difference, and both 64-bit WEP and 128-bit WEP can be cracked. TKIP/RC4 and CCMP/AES encryption have not been cracked.

9. A, C, D, E. Numerous types of Layer 2 DoS attacks exist, including association floods, deauthentication spoofing, disassociation spoofing, authentication floods, PS-Poll floods, and virtual carrier attacks. RF jamming is a Layer 1 DoS attack.

10. A, B. The best way of preventing rogue access is wired port control. An 802.1X/EAP can be used to authorize access through wired ports on an access layer switch. EAP-MD5 and EAP-TLS can be used for wired 802.1 X/EAP authentication to control wired-side access. Unless proper credentials are presented at Layer 2, upper-layer communications are not possible through the wired port. A rogue device cannot act as a wireless portal to network resources if the rogue device is plugged into a managed port that is blocking upper-layer traffic. Therefore, a wired 802.1X/EAP solution is an excellent method of preventing rogue access.

11. A, E. After obtaining the passphrase, an attacker can also associate with the WPA/WPA2 access point and thereby access network resources. The encryption technology is not cracked, but the key can be re-created. If a hacker has the passphrase and captures the 4-Way Handshake, they can re-create the dynamic encryption keys and therefore decrypt traffic. WPA/WPA2-Personal is not considered a strong security solution for the enterprise because if the passphrase is compromised, the attacker can access network resources and decrypt traffic.

12. D. An attack that often generates a lot of press is wireless hijacking, also known as the evil twin attack. The attacker hijacks wireless clients at Layer 2 and Layer 3 by using an evil twin access point and a DHCP server. The hacker may take the attack several steps further and initiate a man-in-the-middle attack and/or a Wi-Fi phishing attack.

13. A, C. Users that are associated with the same access point are vulnerable to peer-to-peer attacks. Most WLAN vendors offer a feature on autonomous access points or WLAN controllers to block wireless clients from communicating with other wireless clients on the same wireless VLAN. This isolates each user on the wireless network to ensure that a wireless station cannot be used to gain Layer 2 or Layer 3 access to another wireless station. This is a highly recommend security practice unless applications require peer-to-peer connectivity. Many VoWiFi phones offer "push-to-talk" capabilities that use multicasting. VoWiFi phones are normally segmented in a separate wireless VLAN from the rest of the wireless data clients. Peer-to-peer blocking should not be enabled in the VoWiFi VLAN if push-to-talk multicasting is required. WPA2-Enterprise requires the use of an 802.1X/EAP solution while WPA2-Personal defines the use of a passphrase or pre-shared key for authentication. In most cases an 802.1X EAP solution is the best choice for security, but WPA2-Personal is usually deployed for security with VoWiFi phones due to the latency issues caused by 802.1X/EAP when roaming.

14. A, C. 802.11 uses a medium contention process called Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). To ensure that only one radio card is transmitting on the half-duplex RF medium, CSMA/CA uses four checks and balances. The four checks and balances are virtual carrier sense, physical carrier sense, the random backoff timer, and interframe spacing. Virtual carrier sense uses a timer mechanism known as the network allocation vector (NAV) timer. Physical carrier sense uses a mechanism called the clear channel assessment (CCA) to determine whether the medium is busy before transmitting. Virtual carrier sense is susceptible to a Layer 2 DoS attack when an attacker manipulates the duration value of 802.11 frames. Physical carrier sense is susceptible to a Layer 1 DoS attack when there is a continuous transmitter on the frequency channel.

15. E. Even with the best authentication and encryption in place, attackers can still see MAC address information in clear text. MAC addresses are needed to direct traffic at Layer 2.

16. C. Wired leakage often occurs when wired stations, servers, or infrastructure devices use a broadcast protocol to communicate or to find other devices with which to replicate. Access points will forward wired broadcast and multicast traffic into the air, since on a certain level APs are media converters going to and from wired and wireless mediums. Layer 2 discovery protocols such as the Cisco Discovery Protocol (CDP) will reveal information about the wired network as well as what can already be seen wirelessly.

17. C, D. The only way to prevent a wireless hijacking, man-in-the-middle, and/or Wi-Fi phishing attack is to use a mutual authentication solution. 802.1X/EAP authentication solutions require that mutual authentication credentials be exchanged before a user can be authorized.

18. B. A malicious eavesdropping attack uses a protocol analyzer for unauthorized capture and viewing of 802.11 frames. A protocol analyzer uses an 802.11 radio to listen passively to 802.11 communications. A protocol analyzer does not transmit and will therefore go undetected by a WIPS solution and no alarms will be triggered.

19. A, C. The radio cards inside the WIPS sensors monitor the 2.4 GHz ISM band and the 5 GHz UNII bands. Older legacy wireless networking equipment exists that transmits in the 900 MHz ISM band, and these devices will not be detected. The radio cards inside the WIPS sensors also use only DSSS and OFDM technologies. Wireless networking equipment exists that uses frequency hopping spread spectrum (FHSS) transmissions in the 2.4 GHz ISM band and will go undetected. The only tool that can detect either a 900 MHz or frequency hopping rogue access point is a spectrum analyzer.

20. C. A wireless intrusion prevention system (WIPS) is capable of mitigating attacks from rogue access points. A WIPS sensor can use Layer 2 DoS attacks as a countermeasure against a rogue device. SNMP may be used to shut down ports to which a rogue AP has been connected. WIPS vendors also use unpublished methods for mitigating rogue attacks.

Chapter 9

Wireless LAN Security Auditing

IN THIS CHAPTER, YOU WILL LEARN ABOUT THE FOLLOWING:

- ✓ **WLAN security audit**
  - OSI Layer 1 audit
  - OSI Layer 2 audit
  - Penetration testing
  - Wired infrastructure audit
  - Social engineering audit
  - WIPS audit
  - Documenting the audit
  - Audit recommendations
- ✓ **WLAN security auditing tools**
  - Linux-based tools
  - Windows-based tools

The diligent practice of WLAN security auditing is just as important to a healthy network as good planning and performance tuning, but is often overlooked due to budgetary and time constraints. When building an 802.11 WLAN, you focus a lot of attention on the users, the intended use of the network, the devices used, channels, application support, security measures, signal strength, and bandwidth utilization. Although often overlooked in the past, proper planning and deployment of 802.11 WLAN security infrastructure should be considered mandatory. Over time, the network utilization and coverage can change, along with the number of users and the applications being used. In addition, the equipment deployed as well as the industry standards and government regulations that apply to the use of wireless communications may evolve.

These changes may directly affect the security posture of the WLAN. The users of a WLAN will often complain if the network becomes "slow" or "unavailable," but will not complain about security holes because they do not know how to look for them. Users only care about their ability to access resources and do their jobs. Security holes, such as weak keys, unencrypted traffic, or rogue devices, do not concern the average user as long as their work is not impeded. Improperly configured security settings may reduce the usability of the network or allow attackers access to private information. While end users serve as a network performance monitor of sorts, there is no such built-in user monitoring for WLAN security mechanisms. Security is sometimes considered a luxury or an undesired expense until there is a breach that costs an organization a lot of time or money. Furthermore, if a WLAN security breach becomes public news, the organization faces embarrassment, potential loss of stock values, and potential legal liabilities.

In this chapter, you will learn about recommended WLAN audit procedures as well as the hardware and software tools needed to carry out a successful audit with the goal of creating a more secure wireless network.

WLAN Security Audit

Security does not make a computer network function, nor does it create a profit for an organization. However, without correctly implemented security, profitability and confidential information are in grave danger. WLAN security audits must be conducted on a regular basis. Audits should also be conducted after any change is made to the WLAN infrastructure in order to ensure that the WLAN is not vulnerable to attacks because of the

changes that were made. Regularly scheduled internal audits are a recommended practice. Larger organizations should also consider hiring a third party for an outside WLAN security audit. When a different set of eyes examines a WLAN during an audit, potential vulnerabilities missed by the internal auditor are often exposed. A security audit should also be used to verify that the WLAN is still meeting security requirements that are often set by industry standards, government regulations, and organizational policies.

In most countries, there are mandated regulations on how to protect and secure data communications within all government agencies. Legislation also often exists for protecting information and communications in certain industries. Various industry standards and U.S. government regulations will be discussed in greater detail in Chapter 13, "Wireless Security Policies."

A series of evaluation procedures will normally comprise a typical WLAN security audit. These auditing best practices include the following:

- Layer 1 audit
- Layer 2 audit
- Penetration testing
- Wired infrastructure audit
- Social engineering audit
- WIPS audit

The physical security and inventory of the deployed WLAN devices should also be audited and documented. If you do not have physical security for the devices, what real security do you have? Wired infrastructure devices are usually locked in server rooms. However, WLAN devices, such as access points and antennas, are often exposed to the naked eye. Physical inspection of devices and cabling is part of a complete WLAN audit. Improperly secured APs are susceptible to theft. It is not uncommon for expensive WLAN devices to have been replaced with low-cost clones purchased from Internet auction sites. Some APs have a console or serial port. An attacker may access the exposed ports of an unsecured AP to extract information about WLAN configuration settings.

A good audit also includes proper documentation as well as the final recommendations to make the WLAN more secure. Security auditing is a method of *threat assessment* with the eventual goal of *risk mitigation*. Any security threats and risks that are found will be presented to the WLAN network owner together with an assessment of their impact and often with a proposal for mitigation. Recommended technical and nontechnical solutions will be part of a final proposal.

Which Term Is Correct? Packets or Frames? Analyzer or Sniffer?

The terminology used during WLAN security audits can often be confusing. A packet and a frame are both packages of data that traverse through a computer network. A packet exists at Layer 3 of the OSI model, whereas a frame exists at Layer 2 of the model. As mentioned earlier in this book, the Layer 3–7 payload, known as the MAC Service Data Unit (MSDU), is essentially an IP packet encapsulated in the body of an 802.11 data frame. Although packets operate at Layer 3 and frames operate at Layer 2 of the OSI model, the terms are often used interchangeably. For example, the term 802.11 packet generator actually refers to a software tool used to generate and transmit 802.11 frames. WLAN protocol analyzers are often referred to as WLAN packet analyzers. The phrase "wireless packet capture" is more commonly used as opposed to the technically correct phrase "wireless frame capture" or "802.11 frame capture." In reality a WLAN protocol analyzer captures 802.11 frames, and most of the troubleshooting and analysis is that of Layer 2 frame exchanges. The IP packet payload can only be analyzed if an 802.11 data frame can be decrypted. WLAN protocol analyzers are also often referred to as "wireless sniffers." Although the term sniffer is commonplace, it should be noted that Sniffer® is a registered trademark of Network General Corporation much like Band-Aid® is a registered trademark for the Johnson & Johnson Consumer Companies.

OSI Layer 1 Audit

WLAN site surveys have changed dramatically over the years. When most individuals are asked to define a wireless site survey, the usual response is that a site survey is for determining RF coverage. Although that definition is absolutely correct, the site survey encompasses so much more, including looking for potential sources of RF interference. Before conducting the coverage analysis site survey, a *spectrum analysis* site survey should be considered mandatory for locating sources of potential interference.

Unfortunately, many site surveys completely ignore spectrum analysis because of the high cost generally associated with purchasing the necessary spectrum analyzer hardware. Spectrum analyzers are frequency domain measurement devices that can measure the amplitude and frequency space of electromagnetic signals. Spectrum analyzer hardware can cost upward of $40,000 (U.S. dollars), thereby making them cost-prohibitive for many smaller and medium-sized businesses. The good news is that several companies have solutions, both hardware and software based, that are designed specifically for 802.11 site survey spectrum analysis and are drastically less expensive.

So what does the spectrum analysis during a site survey have to do with a Layer 1 security audit? Effectively the methods and tools used during both procedures is exactly the same. Spectrum analysis during a site survey is usually for performance reasons, while spectrum analysis during a security audit is to identify potential devices that will cause a

Layer 1 *denial of service (DoS)*. The original site survey is executed prior to deployment and installation of the WLAN infrastructure. The spectrum analysis portion of the survey is performed only one time, and it can be for both performance and security evaluation. Layer 1 security audits are enacted on a regularly scheduled basis after the WLAN infrastructure is already operational.

The main purpose of spectrum analysis during a WLAN site survey is to locate the potential sources of interference that may affect the performance of the WLAN. As you learned in Chapter 8, most RF interference is unintentional. Video cameras, baby monitors, cordless phones, and microwave ovens are all potential sources of unintentional interference. Unintentional interference will result in data corruption and Layer 2 retransmissions that negatively affect WLAN performance.

The main purpose of spectrum analysis during a security audit is to identify any devices that can cause a DoS at Layer 1. Any continuous transmitter will cause a DoS. RF jamming devices can be used by an attacker to cause an intentional Layer 1 DoS attack. Denial of service at Layer 1 usually occurs as an unintentional result of transmissions from non-802.11 devices. Video cameras, baby monitors, cordless phones, and microwave ovens are all potential sources of unintentional interference. Unintentional interference may cause a continuous DoS; however, the disruption of service is often sporadic. This disruption of service will upset the performance of Wi-Fi networks used for data applications but can completely disrupt VoWiFi communications within a WLAN. The majority of unintentional interfering devices transmit in the 2.4 GHz ISM frequency band. The 5 GHz UNII bands are less susceptible to unintentional interference.

The 2.4 to 2.4835 GHz ISM band is an extremely crowded frequency space. The following are potential sources of unintentional interference in the 2.4 GHz ISM band:

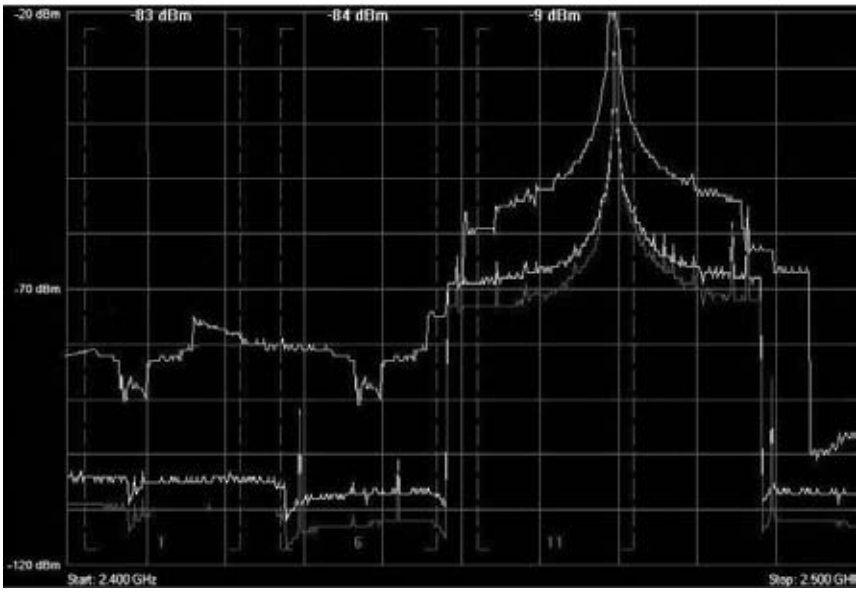
- Microwave ovens
- 2.4 GHz cordless phones, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS)
- Halogen gas lights
- 2.4 GHz video cameras
- Elevator motors
- Cauterizing devices
- Plasma cutters
- Bluetooth radios

During an audit, any source of interference must be identified, documented, and classified as either an intentional or unintentional source of interference that may cause a DoS. As you learned in Chapter 8, 802.11 radios use a *clear channel assessment (CCA)* to evaluate constantly if the RF medium is busy or clear. Any "continuous" RF transmission that is constantly heard during the clear channel evaluation will cause 802.11 transmissions

to cease completely until the signal is no longer present. Interfering devices may prevent an 802.11 radio from transmitting, thereby causing a DoS. There are several types of RF interference:

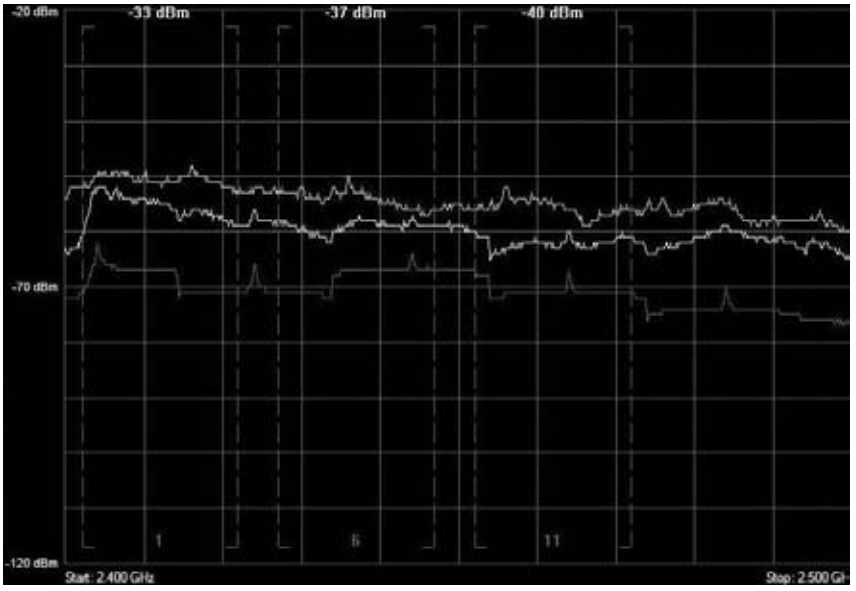
Narrow-band Interference A narrow-band RF signal occupies a smaller and finite frequency space and will not cause a DoS for an entire band such as the 2.4 GHz ISM band. A narrow-band signal is usually very high amplitude and will absolutely disrupt communications in the frequency space in which it is being transmitted. Narrow-band signals can disrupt one or several 802.11 channels. Narrow-band RF interference can also result in corrupted frames and Layer 2 retransmissions. The only way to eliminate *narrow-band interference* is to locate the source of the interfering device with a spectrum analyzer. Figure 9.1 shows a spectrum analyzer capture of a narrow-band signal close to channel 11 in the 2.4 GHz ISM band.

FIGURE 9.1 Narrow-band RF interference



Wide-band Interference A source of interference is typically considered wide band if the transmitting signal has the capability to disrupt the communications of an entire frequency band. Wide-band jammers exist that can create a complete DoS for the 2.4 GHz ISM band. The only way to eliminate *wide-band interference* is to locate the source of the interfering device with a spectrum analyzer and remove the interfering device. Figure 9.2 shows a spectrum analyzer capture of a wide-band signal in the 2.4 GHz ISM band with average amplitude of –60 dBm.

FIGURE 9.2 Wide-band RF interference



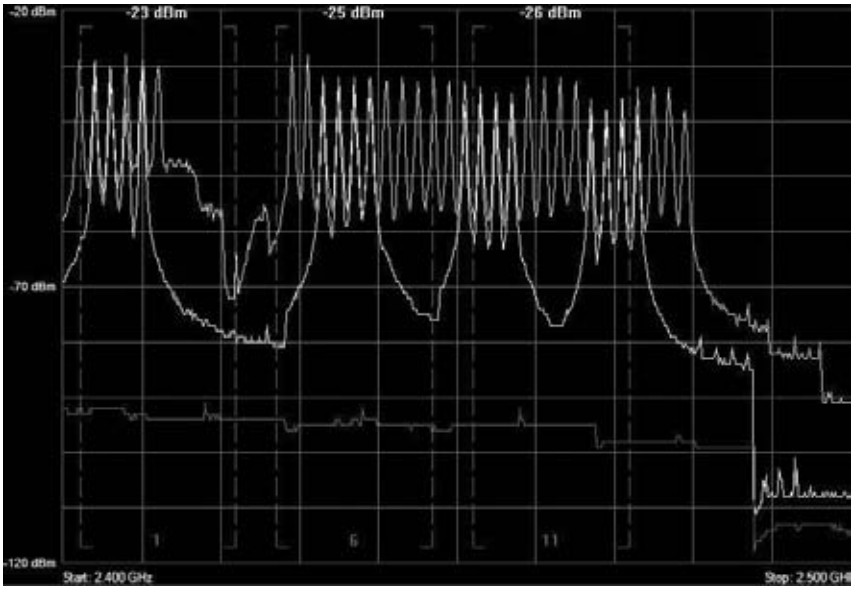
All-Band Interference The term *all-band interference* is typically associated with frequency hopping spread spectrum (FHSS) communications that usually disrupt HR-DSSS and/or ERP-OFDM channel communications at 2.4 GHz. As you learned in earlier chapters, FHSS constantly hops across an entire band, intermittingly transmitting on very small subcarriers of frequency space. A legacy 802.11 FHSS radio, for example, transmits on hops that are 1 MHz wide. While hopping and dwelling, an FHSS device will transmit in sections of the 20–22 MHz channel space used by an 802.11b/g device. Although an FHSS device will not typically cause a DoS, the frame transmissions from the HR-DSSS (802.11b) and ERP-OFDM (802.11g) devices can be corrupted from the all-band transmissions of the FHSS interfering radio.

Bluetooth (BT) is a short-distance RF technology defined by the 802.15 standard. Bluetooth uses FHSS and hops across the 2.4 GHz ISM band at 1,600 hops per second. Older Bluetooth devices were known to cause severe all-band interference. Newer Bluetooth devices utilize adaptive mechanisms to avoid interfering with 802.11 WLANs. Digital Enhanced Cordless Telecommunications (DECT) cordless telephones also use frequency hopping transmissions. Some DECT phones transmit in the 2.4 GHz band. A now-defunct WLAN technology known as HomeRF also used FHSS; therefore, HomeRF devices can potentially cause all-band interference.

The existence of a high number of frequency-hopping transmitters in a finite space will result in some 802.11 data corruption and Layer 2 retransmissions. All-band interference may not cause a continuous DoS; however, the disruption of service due to Layer 2 retransmissions can be significant from a performance perspective. The only way to

eliminate all-band interference is to locate the source of the interfering device with a spectrum analyzer and remove the interfering device. Figure 9.3 shows a spectrum analyzer capture of a frequency hopping transmission in the 2.4 GHz ISM band.

FIGURE 9.3 All-band RF interference



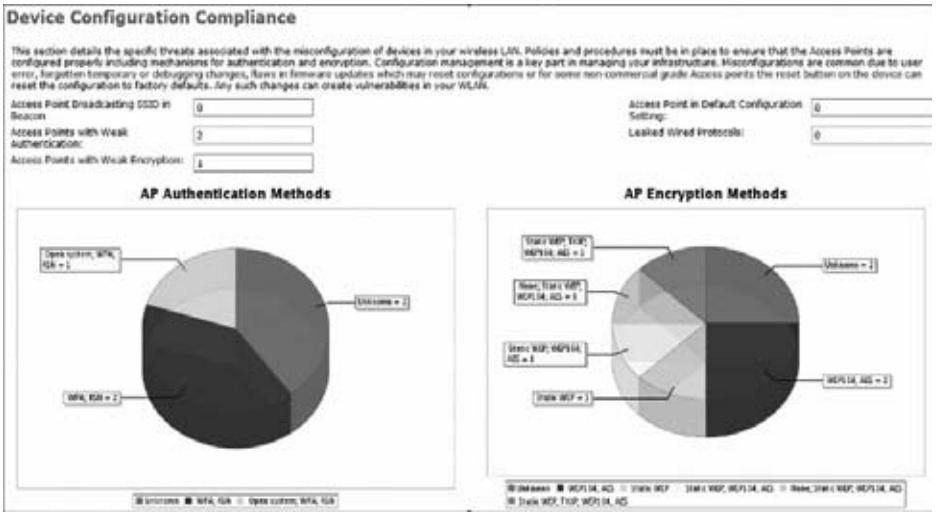
A Layer 1 security audit is normally accomplished using some sort of handheld spectrum analyzer or laptop spectrum analyzer. Some WIPSs are beginning to offer 24/7 spectrum monitoring capabilities with a *Distributed Spectrum Analysis System (DSAS)*. A more detailed discussion of DSAS can be found in Chapter 10, "Wireless Security Monitoring."

OSI Layer 2 Audit

The gathering and analysis of OSI Layer 2 information is a vital part of the wireless LAN security audit process and can reveal a great deal of information about both the WLAN functionality and the security posture of the network being examined. One of the main purposes of a Layer 2 audit is initially to detect any rogue devices or unauthorized 802.11 devices. Identifying rogue devices during an initial security audit is critical, especially if a distributed WIPS monitoring solution has not been deployed. A proper Layer 2 WLAN security audit will also be used initially to identify all authorized 802.11 WLAN devices, including access points and authorized clients. As shown in Figure 9.4, a Layer 2 audit can also be used to validate WLAN security compliance. In other words, if

the mandated security required the use of Protected Extensible Authentication Protocol (PEAP) authentication and CCMP/AES encryption, all authorized devices can be evaluated to verify the proper security configuration. Any authorized devices that have not been properly configured will be flagged.

FIGURE 9.4 Device configuration compliance



The payload of a wireless frame, meaning the Layer 3 and higher information, should normally be hidden due to encryption. The payload may be encrypted but the header and trailer information is always readable without any special decoding required. Any 802.11 frame exchange can be captured and reveal Layer 2 information about the devices directly involved in a frame exchange. A Layer 2 audit is necessary to ensure that no pertinent information is being exposed and that it is properly protected.

The following is a list (in no special order) of some of the more important things auditors should strive to find, identify, and classify at Layer 2 during audits:

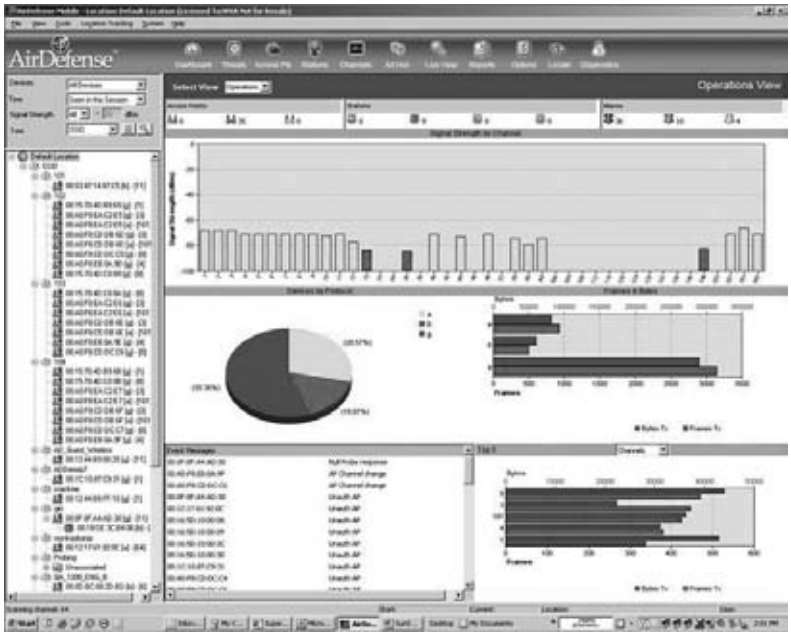
- MAC addresses
- SSID
- BSSID
- Device types being used
- Authentication types
- Encryption types
- Traffic types
- Neighboring devices
- Channels in use
- Default configurations

- Active Layer 2 attacks
- Weak keys in use
- Ad hoc clients

As you can see in Figure 9.5, a simple WLAN protocol analyzer installed on a laptop is usually sufficient to perform a Layer 2 audit. WLAN protocol analyzers are typically used for Layer 2 troubleshooting and WLAN performance analysis. However, as Figure 9.6 shows, some software WLAN protocol analyzers provide a greater emphasis on security auditing and can be used effectively as a mobile wireless intrusion detection system (WIDS) solution. Two examples are Fluke Networks' AirMagnet WiFi Analyzer and Motorola's AirDefense Mobile.

FIGURE 9.5 Layer 2 protocol analyzer

FIGURE 9.6 Mobile WIDS



We highly recommend that you test-drive a mobile WIPS solution to gain hands-on experience with the capabilities that this type of product offers. One such solution is Motorola's AirDefense Mobile. You can download a fully working 30-day trial copy of AirDefense Mobile at `www.airdefense.net/products/admobile/trial.php`. Fluke Networks also offers a mobile protocol analyzer with security auditing capabilities called WiFi Analyzer. You can request a trial version of AirMagnet WiFi analyzer at `http://airmagnet.com/products/wifi_analyzer`.

Penetration Testing

You have already learned that WLAN auditing is a process used to ensure that 802.11 communications and devices are secured and functioning as required by organizational policies, industry standards, and/or governmental regulations. Wireless LAN auditing may also include wireless *penetration testing* if desired as part of the scope of work agreement between the organization and the auditor. A WLAN penetration test is used to evaluate the security of the WLAN by simulating an attack from a malicious intruder. Many of the tools used during WLAN penetration testing are the same tools that hackers may use for malicious purposes. WLAN penetration testing tools are used to find security vulnerabilities due to hardware/software flaws, improper system configuration, and known technical weaknesses.

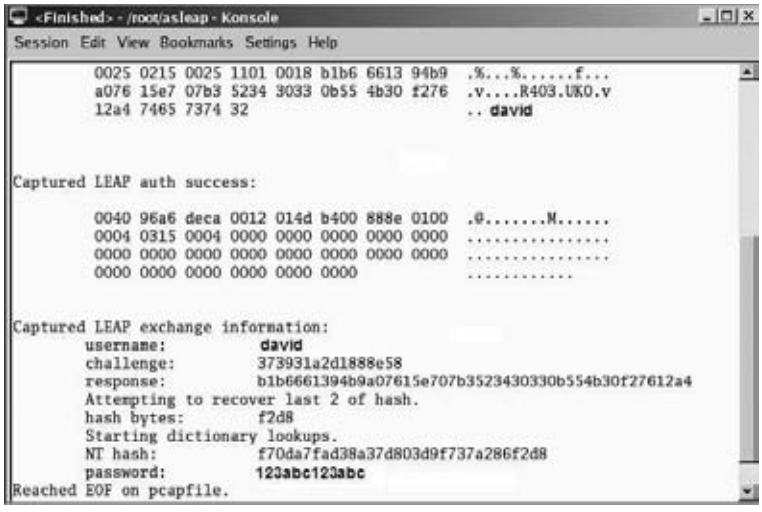
What Is a Rainbow Table?

A *rainbow table* is used to find the original plaintext for a hashed password. A rainbow table is a lookup table offering a time-memory trade-off used in recovering the plaintext password from a password hash generated by a hash function. With rainbow tables, time is initially spent precomputing the hashes and storing the data into a file. This file is later used to speed up the cracking process. Using brute-force methods to crack password hashes takes a long time, but it doesn't require much memory and requires no disk space. Rainbow tables require time to generate, take up disk space, and use more memory in the cracking process, but are much faster when used to crack the hash. More information can be found at the Distributed Rainbow Table Project at `www.freerainbowtables.com`.

A good example of a penetration test is using known authentication cracking software tools to demonstrate the weakness of the chosen passwords or passphrases. Weaker authentication methods are often deployed due to cost concerns. A good penetration test would be an attempt to circumvent weaker authentication methods such as Lightweight Extensible Authentication Protocol (LEAP) or WPA/WPA-2-Personal. You learned in

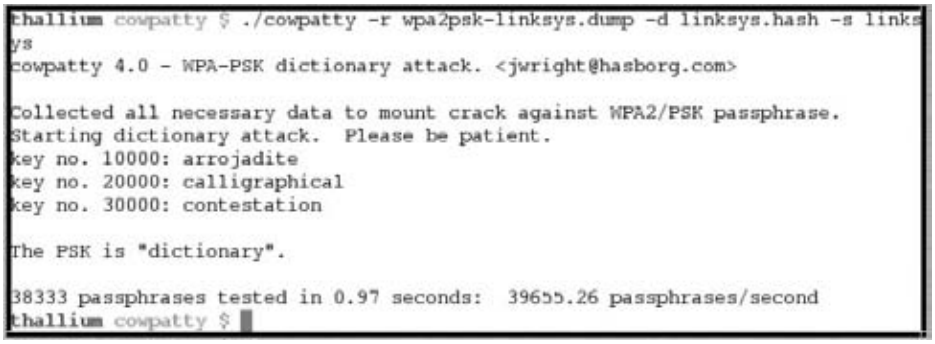
earlier chapters that LEAP is susceptible to an *offline dictionary attack*. As shown in Figure 9.7, a software auditing tool called *Asleap* can be used with a hashed rainbow table of adequate size to reveal the hashed LEAP password in a matter of seconds.

FIGURE 9.7 Asleap



You also have already learned that WPA/WPA2-Personal, using preshared keys, is a weak authentication method that is vulnerable to an offline *brute-force dictionary attack*. There is no difference between cracking WPA or WPA2 preshared keys. The authentication methodology used in both formats is basically the same, so the technique used to obtain the passphrase is the same. As Figure 9.8 shows, a software auditing tool called coWPAtty can be used to derive weak passphrases.

FIGURE 9.8 coWPAtty



The Asleap and coWPAtty authentication cracking auditor tools were created by wireless security expert Joshua Wright. The tools can be downloaded from Joshua's website at `www.willhackforsushi.com`.

Wired Infrastructure Audit

The normal purpose of a WLAN is to act as a wireless portal to network resources that reside on the wired network infrastructure. As you have already learned, penetration testing can be used to see if strong authentication solutions are deployed properly to protect the portal. Once authorized onto network resources, WLAN users can be further restricted as to what resources may be accessed and where they can go. *Role-based access control (RBAC)* security, commonly used by WLAN controllers, can be used to restrict certain groups of users to certain network resources. RBAC is usually accomplished with firewall policies and access control lists. Penetration testing of the firewall used to restrict WLAN user access to certain network resources should be a mandatory procedure during the security audit. All WLAN infrastructure interfaces should also be audited. Wireless infrastructure hardware, such as autonomous access points and WLAN controllers, can be managed by administrators via a web interface, a command-line interface, a serial port, a console connection, and/or Simple Network Management Protocol (SNMP). It is imperative that these interfaces be protected. Interfaces that are not used should be disabled. Strong passwords should be used, and encrypted login capabilities such as Hypertext Transfer Protocol Secure (HTTPS) and Secure Shell (SSH) should be utilized if available.

Social Engineering Audit

The weakest link in security for any type of computer network is usually the network end users. In Chapter 8, you learned how *social engineering* is the act of manipulating people into divulging confidential information for the purpose of obtaining information used to access a computer network. Therefore, social engineering techniques are often used by the security auditor to circumvent the WLAN and gain access to network resources. Social engineering performed by an auditor is a form of penetration testing and is usually the most successful method. An auditor will most likely find lapses in security due to improper employee training or employee policy enforcement. Although penetration testing using software tools is often successful, the auditor will probably have more luck with social engineering techniques used for penetration testing purposes.

Real World Scenario

Social Engineering Audit

Recently, a government agency hired an outside company to perform a computer security audit. One of the auditors sent an email message introducing himself as Albert Kada, the new network administrator. Albert informed all of the government agency employees that he was updating the password database and needed everyone to email Albert their passwords. Over 40 percent of the employees sent their passwords to Al-Qaeda (Albert Kada). After the security audit, it was recommended that all employees be retrained in regard to password policy.

WIPS Audit

If a company has been hired to perform a WLAN security audit, chances are that the customer is not using a distributed *wireless intrusion detection system (WIDS)* or distributed *wireless intrusion prevention system (WIPS)*. Many of the WIDS/WIPS vendors will often perform an initial WLAN security audit for free. The WIPS/WIPS vendor will show the customer potential security holes, make recommendations, and then offer to sell the customer a distributed WIDS/WIPS solution that is capable of full-time WLAN security monitoring.

If a distributed WIDS/WIPS monitoring solution has already been deployed, the monitoring solution should also be audited. Hacker attacks, such as DoS, MAC spoofing, rogue devices, and so on, should be simulated to see if the proper WIDS/WIPS alarms are triggered for each attack. For example, a third-party access point can be connected to a wired port to test the rogue detection capabilities of a distributed WIPS monitoring solution. Another example is when Layer 2 DoS attacks are simulated to verify detection by the WIPS server and sensors. If certain alarms are not triggered, alarm thresholds may need to be adjusted on the WIDS/WIPS server.

WIDS and WIPS monitoring solutions will be discussed in greater detail in Chapter 10.

Documenting the Audit

The job is not finished until the paperwork is done. This is a common quotation but true nonetheless. Documenting the audit is of great importance to both the auditor and the customer. The auditor needs to be able to produce evidence of his or her findings

to the customer and make recommendations for improving security and WLAN health based on these findings. The customer will need documentation to prove compliance with regulations. Documentation can also be used by the customer to have their own IT staff implement the security changes recommended by the auditor.

Documentation of an audit can be presented in several formats. An all-written presentation in PDF format is often used, while some auditors use Microsoft PowerPoint slide shows. The actual deliverable can vary based on the *statement of the work (SOW)* agreement and customer's requirements. The customer may also provide some documentation such as a network topology map and corporate policy documents prior to the audit. Here is some of the documentation required for the audit:

Statement of Work This document outlines the audit requirements, deliverables, and timeline that the auditor will execute for a customer. Pricing and detailed terms and conditions are specified in the SOW.

Liability Waiver It is very important that any auditor obtain signed permission in the form of a liability waiver or hold harmless agreement to perform the security audit. An audit should never take place without authorized permission.

Network Topology Map Understanding the layout of the customer's wired network infrastructure and WLAN infrastructure will speed up the audit process and allow for better planning of penetration testing. A computer network topology map will provide necessary information, such as the location of the wiring closets, access points, WLAN controllers, and firewalls.

Mutual Nondisclosure Agreement Some organizations may not wish to reveal their network topology for security reasons. It may be necessary to obtain security clearance and/or sign nondisclosure agreements to gain access to these documents.

Corporate Security Policy Obtaining a copy of the customer's written security policy document will be valuable for determining risk assessments. Very often the corporate security policy will be nonexistent or outdated.

Audits and or penetration tests should not go beyond the written corporate policy or the SOW agreement. Documentation in IT can be thought of as a type of unicorn, something you have heard about but never see. This does not mean it should not be requested prior to beginning the audit. Often an auditor is called upon to assist the customer in creating documentation such as policy documents.

By finding out what is visible in WLAN communications, the auditor is able to document the information being made available to attackers and to begin to secure the transmissions. If there is a written wireless security policy, auditors are able to determine if WLAN communications are being conducted within the policy guidelines by comparing the information contained in captured traffic with the written policy.

Unfortunately, the existence of a written security policy that governs wireless communications is a rare thing. Most organizations rely on a generic security statement that focuses on inappropriate Internet and phone usage rather than on WLAN security. In the absence of written WLAN usage policy, auditors can compare captured traffic with industry compliance policies or governmental regulations such as PCI or SOX. If there is no organizational awareness of WLAN security, the comparison of current traffic and industry or governmental standards is a very useful tool in helping networks become and remain secure.

Audit Recommendations

The main purpose of the WLAN security audit is to expose potential security holes so that proper solutions and procedures can be implemented. After the audit is completed, recommendations will be made based on the audit findings on how to protect the WLAN and the network infrastructure more securely. Recommendations could include the following:

Stronger Dynamic Encryption If no encryption or weak encryption such as WEP is being used, the recommendations will be to upgrade to an available dynamic encryption method such as CCMP/AES.

Stringent Authentication Penetration testing may reveal weak authentication such as LEAP or WPA/WPA2-Personal. Upgrading to an 802.1X/EAP authentication solution using tunneled authentication will almost always be recommended.

Role-Based access Control (RBAC) Recommendations can be made on how to segment groups of users to certain network resources using firewall policies, access control lists, and wireless VLANs.

Monitoring Recommendations will be made about the types of distributed WIDS/WIPS monitoring solutions that may be needed.

Corporate Policy An extra addendum to the security recommendations might be corporate WLAN policy recommendations. The auditor might assist the customer in drafting a wireless network security policy if they do not already have one.

Training One of the most overlooked areas of WLAN security is proper training. It is highly recommended that security training sessions be scheduled with the customer's network administration personnel. Additionally, condensed training WLAN security sessions should be scheduled with all end users.

Physical Security The installation of enclosure units to protect against theft and unauthorized physical access to access points may be a recommendation. Enclosure units are also often used for aesthetic purposes.

WLAN Security Auditing Tools

To conduct a successful WLAN security audit, you must use tools designed for that purpose. Although attackers may use some of the same tools to exploit poorly secured networks, WLAN security auditors use them to expose areas of the WLAN that are in need of increased protection or reconfiguration. The audit is performed in order to prevent attackers from gaining access to network resources and to assist the organization in reaching the required security levels demanded by industry and policy compliance. Auditors have an advantage over attackers in that they are typically allowed physical access to the premises that they are auditing. This access is much like the access granted during a WLAN site survey, and it may require an escort or special identification to traverse the area. A degree of overlap exists between a good WLAN site survey kit and a good WLAN auditing kit.

The successful WLAN auditor requires not only a thorough knowledge of 802.11 technology but also the proper software and hardware to perform the WLAN penetration testing. The hardware and software used during an audit varies based on the type of WLAN vulnerability to be identified. For example, if an auditor is looking for the source of noise that is causing a potential denial of service, the proper tool is a spectrum analyzer. If the auditor is conducting 802.11 traffic analysis, the proper tool would be a WLAN protocol analyzer.

The tools selected must match the job at hand. Typically a well-equipped auditor will have the following hardware devices and software to assist them in their work, either as part of their own kit or provided by the facility being audited:

- At least one laptop
- WLAN protocol analyzer and audit software
- Spectrum analyzer
- WLAN penetration testing software tools
- 802.11 packet generator software
- 2.4 GHz and 5 GHz signal generator
- Facility blueprints or floor plan
- WLAN cards for each frequency and protocol
- Omni-directional antennas
- Yagi or patch antennas
- Matching pigtail connectors
- Global positioning sensor (GPS)
- Access point
- Camera and/or video recorder
- Phone or walkie-talkie

- Ladders and or lifts
- Battery packs and power cables
- Wheeled cart

This is by no means an exhaustive listing of all the tools used to conduct a WLAN audit. The type and number of tools needed to conduct a successful audit vary based on the type of WLAN being audited and the security requirements of that WLAN. For example, security audits at a Wi-Fi hot spot may only require a visual inspection of the AP and making sure the captive portal is working, while large-scale enterprise WLANs may require several days of capturing 802.11 frames for evaluation as well as penetration testing.

The Layer 1 and Layer 2 auditing tools mentioned earlier in this chapter should all be considered mandatory. WLAN protocol analyzers are typically used for Layer 2 auditing, and spectrum analyzers are used for Layer 1 auditing. Many freeware Linux-based and Windows-based WLAN penetration testing software tools are also widely available. Penetration testing normally should be considered a mandatory part of the audit. Some of the other tools listed are obviously required, such as laptops and WLAN cards. Others require more explanation about their use, such as APs and battery packs. For example, an auditor may require several hours of analysis before rendering a security report; thus it's important that the laptop and other devices have adequate power the entire time they're gathering information. External battery packs to power the devices may be needed in areas where a wall outlet cannot be found. A third-party access point may be used to test the rogue detection capabilities of a distributed WIPS monitoring solution.

Physical inspection or building access may require identification or an escort during the audit. If conducting the audit from off the premises, the use of an antenna may be required to hear the wireless transmissions from inside the building(s). As discussed in Chapter 8, "Wireless Security Risks," a high-gain unidirectional antenna can be used to hear RF signals from a great distance. Antennas are bidirectional passive amplifiers. In the case of an outside audit, proper antenna use often gives the auditor the ability to listen from a remote location. An outside auditor can emulate an attacker who might launch an attack from a location off company grounds.

Physical inspection of devices and cabling is part of a complete WLAN audit. To inspect such devices physically, ladders or lifts may be required. Carrying all of the equipment required for an audit about may become cumbersome and result in the auditor not covering the entire area. The use of a wheeled cart can reduce the wear and tear on the auditor (as will a comfortable pair of shoes), just like in a WLAN site survey. Pen and paper along with a camera and video recorder will give the auditor the ability to take notes and document what they find as part of the deliverable presented at the end of the audit. In a large outdoor area, the auditor may find the use of a GPS may be required to record the location of outdoor 802.11 devices, such as bridges and mesh access points.

A larger deployment may require a team of auditors who need to communicate with one another during the audit. Having phones and or walkie-talkies will facilitate this

communication. It is easy to see how the hardware and software used as part of a WLAN security audit resembles a kit used as part of a pre- or post-deployment WLAN site survey. Unlike a site survey, the audit will monitor channels, frequencies, and areas of coverage not required by the WLAN.

Many of the tools traditionally used for penetration testing are Linux based. Today, however, many of these tools are supported on a Windows platform. Which tool is used may depend on whether users being audited are Linux, Windows, or Mac OS users. There are fewer tools available for WLAN analysis for use on Mac OS than for Linux and Windows platforms. Table 9.1 contains a list of some of the more common WLAN security-auditing tools.

TABLE 9.1 Common Tools and Uses

Type of Use	Possible Audit/Attack	Tools
Wireless discovery	Eavesdropping, discovery of rogue APs, ad hoc STAs, and open/misconfig-ured APs	NetStumbler, Kismet, Wellenreiter, WiFiFoFum, WiFi Hopper, Win Sniffer, Wireshark, and commercial WLAN protocol analyzers
Encryption/authentication	WEP, WPA, LEAP cracking, dictionary attacks	Asleap, Aircrack-ng, coWPAtty, AirSnort, WEPCrack, WZCook, andTHC-LEAPcracker
Masquerade	MAC spoofing, man-in-the-middle attacks, evil twin attacks, Wi-Fi phishing attacks	Airsnarf, Ettercap Karma, Hotspotter, HostAP, SMAC
Insertion	Multicast/broadcast injection, routing cache poisoning, man-in-the-middle attacks	Airpwn, WEPWedgie, chopchop, VIPPR, IrPass, CDPsniffer
Denial-of-service	Layer 1 and Layer 2 DoS	AirJack, Void11, Bugtraq, IKECrack, FakeAP, and RF signal generators

WLAN penetration testing tools are freely available on the Internet; however, there is often a learning curve on how to properly use a wide variety of software programs. Several commercial vendors offer automated WLAN assessment solutions such as Immunity's SILICA-U solution shown in Figure 9.9.

FIGURE 9.9 Immunity SILICA-U WLAN security assessment software

Linux-Based Tools

Some of the most effective wireless auditing tools run on Linux platforms, many of which can be accessed from a bootable CD. In this section, we will examine some of these tools and explain their use in conducting security audits.

There are several tools from which to choose to perform the same or similar tasks. The tools you choose will vary based on personal preference and the task at hand. The basics are the same no matter which tool you select. The devices and vulnerabilities must be discovered and documented. To find these vulnerabilities, you can use tools such as Kismet, AirSnort, and Aircrack-ng.

Where Can You Find WLAN Penetration Software Tools?

BackTrack is the probably the most popular Linux-based distribution of tools focused on penetration testing. Currently BackTrack consists of more than 300 different up-to-date tools that are logically structured according to the workflow of security professionals. The BackTrack platform can boot directly from a CD-ROM drive or can be run from a virtualization image such as VMware. A free ISO image of BackTrack can be downloaded from `www.remote-exploit.org/backtrack_download.html`.

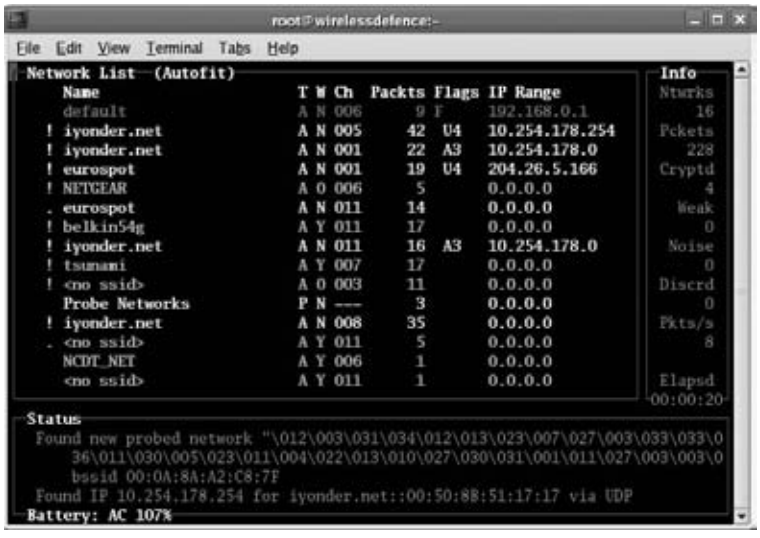
Another good website with information about WLAN auditing software tools is Wirelessdefence.org, which provides a collection of "Top tips" for the auditing of 802.11

networks and is an attempt to provide a "one-stop shop" for common tasks encountered by WLAN security auditors. Many WLAN auditing tools are available for download at `http://wirelessdefence.org`.

Commercially packaged WLAN penetration tools are also available. Immunity offers security assessment and penetration testing solutions. Information about Immunity's WLAN security assessment solutions, SILICA and SILICA-U can be found at `www.immunityinc.com`.

Blueprinting or enumerating network devices should be part of every audit. Looking for anything in use, not just the device traffic you would expect, will reveal rogue devices as well as incorrect configuration of authorized devices. Wardriving software tools are still often used for simple WLAN discovery while other tools are used for packet capture. Since these tools are largely freeware and run on the Linux platform, there are lots of user groups and online tutorials and videos detailing their usage. *THC-wardrive* is a Linux-based wardriving tool that uses both an 802.11 radio and a GPS device to link the discovered 802.11 devices with latitude and longitude coordinates. As shown in Figure 9.10, *Kismet* is a Linux-based 802.11 Layer 2 wireless protocol analyzer and intrusion detection system. Kismet will work with any wireless card which supports raw monitoring (rfmon) mode, and it can sniff 802.11b, 802.11a, and 802.11g traffic.

FIGURE 9.10 Kismet



Once the target has been identified, the auditor must then determine what additional information might be extracted using penetration testing. For example, if the auditor has been tasked with determining the WEP key or the WPA preshared key (PSK), they may

use a tool such as AirSnort or Aircrack-ng. These tools are used to derive keys. *AirSnort* passively gathers packets until enough containing the *initialization vector* (IV) are captured, and then it cracks the WEP key offline. It takes roughly 300,000 to 500,000 IVs in the packet capture to crack the WEP key based on the complexity of the WEP key used. As shown in Figure 9.11, Aircrack-ng is a set of tools used together for cracking WEP and WPA-PSK. The Aircrack-ng tools include Airodump (used for packet capturing), Aireplay (used to inject traffic), Aircrack (used to crack WEP and WPA-PSK), and AirPcap (used to decode WEP and WPA-PSK captures). Aircrack-ng enables WEP and WPA-PSK traffic to be cracked in a short time frame as compared to older methods.

FIGURE 9.11 Aircrack-ng

More information about the Aircrack-ng auditor tools can be found at www.aircrack-ng.org.

No matter which tools are used, the auditor's goals remain constant—find the devices, get on the network, and/or decode the data. Attackers use the same tools but for malicious reasons. Although there are many tools from which to choose, auditors and attackers alike find some tools they prefer more than others, with speed and ease of use weighing heavily in the decision. Most of the modern Linux command-line tools have been ported over to GUI-based tools that require less interaction and allow for quicker rendering of the desired information.

Windows-Based Tools

In the early days of wireless networking and WLAN security auditing, the auditor and even the attacker only had Linux-based tools available for true assessment and launching of wireless attacks. However, just as with other tools and applications, wireless auditing tools have over time become easier to use and more powerful. In this case, the tools that were once only available for use on Linux platforms have been ported over to Windows formats, reducing the amount of command-line work required. As in the use of Linux tools described earlier, auditing with Windows-based tools basically consists of discovery, cracking, and access. The wireless auditing tools that are used on Windows-based platforms offer fewer freeware options, but have a large selection available for purchase. There are both active and passive discovery tools for this platform as well. One of the most popular WLAN discovery tools is NetStumbler. This freeware tool finds networks by using null probe request frames.

A copy of NetStumbler is included on the CD that accompanies this book and can also be downloaded at `www.netstumbler.com`.

Other GUI-based freeware WLAN discovery tools include WiFiFoFum, WiFi Hopper, and many more. Although the GUI-based tools provide the same basic information as the command-line Linux-based tools, they present the information in a more intuitive fashion. GUI-based tools have made it easier for more people to conduct wireless audits and are even used by Linux users in either a Linux GUI or in Windows. Packet-capturing tools, such as the freeware tool Wireshark or commercial 802.11 protocol analyzers such as WildPackets' OmniPeek, do a great job of gathering 802.11 frames and allowing the user to filter their view based on a vast number of items—from the MAC address to the frame subtype. These tools let you see what each 802.11 device detected is doing, which is valuable information to auditors and attackers alike.

Summary

Diligently conducting WLAN security audits will reveal areas where improvements can be made in protecting the wireless network. The WLAN audit process involves inspection of Layer 1, Layer 2, the wired network, and the WIPS monitoring solution. The information gathered during these audits can be leveraged to make the proper recommendations for protecting both the WLAN as well as the wired network resources. Numerous tools are available to assist the auditor in their duties; some are commercial tools and others are freeware. Many of the tools used by hackers can also be used during a WLAN security audit for penetration testing. The best tool found in any auditor's toolbox is social engineering skills.

Exam Essentials

Explain the various components of a WLAN security audit. These include a Layer 1 and 2 audit, penetration testing, wired infrastructure audit, social engineering audit, and possibly a WIPS audit.

Describe social engineering techniques. Explain why social engineering skills is usually the most successful WLAN auditing tool.

Understand the various methods of WLAN security auditing. Explain the importance of auditing both Layers 1 and 2 of the OSI model. Define aspects of penetration testing, wired infrastructure auditing, and WIPS auditing.

Explain WLAN security auditing and penetration testing tools. Discuss how Layer 1 and Layer 2 tools are used during a WLAN security audit. Describe some of the methods and tools used during WLAN penetration testing.

Key Terms

Before you take the exam, be certain you are familiar with the following terms:

Aircrack-ng

AirSnort

all-band interference

Asleap

BackTrack

Bluetooth (BT)

brute force dictionary attack

clear channel assessment (CCA)

denial of service (DoS)

Distributed Spectrum Analysis System (DSAS)

initialization vector

Kismet

narrowband interference

offline dictionary attack

penetration testing

rainbow table

risk mitigation.

Role-based access control (RBAC)

social engineering

spectrum analysis

statement of the work (SOW)

THC-wardrive

threat assessment

wideband interference

wireless intrusion detection system (WIDS)

wireless intrusion prevention system (WIPS)

Review Questions

1. Which of these devices are potential sources of all-band interference? (Choose all that apply.)
   - **A.** Bluetooth
   - **B.** Microwave oven
   - **C.** 2.4 GHz DSSS cordless phone
   - **D.** 802.11 FHSS access point
   - **E.** HomeRF access point
   - **F.** 2.4 GHz DECT phone
2. Which of these WLAN auditing tools has the most success in compromising network resources when penetration testing is performed?
   - **A.** WLAN protocol analyzer
   - **B.** Asleap
   - **C.** Aircrack-ng
   - **D.** coWPAtty
   - **E.** Social engineering
   - **F.** Kismet
3. A WLAN security auditor recently walked into the ACME Company corporate headquarters and presented documentation to ACME management based on the WLAN penetration testing that was performed during the audit. ACME management was not pleased and decided to call the police and have the WLAN security auditor arrested. What documentation did the auditor fail to obtain prior to the WLAN security audit?
   - **A.** Written corporate policy
   - **B.** Liability waiver
   - **C.** Statement of work
   - **D.** Nondisclosure agreement
   - **E.** Network topology map
4. What would be the intended purpose of simulating Layer 2 deauthentication attacks as part of a WLAN audit?
   - **A.** Audit Layer 1
   - **B.** Audit Layer 2
   - **C.** Audit the wired infrastructure
   - **D.** Audit the WIPS

5. Management has asked the WLAN administrator to perform a thorough WLAN security audit. The administrator explains that a wired-side audit is necessary to ensure a secure WLAN. What procedures should be followed during the wired-side portion of a WLAN audit? (Choose all that apply.)
   - **A.** Audit firewall policies and rules
   - **B.** Audit WLAN management interfaces
   - **C.** Audit core Layer 3 switch
   - **D.** Audit application services

6. What are some of the recommendations that might be made to a customer after a successful WLAN security audit? (Choose all that apply.)
   - **A.** Physical security
   - **B.** Employee training
   - **C.** Dynamic RF configuration
   - **D.** Monitoring capabilities
   - **E.** AP and client power settings

7. Which of these tools are required for a proper WLAN security audit? (Choose all that apply.)
   - **A.** Spectrum analyzer
   - **B.** WLAN protocol analyzer
   - **C.** WLAN penetration testing software tools
   - **D.** Global positioning sensor (GPS)
   - **E.** Cameras

8. The management at the ACME Corporation has asked Bob to perform a WLAN security audit. Bob informs management that he will need to purchase a Yagi antenna for the audit. What reasons should Bob give management to justify the purchase of the Yagi antenna? (Choose all that apply.)
   - **A.** Attackers do not need physical access to the facility.
   - **B.** Yagi antennas are used in high multipath areas.
   - **C.** RF signals can be amplified from great distances.
   - **D.** Yagi antennas are used for indoor audits.
   - **E.** Spectrum analyzers require directional antennas.

9. As an auditor you have been asked to determine if the WLAN access points and client devices have been configured with the proper encryption. What should you use to answer this question for your customer? (Choose all that apply.)
   - **A.** Written corporate security policy
   - **B.** WLAN protocol analyzer
   - **C.** Aircrack-ng
   - **D.** coWPAtty
   - **E.** Asleap

10. What is some of the proper documentation needed prior to the WLAN security audit?

A. Statement of work

B. Liability waiver

C. Nondisclosure agreement

D. All of the above

11. A thorough security audit was conducted when a WLAN was deployed over 12 months ago and found no security issues. Recently, the organization failed to meet an industry compliance that the WLAN initially was able to meet due to security failures. What should have been done to help prevent the noncompliance issue the company now faces? (Choose all that apply.)

A. Update to the corporate security policy.

B. Remove all WLAN devices from the network.

C. Upgrade all firmware.

D. Perform a periodic WLAN audit.

12. As part of an audit and covered in the statement of work and nondisclosure agreements, you have been asked to determine if an outsider with no inside access or information would be able to gain access to the WLAN used in your client's WPA2-Personal protected warehouse. Which tools should you use to provide the answer? (Choose all that apply.)

A. WLAN protocol analyzer

B. Aircrack-ng

C. Dictionary file

D. NetStumbler

E. coWPAtty

F. Asleap

13. What would be the intended purpose of using a third-party AP as part of a WLAN audit?

A. Audit Layer 1.

B. Audit Layer 2.

C. Audit the wired infrastructure.

D. Audit the WIPS.

14. Users have recently been complaining about lost connections at various times of the day. An original site survey was conducted that initially confirmed connectivity in all areas of the facility. Which tools must you use as part of your audit to determine the unexplained cause of loss connectivity? (Choose all that apply.)

A. High-gain Yagi antenna

B. Low-gain dipole antenna

C. WLAN protocol analyzer

D. Spectrum analyzer

E. Rainbow table

15. While conducting a WLAN security audit, you find an access point being used by employees on the network configured with all of the correct corporate security settings. This AP is not on the authorized AP list of the company's WIPS, but is configured securely and according to corporate written security policy. What should you do about this AP?

A. Unplug it from the wired LAN immediately.

B. Include it in your report to the company.

C. Nothing; it is secured by company standard.

D. Crack its security and decode the data.

16. What is the main purpose of using a WLAN protocol analyzer during the Layer 2 analysis of a WLAN security audit? (Choose all that apply.)

A. Identifying unauthorized devices

B. Auditing the wired infrastructure

C. Performing penetration testing

D. Validating security compliance of authorized devices

E. Auditing the WIPS

17. During a WLAN audit, you see an AP deployed in a common hallway of a multitenant building. This AP provides coverage to a small meeting room used by your customer. It was deployed there to keep the small meeting room from looking cluttered and is using the appropriate authentication and encryption as defined by the written company security policy. Is this AP a risk to the company's network?

A. Yes, it is not on company property.

B. No, it is using required security settings.

18. When conducting a WLAN security audit, which of the following items would be of the least amount of use to the auditor?

A. Physical access to the building

B. Floor plan

C. Security escort

D. Ladder or lift

E. All of these are useful.

19. As an auditor, you have been asked to determine if the WLAN access points and client devices have been configured with EAP-TTLS authentication. What should you use to answer this question for your customer?

A. WLAN discovery tool

B. WLAN protocol analyzer

C. Aircrack-ng

D. coWPAtty

E. Asleap

20. Another auditor tells you that they use the same toolkit to conduct audits as they use to conduct WLAN site survey work. Why would they do this since they are performing two different types of work?

A. Many auditors cannot afford a proper auditing kit.

B. The two types of work are similar enough to use the same tools.

C. They have never been shown how to conduct an audit.

D. Their scope of work document limits them to passive auditing.

Answers to Review Questions

1. A, D, E, F. All the devices listed are known sources of RF interference in the 2.4 GHz ISM band. All-band interference is caused by frequency-hopping radio transmissions. FHSS is used by Bluetooth, legacy 802.11 FHSS access points, HomeRF equipment, and Digital Enhanced Cordless Telecommunications (DECT) telephones. DECT telephones can use multiple frequencies, including the 2.4 GHz ISM band.

2. E. The weakest link in security for any type of computer network is usually the network end-users. Social engineering is the act of manipulating people into divulging confidential information for the purpose of obtaining information used to access a computer network. Therefore, social engineering techniques are often used by the security auditor to circumvent the WLAN and gain access to network resources. Social engineering performed by an auditor is a form of penetration testing and is usually the most successful method. An auditor will most likely find lapses in security due to improper employee training or employee policy enforcement. Although penetration testing using software tools is often successful, the auditor will probably have more luck with social engineering techniques used for penetration testing purposes.

3. B. The liability waiver, scope of work, and nondisclosure agreements should all be completed prior to conducting a WLAN audit. It is very important that any auditor get signed permission in the form of a liability waiver or hold harmless agreement to perform the security audit. An audit should never take place without authorized permission. Anyone who performs a WLAN security audit and penetration testing without permission risks arrest and prosecution.

4. D. If a distributed WIDS/WIPS monitoring solution has already been deployed, the monitoring solution should also be audited. Hacker attacks such as denial of service, MAC spoofing, rogue devices, and so forth should be simulated to see if the proper WIDS/WIPS alarms are triggered for each attack. For example, deauthentication and dissociation attacks can be simulated to verify detection by the WIPS server and sensors. If certain alarms are not triggered, alarm thresholds may need to be adjusted on the WIDS/WIPS server.

5. A, B. Once authorized onto network resources, WLAN users can be further restricted as to what resources may be accessed and where they can go. Role-based access control (RBAC) security commonly used by WLAN controllers can be used to restrict certain groups of users to certain network resources. RBAC is usually accomplished with firewall policies and access control lists. Penetration testing of the firewall used to restrict WLAN user access to certain network resources should be a mandatory procedure during the security audit. All WLAN infrastructure management interfaces should also be audited. Interfaces that are not used should be disabled. Strong passwords should be used, and encrypted login capabilities such as Hypertext Transfer Protocol Secure (HTTPS) and Secure Shell (SSH) should be utilized if available.

6. A, B, D. Stronger dynamic encryption, stringent authentication methods, role-based access control proposals, WIDS/WIPS monitoring recommendations, corporate policy suggestions, employee training, and physical security advice may all be the result of a successful WLAN audit.

7. A, B, C. The Layer 1 and Layer 2 auditing tools should be considered mandatory. WLAN protocol analyzers are typically used for Layer 2 auditing and spectrum analyzers are used for Layer 1 auditing. Many freeware Linux-based and Windows-based WLAN penetration testing software tools are also widely available. Penetration testing normally should be considered a mandatory part of the audit. Many other tools such as cameras, battery packs, and GPS devices may be needed but are not considered mandatory.

8. A, C. Yagi antennas are often deployed to reduce reflections in high multipath environments; however, this has nothing to do with a WLAN security audit. A high-gain unidirectional antenna can be used to hear RF signals from a great distance. Antennas are bidirectional passive amplifiers. In the case of an outside audit, proper antenna use often gives the auditor the ability to listen from a remote location. Just because the signal is not intentionally propagated beyond the property does not mean it cannot be heard with the right equipment. An outside auditor can emulate an outside attacker who can possibly launch an attack from areas that cannot be secured physically.

9. A, B. To learn which type of encryption the company has mandated, you should consult the written security policy. Any WLAN protocol analyzer can verify that all corporate WLAN devices are using the proper encryption methods. coWPAtty, Asleap, and Aircrack-ng can be used to attack devices and crack WEP and WPA-PSK keys but are not used simply to determine the encryption types that are being used and whether they meet corporate goals.

10. D. The statement of work (SOW) document outlines the audit requirements, deliverables, and timeline that the auditor will execute for a customer. Pricing and detailed terms and conditions are specified in the SOW. A liability waiver grants authorized permission to perform the security audit. A mutual nondisclosure agreement is necessary because organizations may not wish to reveal their network topology for security reasons. Additionally, a network topology map is useful for understanding the layout of the customer's wired network infrastructure and WLAN infrastructure. If possible, obtaining a copy of the customer's written security policy document will be valuable for determining risk assessments. Very often the corporate security policy will be nonexistent or outdated.

11. A, D. Periodic auditing, in addition to the initial audit, should have revealed the flaws in security. Many post-deployment changes to a network can reduce the security posture to an unacceptable level. Devices added to the network, either as legitimate or rogue, can change the level of security of a network. Updating a written policy does not ensure that the policy is being followed. However, if the policy does not address current regulatory issues, it also needs to be updated. This should be checked regularly.

12. A, B, C, E. WPA2-Personal authentication, often referred to as WPA2-PSK, can be compromised with an offline brute-force dictionary attack. A WLAN protocol analyzer is needed to capture the 4-way Handshake to get the seed key for cracking. Authentication cracking audit tools such as Aircrack-ng or coWPAtty use a dictionary file to crack the static passphrase used for authentication. If an auditor is not able to capture the 4-way

Handshake because the stations are already connected, a deauthentication or disassociation flood can be used to kick them off the network, forcing the client stations to reauthenticate. Asleap is an authentication cracking audit tool used to compromise LEAP. NetStumbler is a WLAN discovery tool.

13. D. If a distributed WIDS/WIPS monitoring solution has already been deployed, the monitoring solution should also be audited. Hacker attacks such as denial of service, MAC spoofing, rogue devices, and so on should be simulated to see if the proper WIDS/WIPS alarms are triggered for each attack. For example, a third-party access point can be connected to a wired port to test the rogue detection capabilities of a distributed WIPS monitoring solution. If certain alarms are not triggered, alarm thresholds may need to be adjusted on the WIDS/WIPS server.

14. C, D. Without collecting information from both Layer 1 and Layer 2, there is no certain way to determine the cause of the disconnections. There could be Layer 1 or Layer 2 DoS attack disrupting service. A rainbow table is used for cracking and the dipole antenna, regardless of gain, is not required; other antenna types could be used.

15. B. This AP should be reported to the company as quickly as possible. Often the networking team deploys APs without consulting the security team and having them added to the WIPS as authorized. Unplugging it immediately may disrupt legitimate traffic. Cracking its security and decoding the traffic may not be allowed by the scope of work agreement or corporate policy.

16. A, D. One of the main purposes of a Layer 2 audit is to detect initially any rogue devices or unauthorized 802.11 devices. Identifying rogue devices during an initial security audit is critical, especially if a distributed WIPS monitoring solution has not been deployed. A proper Layer 2 WLAN security audit will also be used to identify initially all authorized 802.11 WLAN devices, including access points and authorized clients. The audit can also be used to validate WLAN security compliance. The mandated authentication and encryption of all authorized devices can be evaluated to verify the proper security configuration. Any authorized devices that have not been properly configured will be flagged.

17. A. If there is no physical security for the AP, it could be compromised by an attacker that gains physical access. Since this one is in a common hallway of a multitenant building, there is a very high likelihood of it being compromised or stolen. Physical security of the devices being used is just as important as protecting the communications.

18. E. All of these items are of use. Part of the audit should include physical inspection of authorized devices. This may require the items listed depending on the environment and may require even other tools, such as a GPS.

19. B. Any WLAN protocol analyzer can verify that all corporate WLAN devices are using the proper authentication methods. coWPAtty, Asleap, and Aircrack-ng are used during penetration tests to compromise weaker authentication methods than EAP-TTLS. WLAN discovery tools such as NetStumbler do not capture 802.11 frames but instead find 802.11 devices using null probe request frames.

20. B. Depending on the contents of the toolkit, this is a common practice. WLAN audits and site surveys are similar and the same tools can be used to conduct both types of work. Spectrum analysis and WLAN protocol analyzer tools are widely used in both formats.

Chapter 10

Wireless Security Monitoring

IN THIS CHAPTER, YOU WILL LEARN ABOUT THE FOLLOWING:

- ✓ **Wireless intrusion detection and prevention systems (WIDS and WIPS)**
  - WIDS/WIPS infrastructure components
  - WIDS/WIPS architecture models
  - Multiple radio sensors
  - Sensor placement
- ✓ **Device classification**
  - Rogue detection
  - Rogue mitigation
  - Device tracking
- ✓ **WIDS/WIPS analysis**
  - Signature analysis
  - Behavioral analysis
  - Protocol analysis
  - Spectrum analysis
  - Forensic analysis
  - Performance analysis
- ✓ **Monitoring**
  - Policy enforcement
  - Alarms and notification
  - False positives
  - Reports

- ✓ **802.11n**
- ✓ **Proprietary WIPS**
  - Cloaking
  - Management frame protection
- ✓ **802.11w**

Wireless intrusion monitoring has evolved, and most current systems have methods to prevent and mitigate some of the known wireless attacks. While most systems are distributed for scalability across a large enterprise, single laptop versions of intrusion monitoring systems also exist. Most wireless intrusion monitoring exists at Layer 2, but Layer 1 wireless intrusion monitoring systems are now also available to scan for potential Layer 1 attacks. A large-scale enterprise WLAN requires more than spot checks with handheld scanners and laptop-based tools. These basic tools by themselves are not going to offer the needed level of monitoring or security. Spot checks or mobile scans can be a vital part of a security plan but, by themselves, leave much to be desired as a total solution. Large enterprises require a distributed solution with centralized management capabilities and 24/7 monitoring capabilities. Distributed monitoring solutions may also have prevention capabilities, including mitigating rogue APs and clients. The use of distributed WLAN monitoring and rogue prevention reduces the time and expense required to maintain a healthy and secure
wireless network.

Wireless Intrusion Detection and Prevention Systems (WIDS and WIPS)

When most people think of wireless networking, they think only in terms of access and not in terms of attacks or intrusions. However, it has become increasingly necessary to monitor constantly for many types of WLAN attacks because of the potential damage they can cause. Businesses of all sizes have begun to deploy 802.11 wireless networks for mobility and access and, at the same time, are running a *wireless intrusion detection system (WIDS)* to monitor for attacks. Because many organizations are very concerned about the potential damage that results from rogue access points, it is not unusual for a company to deploy a WIDS prior to deploying the WLAN that is meant to provide wireless client acces. Most WIDS vendors prefer to call their product a *wireless intrusion prevention system (WIPS)*. The reason that they refer to their products as prevention systems is that all of them are now capable of mitigating attacks from rogue access points and rogue clients.

Wireless intrusion detection systems and wireless intrusion prevention systems share many common features that help administrators and security staff members alike in the maintenance and protection of WLAN traffic. WIDSs and WIPSs both use a combination of sensors and appliances in the gathering and analysis of wireless traffic. Some also use information gained from integration with managed switches and WLAN controllers as well as information reported from access points. The key thing to understand about WIDSs and WIPSs is that they use the same information that an auditor or an administrator would gather using laptop-based tools or handheld devices to conduct an audit, but do so 24 hours per day using distributed sensors. A WIDS solution gathers information from the 802.11 radio transmissions detected by multiple sensors and then correlates the captured information. A distributed WIDS solution offers the scalability that cannot be provided by an auditor with a single protocol analyzer.

WIPSs act in a similar manner, with the additional capability of being able to keep rogue stations off legitimate WLANs, and some even help keep rogue APs off the wired network. WIPS are also able to enforce WLAN policy to stop authorized stations from engaging in unauthorized behaviors, such as connecting to unauthorized APs, forming ad hoc connections, and communicating without using approved authentication and encryption methods. Their names describe their functions; a WIDS detects and notifies about potential attacks, whereas a WIPS functions as a WIDS while additionally protecting the WLAN using various methods beyond simple detection and notification.

WIDS/WIPS Infrastructure Components

The components of a WIDS/WIPS and their abilities vary from manufacturer to manufacturer. However, their core functions and hardware are similar. The typical WIDS/WIPS solution is a distributed client/server model that consists of three primary components:

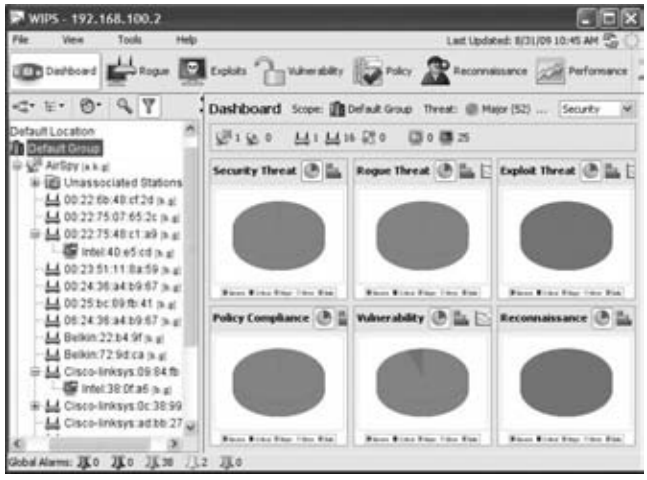
- WIDS/WIPS server
- Management consoles
- Sensors

A *WIDS/WIPS server* is a software server or hardware server appliance acting as a central point of monitoring security and performance data collection. The server uses signature analysis, behavior analysis, protocol analysis, and RF spectrum analysis to detect potential threats. Signature analysis looks for patterns associated with common WLAN attacks. Behavior analysis looks for 802.11 anomalies. Protocol analysis dissects the MAC layer information from 802.11 frames. Protocol analysis may also look at the Layer 3–7

information of 802.11 data frames that are not encrypted. Spectrum analysis monitors RF statistics, such as signal strength and signal-to-noise ratio (SNR). Performance analysis can be used to gauge WLAN health statistics, such as capacity and coverage.

A software-based *management console* is used to communicate back to a WIDS/WIPS server from a desktop station. As you can see in Figure 10.1, the management console is the software interface used for administration and configuration of the server and sensors. The management console can also be used for 24/7 monitoring of 802.11 wireless networks.

FIGURE 10.1 WIDS/WIPS management console



Hardware or software-based *sensors* may be placed strategically to listen to and capture all 802.11 communications. Sensors are the eyes and ears of a WIDS/WIPS monitoring solution. Sensors use 802.11 radios to collect information used in securing and analyzing WLAN traffic. As shown in Figure 10.2, WIDS/WIPS sensors use 802.11 radio chipsets and most often the same hardware as 802.11 access points. However, the sensors are tasked with being a listening device rather than an AP that provides client access. Sensors constantly scan across all 14 channels of the 2.4 GHz ISM band as well as all 23 channels of the 5 GHz UNII frequency bands. Although rarely used in WLAN deployments, Channel 165 of the 5 GHz ISM band is also often monitored as well as some channels in 4.9 GHz range, which is reserved for public safety in the United States

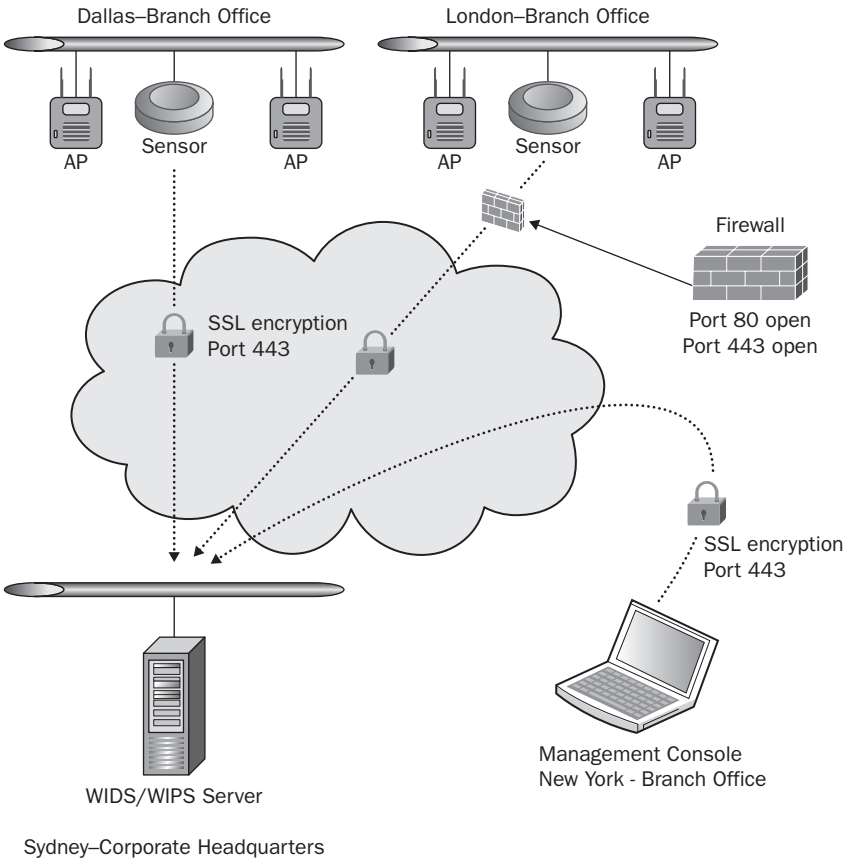
but is a common channel band in Japan. The channel scanning interval is usually set at a fixed rate between 100 ms to 1 second. However, the channel scanning interval can be adjusted for shorter or longer times. Usually sensors are set to continuously scan across all 802.11 channels. Sensors can also be configured to monitor on a single fixed channel. The majority of WIDS/WIPS sensors are hardware based. Some WIDS/WIPS solutions offer sensor software that can be installed on computer. The sensor software can then use the computer's 802.11 radio for scanning. Figure 10.2 shows a Fluke Networks AirMagnet hardware sensor and a Motorola AirDefense hardware sensor.

FIGURE 10.2 WIDS/WIPS hardware sensors

Communications from the sensors and management consoles back to the server are usually proprietary protocols, which are usually protected by an encrypted *secure-sockets-layer (SSL)* tunnel. Typically, a sensor also sends a continuous heartbeat message back to the IDS server to indicate that the sensor is still functional. Sensors can usually be centrally managed from the management console interface or may also be managed individually through telnet, SSH, or a web browser. Most applications use port 80 for web management and port 883 for SSL communications. These ports will need to be open on any firewall located between a sensor and the WIDS/WIPS server. Depending on the vendor, other vendor-specific ports may also need to be open to permit communications between the sensors and the WIDS/WIPS server. Sensors may also be used for remote packet capturing.

As shown in Figure 10.3, the three components of the WIDS/WIPS distributed architecture can exist at a single WLAN enterprise site or can scale to monitor multiple WLAN sites across a wide area network (WAN). The WIDS/WIPS server might reside in Sydney, Australia, while the WLANs that are being monitored may reside in Dallas and London. The management console usually resides at the network operations center (NOC) along with the server, but a management console can also exist at another remote location.

FIGURE 10.3 WIDS/WIPS distributed architecture



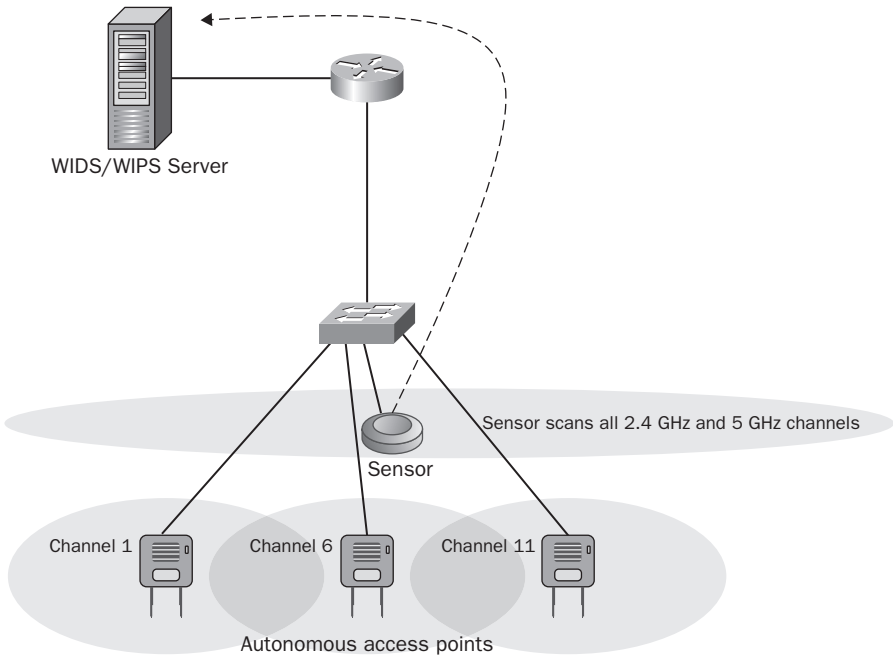
WIDS/WIPS Architecture Models

The three major components of a WIDS/WIPS solution can monitor an 802.11 WLAN using one of three of the following architecture models:

- Overlay
- Integrated
- Integration Enabled

As Figure 10.4 shows, an *overlay* WIDS/WIPS architecture is deployed on top of the existing wireless network. This model uses an independent vendor's WIDS/WIPS solution and can be deployed to monitor any preexisting or planned WLAN. The overlay systems typically have more extensive features and monitoring capabilities, but they are usually more expensive. The overlay solution consists of a WIDS server and sensors that are not part of the WLAN solution that provides access to clients.

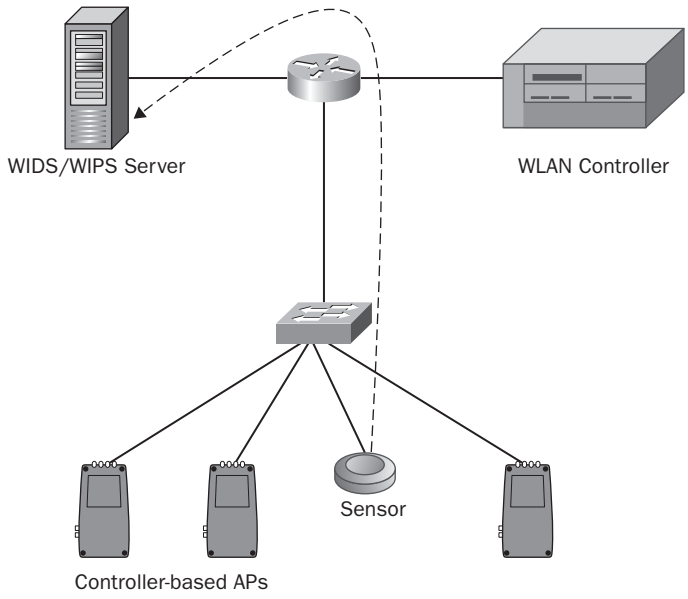
FIGURE 10.4 Overlay WIDS/WIPS—autonomous APs



Overlay architecture can be used to monitor a WLAN that uses autonomous APs, as shown in Figure 10.4, or can be used to monitor the more common WLAN controller solutions, as shown in Figure 10.5.

An overlay solution uses *standalone sensors* to monitor the preexisting WLAN. Standalone sensors use dedicated radios that function only as sensors and are not used as APs. The standalone sensors require their own cable run and communicate back to the WIDS/WIPS server over the IP network. Usually, standalone sensors can use a single 802.11a/b/g radio to monitor both the 2.4 GHz ISM band and the 5 GHz UNII bands.

FIGURE 10.5 Overlay WIDS/WIPS—WLAN controller



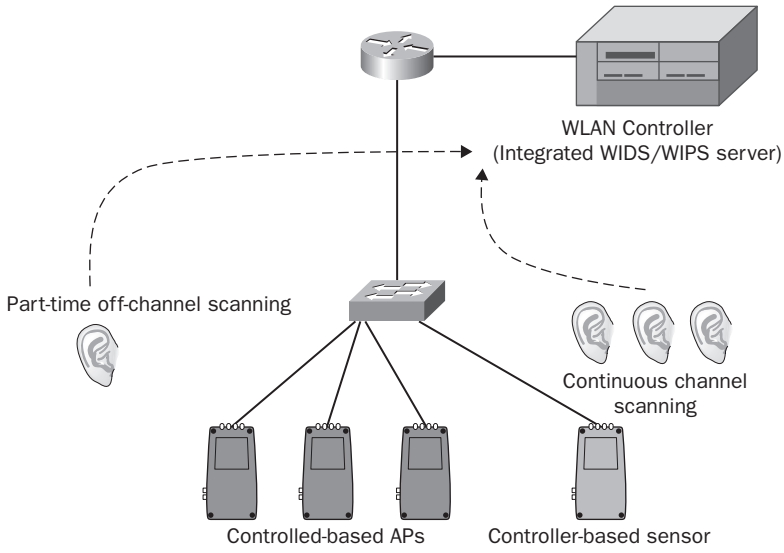
Standalone sensors may also have two radios: one to monitor the 2.4 GHz channels and another to monitor the 5 GHz channels.

Overlay solutions increase hardware and deployment costs but generally offer more functionality. Overlay WIDS/WIPS servers typically use a wider range of attack signatures to recognize potential threats and collect more information for WLAN health analysis. Another major advantage of the overlay model is that if the WLAN goes down, the WIDS/WIPS monitoring continues because the overlay solution is independent of the WLAN infrastructure.

An *integrated* WIDS/WIPS architecture is used by many of the WLAN controller vendors using the WLAN architecture to provide client access and security monitoring. As shown in Figure 10.6, the centralized WIDS/WIPS server exists as a software module within the WLAN controller. The WLAN controller-based access points can be configured in a full-time sensor-only mode or can act as part-time sensors when not transmitting as access points. WLAN controller-based APs are often called "thin" APs or "lightweight" APs. The controller-based APs have full access point functionality and are centrally managed by the WLAN controller. In most WLAN controller designs, the APs tunnel all of the 802.11 client traffic back to the WLAN controller. You can find further discussion about WLAN controllers in Chapter 12, "Wireless Security Infrastructure."

Controller-based APs have the capability to be converted to *full-time sensors*. Instead of providing access to clients, the controller-based APs scan all channels, continuously listening for attacks. Most controller-based APs use a *software defined radio (SDR)* that

FIGURE 10.6 Integrated WIDS/WIPS



has the ability to operate either as a 2.4 GHz transceiver or as a 5 GHz transceiver, but it cannot transmit on both frequency bands at the same time. However, because the SDR uses a dual-frequency chipset, a single radio access point that has been converted into a full-time sensor can listen to both the 2.4 GHz and 5 GHz frequency bands. Many controller-based APs have two radios, both of which can be converted to a sensor. One radio can monitor the 2.4 GHz channels while the other radio monitors the 5 GHz channels. A lightweight AP with two radios could also be used to provide access on a single frequency band while the other radio is used as a full-time sensor to scan the channels of both bands.

Most controller-based APs also function as part-time sensors. In WLAN controller deployments, the controller-based access points use *off-channel scanning* procedures for dynamic RF spectrum management purposes. For example, a controller-based AP that is providing client access on channel six will monitor other channels as well. The AP will stay on channel six for 10 seconds. During the 10-second interval, the AP is capable of sending transmissions to an associated client as well as receiving transmissions from an associated client. After the 10-second interval, the AP will listen off-channel on channel seven for 110 ms. The AP will then return to channel six for 10 seconds and then go off-channel to monitor channel eight for 110 ms. This round-robin method of off-channel scanning is used by the APs to listen for the beacon frame transmissions of other access points as well as monitor for any other RF transmissions off-channel. Any RF information heard by any of the lightweight access points is reported back to the WLAN controller. Based on all the RF monitoring from multiple access points, the WLAN controller will make dynamic changes

to the RF settings of the controller-based APs. Some controller-based access points may be told to change to a different channel, while other APs may be told to change their transmit power settings. Although the main purpose of off-channel scanning is to provide dynamic RF capabilities, the off-channel scanning also allows the APs to be *part-time sensors* for the WIDS/WIPS server module in the WLAN controller. The off-channel scanning used by the controller-based APs effectively provides time slicing between AP and sensor functionality.

Time slicing between AP and sensor functionality may reduce hardware and deployment expense, but offers limited detection and prevention. Many customers of WLAN controller vendors opt not to pay for the extra expense of deploying some controller-based APs as full-time sensors and only use the part-time, time-slicing capabilities of the access points. If you hired a security guard to watch the main entrance to your place of business, would you want the security guard to take a break for 55 minutes every hour and only watch the main gate for 5 minutes of each hour? An attacker might recognize that a WIPS solution is only using part-time sensors. The attacker could launch a brief attack during the period that the APs are providing access. The attack occurs when the AP is not performing off-channel scanning and the attack is therefore not detected.

Another problem with part-time sensors is that they may suspend off-channel scanning if a VoWiFi phone is associated with the access point. Off-channel scanning is notorious for causing "choppy audio" during an active voice call from a VoWiFi device associated to a controller-based AP. Most WLAN controller vendors now have an option that suspends off-channel scanning if any voice protocols, such as Session Initiation Protocol (SIP) or SpectraLink Radio Protocol (SRP), are detected. If the off-channel scanning is suspended due to VoWiFi communications, the WLAN security monitoring is also suspended.

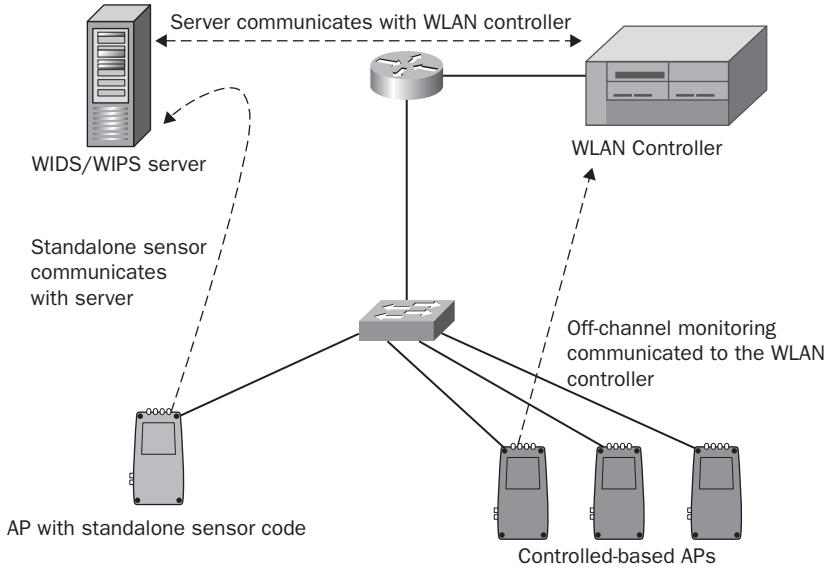
An additional problem with part-time sensors is wireless rogue containment, which will be discussed later in this chapter. If a time slicing AP/sensor must go off-channel for an extended period of time to contain a rogue device, the AP is not on its home channel providing access to clients. It should be noted, however, that most WLAN controller companies support a configuration setting that prevents a time slicing AP/sensor from performing wireless rogue containment when clients are associated.

Although the controller-based APs act as part-time sensors for the integrated IDS server, it is a highly recommended practice also to deploy some controller-based APs as full-time sensors when using an integrated WIDS/WIPS server solution.

An *integrated-enabled* WIDS/WIPS architecture is used by Wi-Fi vendors to integrate their WLAN architecture and management systems with the overlay WIDS/WIPS vendors that use a standalone server. The Wi-Fi vendor's access points integrate software code that can be used to turn the APs into sensors that will communicate with the third-party WIDS/WIPS server. Originally, integration-enabled solutions existed primarily for the purpose of converting autonomous access points into sensors that communicated with a third-party WIDS/WIPS server. However, integration-enabled solutions now exist in WLAN controller-based deployments. As shown in Figure 10.7, a lightweight access point is converted into a full-time sensor that communicates directly with a separate WIDS/WIPS server and no longer communicates directly with the WLAN controller. Effectively, the controller-based access

point is now a standalone sensor. At the same time, other controller-based access points still send WLAN traffic to the WLAN controller to provide access for WLAN clients. Furthermore, an integration-enabled WIDS/WIPS server may also communicate directly with the WLAN controller to gather additional monitoring information from the controller-based access points that speak only with the controller. Although the controller-based APs do not communicate directly with the WIDS/WIPS server, monitoring information obtained during the off-channel scanning used primarily for dynamic RF can still be utilized for security monitoring. The independent WIDS/WIPS server compiles information from both the standalone sensors and the WLAN controller.

FIGURE 10.7 Integrated-enabled WIDS/WIPS



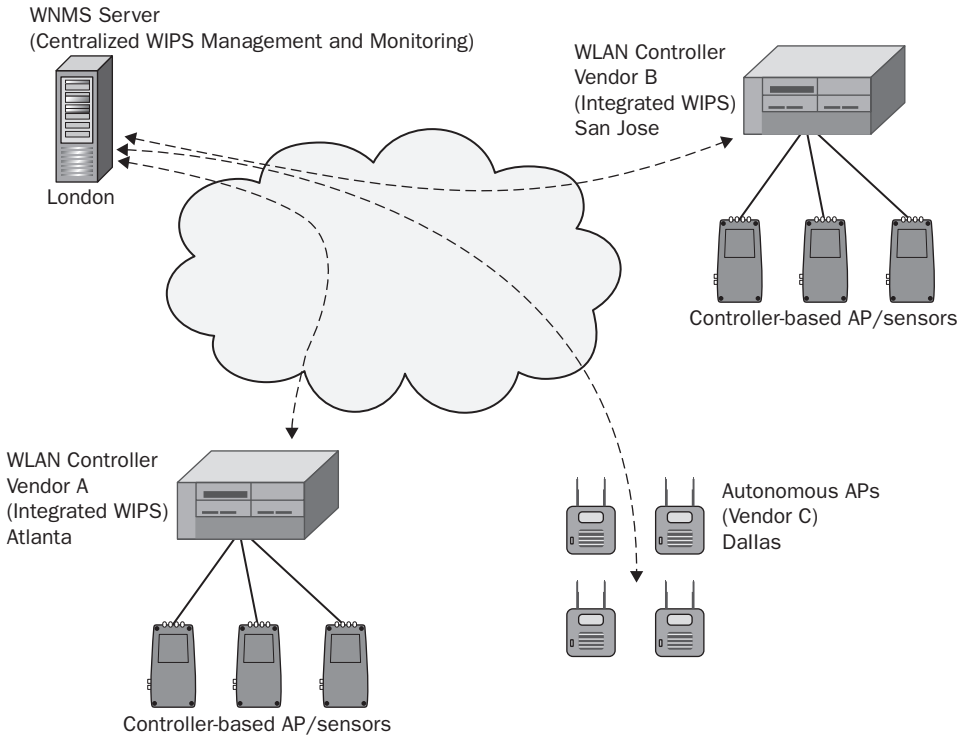
Some large-scale enterprise WLAN deployments use a *wireless network management system (WNMS)* server. A WNMS server provides a central point of management to configure WLAN devices and push firmware to WLAN devices. WNMS solutions can be either vender specific or vender neutral. In the past, the whole point of a WNMS server was to provide a central point of management for autonomous access points. Eventually, WLAN controllers effectively replaced WNMS servers as a central point of management for access points. However, at times, multiple WLAN controllers are needed in large-scale WLAN enterprise deployments. Currently, most WNMS servers are used as a central point of management for multiple WLAN controllers in a large-scale WLAN enterprise. The current WNMS servers that are used to manage multiple WLAN controllers from a single vendor may also be used to manage other vendors' WLAN infrastructure, including autonomous APs. An enterprise WIDS/WIPS may be configured to work together with a wireless network management system (WNMS) that allows for security alerts to be monitored from a centralized location.

Wireless Network Management System (WNMS)

An example of a third-party WNMS solution would be the AirWave Management Platform (AMP), which can be used for WLAN management and monitoring. You can learn more about the AirWave solution online at `www.airwave.com/resources/technology-tours`.

As shown in Figure 10.8, some large-scale enterprise deployments may use a WNMS server as a centralized WIDS/WIPS management and monitoring solution, drawing information from controllers and APs alike.

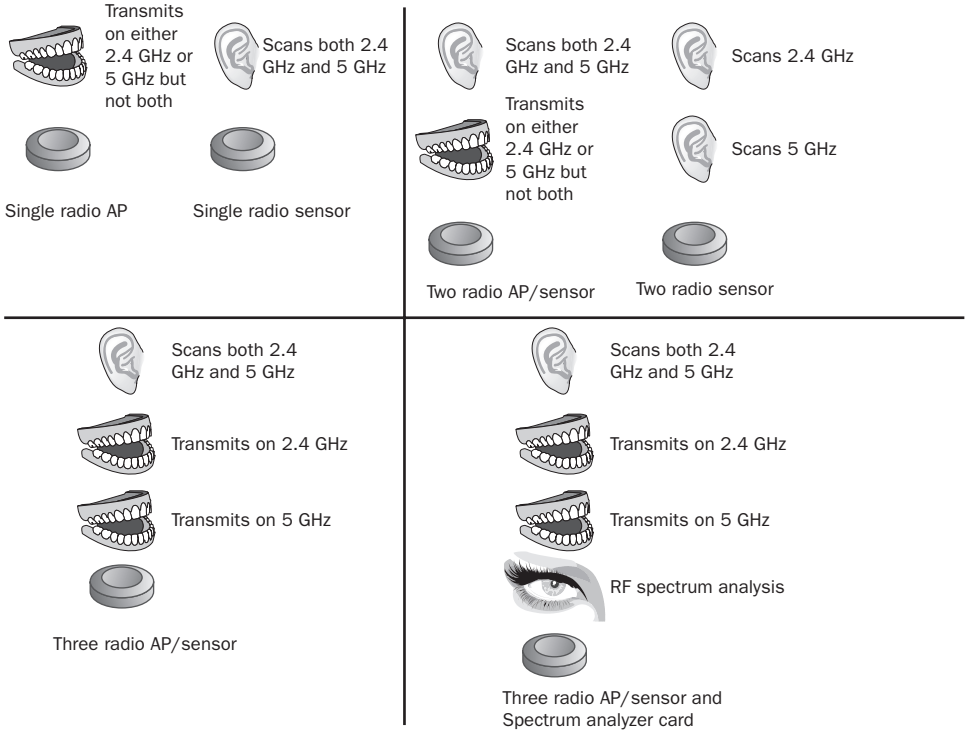
Figure 10.8 WNMS for security monitoring



Multiple Radio Sensors

As Figure 10.9 shows, the latest innovations in WLAN security monitoring use multiple radio devices that are not locked to a frequency, protocol, or function. This innovative technique allows a single cable drop to be used, thereby reducing deployment costs; a single housing to be used, thus reducing hardware costs; and multiple radios to be used in the housing, thereby increasing functionality. A device with three radios can use one radio for 2.4 GHz coverage, one radio for 5 GHz coverage, and the third radio as a sensor to monitor and scan both bands. In a mesh deployment, one radio can be used as a 2.4 GHz AP for local coverage, one for a 5 GHz mesh back-haul connection, and a third as a sensor for the coverage area. Some WLAN vendors are even making 802.11 devices with three radios along with a modular spectrum analyzer card used for RF spectrum analysis. Multiple radio devices allow WLAN coverage and WIDS/WIPS on separate dedicated radios, increasing security and WLAN performance monitoring abilities at a reduced expense.

FIGURE 10.9 Multiple 802.11 radio devices

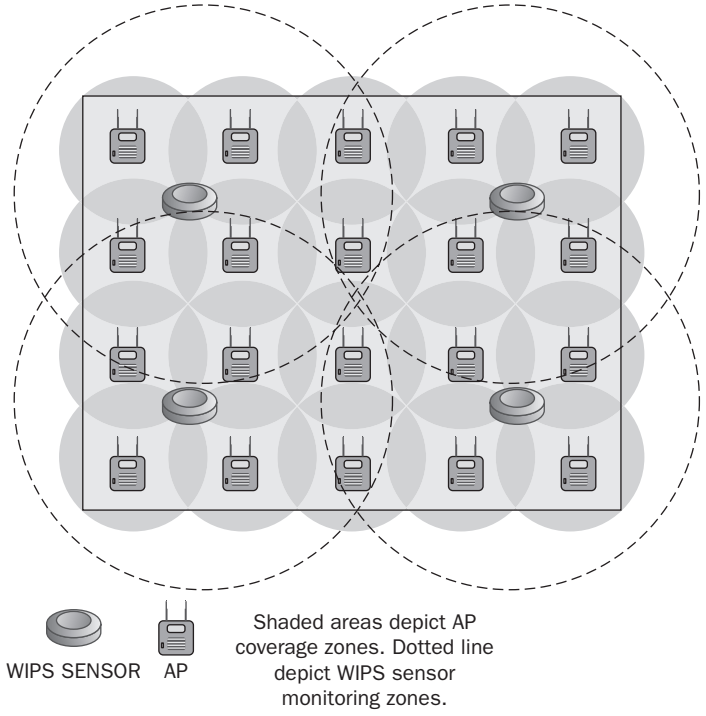


Sensor Placement

Sensor placement is an often-discussed topic when deploying a WIDS/WIPS solution. The question that is always asked is "How many sensors do I need?" The answer often depends on the budget and the value of what network resources are being protected by WLAN security monitoring. The best answer is that you can never have too many sensors. When WLAN security monitoring is deployed, the more ears the better.

Every WLAN vendor has their own sensor deployment recommendations and guidelines; however, a ratio of one sensor for every three-to-five access points is highly recommended. As shown in Figure 10.10, full-time sensors are often placed strategically at the intersection points of three AP coverage cells. A common mistake is placing the sensors in a straight line as opposed to staggered sensor arrangement (which will assure a wider area of monitoring). Another common sensor placement recommendation is to arrange sensors around the perimeter of the building. Perimeter placement increases the effectiveness of triangulation and also helps to detect WLAN devices that might be outside the building. Some of the better WLAN predictive modeling software solutions will also create models for recommended sensor placement.

FIGURE 10.10 Sensor placement



If an integrated WIDS/WIPS solution is deployed, all access points are controller-based and are deployed as part-time sensors. Once again, it is strongly recommended to deploy full-time sensors with an integrated solution. When WLAN security monitoring is an extremely high priority and cost is not an issue, the more sensor devices the better. WIDS/WIPS deployments at military bases often follow a ratio of one sensor for ever two APs or may even deploy sensors with a 1:1 ratio.

Device Classification

Although the upper-layer payload of 802.11 data frames is usually encrypted, the Layer 2 information remains exposed to allow for MAC layer communications to occur. All Layer 2 information is captured and analyzed by WIDS/WIPS solutions. Any 802.11-based device transmitting within the hearing range of a sensor will eventually be detected as the sensor sweeps the channels. WIDS/WIPS can also integrate with WLAN controllers and access layer switches pulling information from them for use in detecting wired devices. Information freely available in 802.11 management frames will allow the WIDS/WIPS initially to determine if an 802.11 device is an access point, client station, or ad hoc client station. If an 802.11 wireless device is transmitting within the hearing range of a sensor, it will be detected by the WIDS/WIPS and then will be classified as shown in Figure 10.11.

FIGURE 10.11 WIDS/WIPS device classification

Most WIDS/WIPS vendors categorize access points and client stations in four or more classifications. Wi-Fi vendors may have different names for the various classifications, but most solutions classify 802.11 radios as follows:

Authorized Device This classification refers to any client station or access point that is an authorized member of the company's wireless network. An overlay WIDS/WIPS solution usually requires initial manual input to classify radios as authorized infrastructure devices. A network administrator can manually label each radio as an infrastructure device after detection from the WIPS or can import a list of all the company's radio card MAC addresses into the system. Devices may also be authorized in bulk from a comma-delimited file. Integrated solutions automatically classify any controller-based APs as authorized devices. An integrated solution will also automatically classify client stations as authorized if the client stations are properly authenticated.

Unauthorized Device The unauthorized device classification is assigned automatically to any new 802.11 radios that have been detected but not classified as rogues. Unknown

devices are considered to be unauthorized and are usually investigated further to determine whether they are a neighbor's device or a potential future threat. Unauthorized devices may later be manually classified as a known neighbor device.

Neighbor Device This classification refers to any client station or access point that is detected by the WIPS and whose identity is known. This type of device initially is detected as an unauthorized device. The neighbor device label is then typically assigned manually by an administrator. Devices manually classified as known are most often 802.11 access points or client radio devices of neighboring businesses that are not considered a threat.

Rogue Device The rogue classification refers to any client station or access point that is considered an interfering device and a potential threat. Most WIDS/WIPS solutions define rogue access points as devices that are actually plugged into the wired network backbone and are not known or managed by the organization. Most of the WIDS/WIPS vendors use a variety of methods to determine whether a rogue access point is actually plugged into the wired infrastructure.

Many WIDS/WIPS solutions also have the ability to conduct *auto-classification*. As shown in Figure 10.12, WLAN devices can be automatically added to any classification based on a variety of variables, including authentication method, encryption method, SSID, IP addresses, and so on. Auto-classification capabilities should be used carefully to ensure that only proper devices are classified as authorized.

FIGURE 10.12 WIDS/WIPS device auto-classification

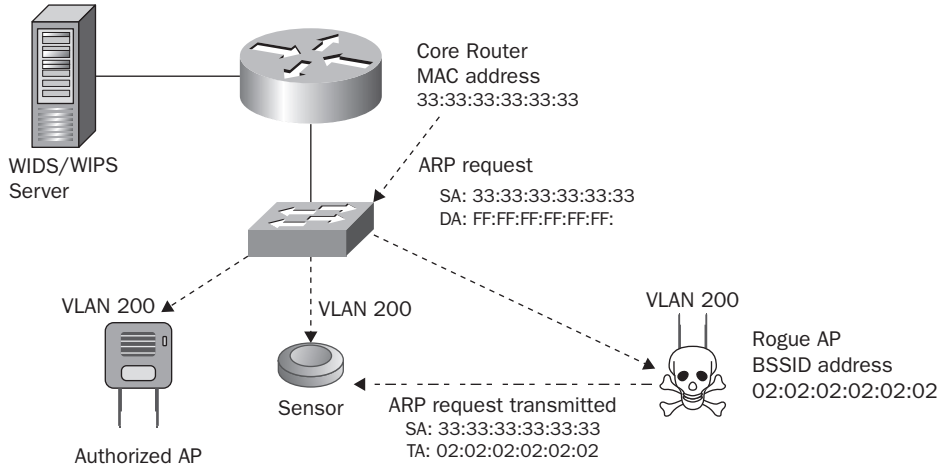
Rogue Detection

As already mentioned, most WIDS/WIPS define rogue APs as devices that are actually plugged into the wired network. Most of the WIDS/WIPS vendors use a variety of wireless and wired detection methods to determine whether a rogue access point is actually plugged into the wired infrastructure. Some of the rogue detection and classification methods are published while many remain proprietary and trade secrets. Any 802.11 device that is not already authorized will automatically be classified as an unauthorized device. However, rogue classification is a little more complex.

One effective approach for classifying rogue APs is to poll access layer switches with *Simple Network Management Protocol (SNMP)* to determine MAC addresses associated with each physical port on the switch. Given that an AP acts as a Layer 2 bridge, the WIDS/WIPS solution builds a MAC table that correlates both the wired-side MAC address and wireless-side MAC address (BSSID) of the access point. This correlated MAC table can then be compared to the database of authorized devices. Any unauthorized device that is detected by both a sensor on the wireless side and by SNMP on the wired side will then be classified as a rogue AP.

As shown in Figure 10.13, another method often used to determine whether a device is connected to the wired backbone is by looking at ARP requests from a wired device, such as a core router, and analyzing MAC tables. The following is an example of steps that would have to occur to classify the device as a rogue:

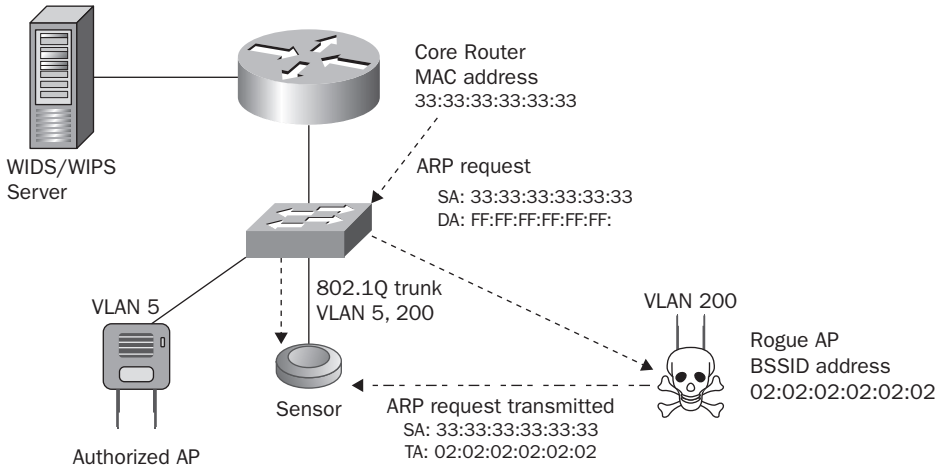
FIGURE 10.13 Rogue detection—single broadcast domain



1. A rogue AP with BSSID of 02:02:02:02:02:02 is plugged into the wired network.
2. A sensor detects a new BSSID on the air and initially classifies this AP as unauthorized. The new AP has not yet been classified as a rogue AP.
3. A default gateway router on the wired network with the MAC address 33:33:33:33:33:33 broadcasts an ARP request packet looking for a host on a particular subnet. Because this ARP packet is a broadcast packet, the rogue AP receives the packet and transmits it out the wireless interface.
4. If the sensor and authorized APs are on the same subnet as the rogue AP, the sensor receives the ARP broadcast on its wired interface. This MAC address is stored in the wired-side MAC table and is shared with all other sensors within the WIDS.
5. When the ARP packet is transmitted into the air by the rogue AP, the source address (SA) is the originating router's address of 33:33:33:33:33:33, and the transmitter address is the BSSID of the rogue 02:02:02:02:02:02.
6. The WIDS/WIPS solution will look at the wired/wireless MAC tables. Any unauthorized BSSID transmitting an ARP request with the source address of the wired router will now be classified as a rogue AP.

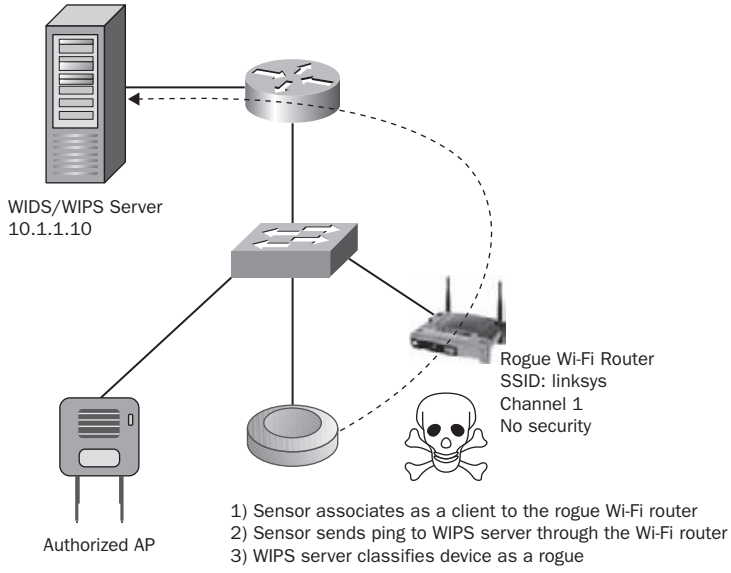
This will only work if the rogue device is plugged into the same broadcast domain as the sensor. Because many networks are designed with a large number of VLANs, a rogue AP could be plugged into a different VLAN than the sensors. As Figure 10.14 shows, the sensor would need to have an 802.1Q trunk link in order to receive the ARP request from the wired side.

FIGURE 10.14 Rogue detection—trunked sensor



All of these rogue detection and classification methods work well if the rogue device is indeed an access point. An access point is a Layer 2 device that bridges the 802.3 Ethernet interface and the 802.11 radio interface. Unfortunately, most rogue devices that are installed are low-cost home Wi-Fi routers and are not bridged devices. Therefore, most rogue devices have separate Layer 3 interfaces and are normally configured to use network address translation (NAT). As shown in Figure 10.15, one method of classifying Layer 3 rogue devices is to have a nearby sensor associate as a client station to the unauthorized suspect rogue AP or Wi-Fi router. The sensor then sends traffic, such as a ping, back to the WIDS/WIPS server. If the traffic reaches the server on the wired side, the suspected rogue AP is confirmed to be on the internal network and then classified as a rogue.

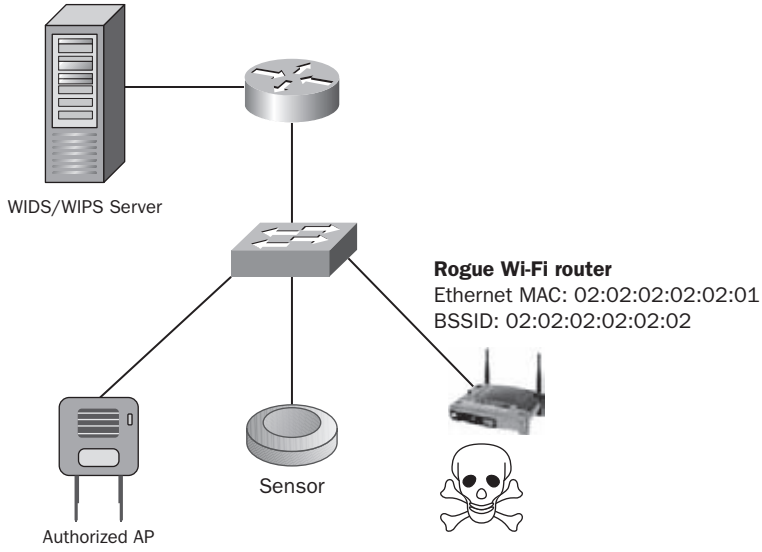
FIGURE 10.15 Layer 3 Rogue detection—active sensor



The problem with this method is that very often a rogue AP will have configured security, such as WEP or WPA. A sensor will not be able to associate with the rogue AP and send traffic because the sensor does not know the rogue APs security settings.

Luckily, the majority of the WLAN vendors that manufacture home Wi-Fi routers use MAC addresses that are one bit apart on the wireless and wired interfaces. As shown in Figure 10.16, the methods of Layer 2 rogue detection mentioned earlier can be augmented by looking for wired MAC addresses one bit higher or one bit lower than the BSSID detected by a sensor.

FIGURE 10.16 Layer 3 Rogue detection—1 bit MAC comparison



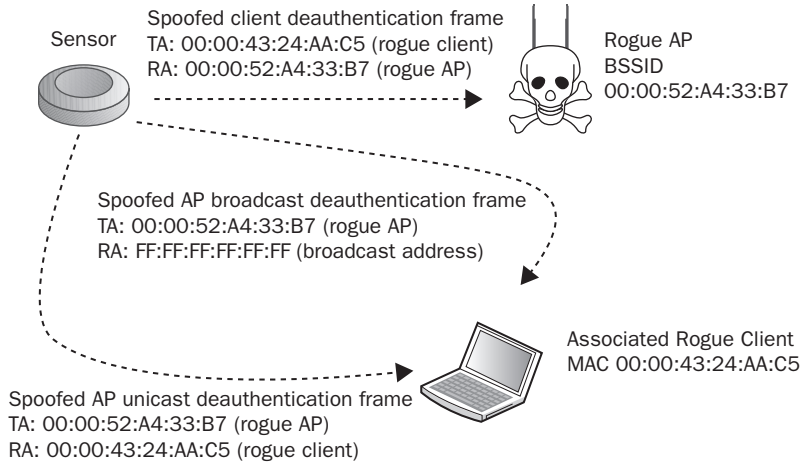
Another method for possibly determining whether there is a potential rogue device connected to the wired network is to examine the *time to live (TTL)* values of IP packets. Wi-Fi routers will lower the TTL value of a packet when it flows through the device. As mentioned earlier, WIDS/WIPS vendors may also use proprietary methods of rogue detection and classification. Although the art of rogue detection and classification has become quite successful, any device that is initially classified as unauthorized should also be investigated and treated as a potential rogue threat until determined otherwise. Once an unauthorized 802.11 device has been determined not to be a threat, the device can then be classified manually as a neighbor device.

Rogue Mitigation

Once a client station or access point has been classified as a rogue device, the WIPS can effectively mitigate the attack. Every WIPS vendor has several ways of accomplishing this, but the most common method is wireless *rogue containment* using spoofed deauthentication frames. Rogue containment is accomplished wirelessly when the WIPS' sensors become active and begin transmitting deauthentication frames that spoof the MAC addresses of the rogue access points, rogue ad hoc networks, and rogue clients. The WIPS is using a known Layer 2 denial-of-service attack as a countermeasure. The effect is that all communications between the rogue access point and clients are rendered useless. Any client devices trying to communicate through the rogue AP will be deauthenticated at Layer 2 and all upper-layer 3–7 communications will be disrupted. This prevents an attacker from accessing network resources through the unauthorized portal of the rogue AP. This also prevents accidental associations of legitimate clients to the rogue AP. This

countermeasure can be used to disable rogue access points, individual client stations, and rogue ad hoc networks. Every WIPS vendor has their own marketing name for Layer 2 wireless rogue containment, including air termination, rogue blocking, and rogue disabling. As shown in Figure 10.17, the sensor transmits deauthentication frames spoofing the rogue APs MAC address as the transmitter address (TA). The receiver address (RA) of the spoofed frames may be a broadcast address to deauthenticate all client stations or may be a unicast address to a single, associated rogue client station. Hackers have figured out how to tinker with client card firmware so that client stations will ignore deauthentication frames. Therefore, as shown in Figure 10.17, most WIPS sensors will also transmit deauthentication frames spoofing the client station's MAC address as the transmitter address and spoofing the rogue AP MAC address as the receiver address.

FIGURE 10.17 Wireless rogue containment



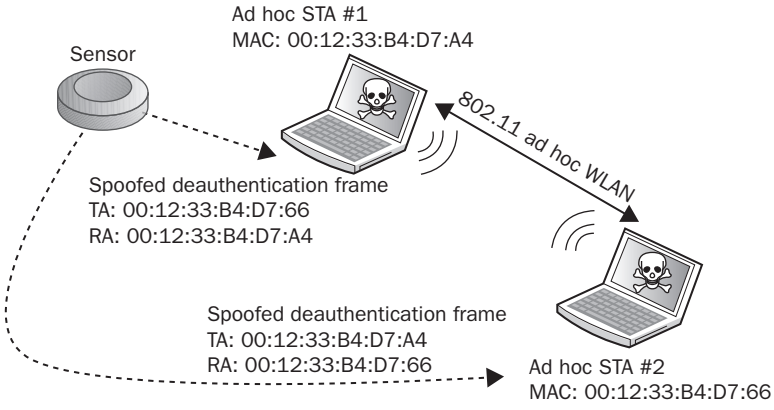
Wireless rogue containment should be used very carefully. Rogue devices can be manually terminated using wireless rogue containment or a WIPS can be configured to automatically terminate any devices that are classified as rogue. Many WIPS can also be configured to terminate all devices except for those that are classified as authorized. Using a deauthentication countermeasure against all unauthorized devices is usually not a good idea because the WIPS may accidently terminate legitimate APs and clients from neighboring businesses. Improper use of wireless rogue containment capabilities can create legal problems. Any device that has been classified as rogue is a device that has been determined by the WIPS to be connected to the corporate backbone and probably should be wirelessly contained automatically. However, some organizations choose to only use wireless rogue containment as a manual procedure when rogue devices are discovered.

As mentioned earlier in this chapter, if a WLAN controller solution with an integrated WIPS is deployed, using the APs for rogue containment is not a recommended practice. If a time slicing AP/sensor must go off-channel for an extended period of time to contain a rogue

device, the AP is not on its home channel providing access to clients. If the AP is performing rogue containment instead of providing access, the performance of the WLAN can be affected. Most WLAN controller companies have a configuration setting that prevents a time slicing AP/sensor from performing rogue termination when clients are associated. If clients are associated to all the APs, then rogue containment may not occur when needed. Although the controller-based access points act as part-time sensors for the integrated IDS server, it is a highly recommended practice also to deploy some controller-based APs as full-time sensors when using an integrated WIDS/WIPS server solution. The full-time sensors would be used for rogue containment instead of the time slicing AP/sensors.

As mentioned in Chapter 8, "Wireless Security Risks," ad hoc WLANs are a huge security risk because the Ethernet connection and the Wi-Fi card can be bridged together. An intruder might also access the ad hoc WLAN and then potentially route their way to the Ethernet connection and get onto the wired network. A WIPS solution can easily detect an ad hoc WLAN because ad hoc stations transmit 802.11 Beacon frames that indicate they are participating in an *independent basic service set (IBSS)*. As shown in Figure 10.18, after detecting the ad hoc stations, a WIPS can send spoofed deauthentication frames to disrupt communications within the IBSS. Automatic wireless termination of ad hoc WLANs is usually recommended.

FIGURE 10.18 Ad hoc containment



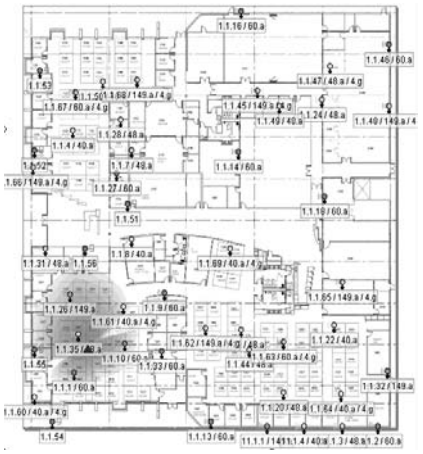
Many WIPS also use a wired-side termination process to effectively mitigate rogue devices. The wired-side termination method of rogue mitigation uses the Simple Network Management Protocol (SNMP) for *port suppression*. Most WIPSs can determine that the rogue access point is connected to the wired infrastructure and may be able to use SNMP to disable the managed switch port that is connected to the rogue access point. Port suppression uses an SNMP agent to shut down the physical port on the network switch through which a rogue device is communicating. If the physical port on the switch is disabled, the gateway to wired network is effectively closed and an attacker cannot use the rogue AP to access network resources.

WIPS vendors have other proprietary methods of disabling rogue access points and client stations and often their methods are not published. Currently, the main attack mitigated by a WIPS is rogue devices. In the future, other wireless attacks might be mitigated as well.

Device Tracking

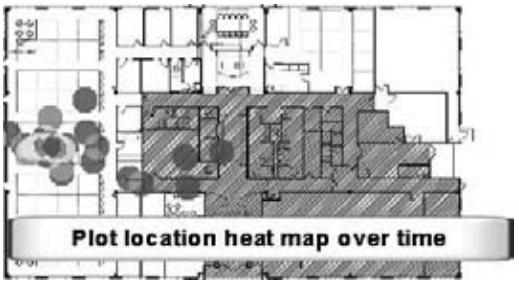
Once a device has been detected and classified, the internal monitoring capabilities of a WIDS/WIPS server can be used to locate the device. As shown in Figure 10.19, the location of devices can be shown visually onto a graphic image of the building's floor plan that has been imported into the WIDS/WIPS server. Location tracking is often used to pinpoint the location of rogue APs, but *location tracking* can also be used to establish the vicinity of authorized APs and client stations.

FIGURE 10.19 Location tracking



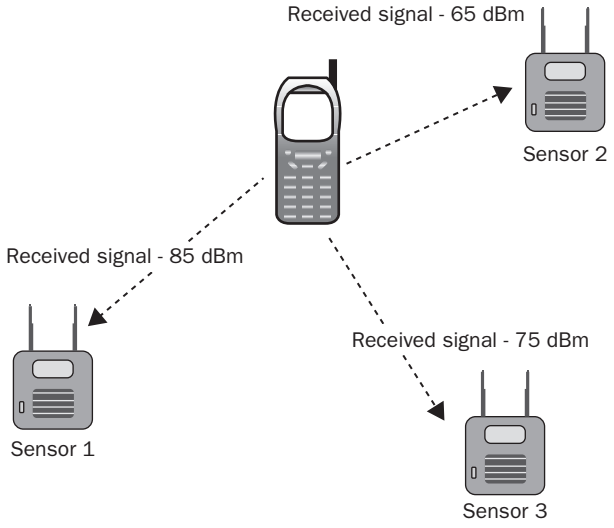
The method used to find devices will vary based on vendor implementation and optional configurations. Some methods of location tracking use *received signal strength indicator (RSSI)* values reported from sensors and authorized APs within listening range of the device being tracked. Newer features also include historical location tracking. As shown in Figure 10.20, historical tracking allows the WIDS/WIPS to show where a device has been detected in the past, even if the device is not currently transmitting. Historical tracking capabilities are used to monitor the movements of rogue client stations. Historical tracking also provides data that can be used to find missing devices, such as handheld scanners that may have become misplaced in a retail, warehousing, or logistics environment. Furthermore, the historical data can also be used to find trends in worker movement throughout the day as required by their jobs. Whether the device you have detected is rogue, authorized, or just neighboring, it eventually becomes necessary to know the physical location of a device.

FIGURE 10.20 Historical tracking



The most common location tracking method is known as *RF triangulation*. Triangulation, as it relates to WIDS/WIPS, is a way of using received signals detected by sensors that are in known locations to find devices that are in unknown locations. Within the WIDS/WIPS tracking module, sensors are positioned on a map of the area where the sensors are actually deployed. Each sensor reporting that it hears the target device provides a data point for use in finding the target based upon the RSSI value of the target's signal. Sensors that detect the target with stronger signal strength, a higher RSSI value, are believed to be closer to the target. Those sensors detecting the target with weaker signal strength, a lower RSSI value, are determined to be farther away from the target. Because RSSI provides an estimate of distance but not direction, at least three sensors are needed to determine the location of a monitored device. As shown in Figure 10.21, RF triangulation provides an approximation of the target's location based solely on the varied RSSI values detected and reported by multiple sensors.

FIGURE 10.21 RF triangulation



RF triangulation usually results in an estimated location within approximately 10 meters. However, this method does not take into account the RF noise in the area, nor does it account for the attenuation, reflection, absorption, scattering, or multipath that may be occurring as the target's signal propagates throughout the area. The antenna orientation of a mobile client station will also affect the RSSI measurement. The accuracy of RSSI measurement is affected by distance as well. The doubling of the distance between a sensor and a device tends to double the inaccuracy of the measurement. Therefore, RF triangulation is usually used as an approximation. In most cases, an approximation of 10 meters is accurate enough to locate a device physically.

Real World Scenario

Will Location Tracking Improve in the Future?

In the past, some vendors used proprietary software mechanisms on client stations to measure RSSI from access points continuously and to report this measurement back to a location tracking module of a WIDS/WIPS server. Because more statistical data is collected from the clients and not just APs or sensors, the accuracy of tracking authorized clients is enhanced. The ratified 802.11k-2008 amendment defines standards for *radio resource measurement (RRM)*. WLAN radio resource measurements enable STAs to understand the radio environment in which they exist by measuring RSSI, signal noise, and other statistics. Radio measurement data can be made available to upper protocol layers where it may be used by other applications, including location tracking services of a WIPS. The standardized RRM capabilities will most likely improve location tracking accuracy in the near future when the radio chipsets of client stations begin to support 802.11k mechanisms. One optional measurement defined by 802.11k is *location configuration information (LCI)* that can be used by an 802.11 client device that might also have GPS capabilities. LCI measurements can be used to report latitude, longitude, and altitude.

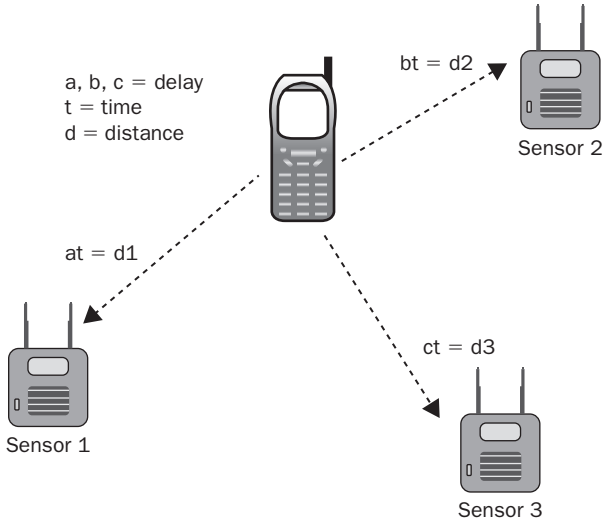
A more complex yet more accurate method of device location tracking is *RF fingerprinting*. RF fingerprinting also uses the RSSI values of transmitting devices as detected by sensors. However, RF fingerprinting does not rely on these values alone. RF fingerprinting also uses the RSSI values of devices whose locations are known as points of comparison. Rather than just listening to the target device's signal and estimating the target's location, this method compares the target's detected RSSI values with the RSSI values of the known reference points. The idea here is that if the target and the known reference point have similar RSSI values, they must be close to each other. RF fingerprinting relies on building up a database of actual measurements and relates them to

particular locations. This method can reduce the size of the search pattern from 10 meters down to about 1 or 2 meters and may be deployed using fewer sensors. However, RF fingerprinting can also be time-consuming and expensive.

The method used to document RSSI reference points on a map is known as *RF calibration*. The calibration is often done by an administrator using an 802.11 device (usually a laptop) moving throughout the area and taking many samples of RSSI data to be imported into the RF fingerprinting engine. If anything in the area changes the RF environment—such as new walls, neighboring devices, new interference sources, or the removal of these things—the RF fingerprinting will not function correctly until the engine can be recalibrated to include these changes in the RF environment. Recalibration is often overlooked by WLAN administrators who are busy with other tasks. The result of using a poorly calibrated RF Fingerprinting engine to track devices may be less accurate findings than just using RSSI values and RF triangulation. Although the RF fingerprinting method is more accurate than triangulation alone, it is more costly to implement and more labor intensive to maintain. The 8 or 9 meter accuracy improvement that RF fingerprinting provides is useful for locating rogue APs and for tracking Wi-Fi RFID tags. Several companies such as AeroScout and Ekahau provide WLAN *real-time location systems (RTLS)* that utilize RF fingerprinting methods. Several of the WLAN vendors and WIDS/WIPS vendors partner with RTLS vendors to take advantage of the increased accuracy provided by RF fingerprinting.

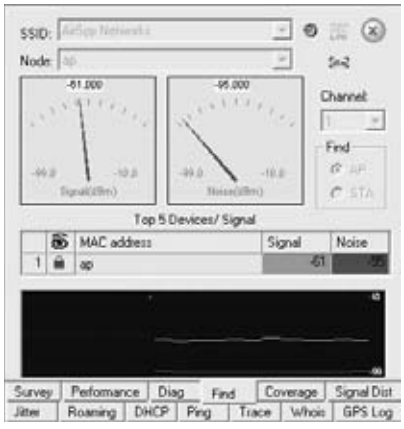
Time difference of arrival (TDoA) is another method that can be used for location tracking. As shown in Figure 10.22, TDoA uses the variation of arrival times of the same transmitted signal at three or more receivers, in our case, sensors. The transmitted signal will arrive at the sensors at different times due to distance between the transmitter and the multiple sensors. The speed of travel of the radio frequency is a known factor, and each of the synchronized TDoA sensors report the time of arrival of the signal from the transmitting device. In theory, if the transmitter were exactly at the midpoint between sensors, there would be no difference of arrival times, thus making the target easily located in the center of sensor coverage, equally distanced from all sensors. Ordinarily, the sensor that receives the signal first is deemed closer to the source of the transmission and the one receiving the signal last should be the farthest away from the source. The TDoA is also used in determining the *angle of arrival (AoA)* of a signal in an antenna array. TDoA does not require the calibration of RF fingerprinting, nor does it use the RSSI values as triangulation methods use them. TDoA simply uses the time stamps of the signal's arrival at various known locations. Some WLAN vendors are using TDoA technology to assist in tracking Wi-Fi RFID tags. Wi-Fi TDoA sensors are typically used for location tracking in line-of-sight environments, such as outdoor deployments or warehouses with high ceilings.

FIGURE 10.22 Time difference of arrival (TDoA)



It is possible to conduct device tracking with a single mobile receiver taking multiple readings in several locations by hand using a laptop or handheld device. However, the speed at which distributed systems are able to accomplish this same task makes location tracking an important and reliable part of WLAN security monitoring. Using a single mobile device to supplement location tracking is a good practice for "last mile" discovery. As shown in Figure 10.23, mobile devices usually use a graph, needle, and/or sound to indicate proximity to the target device. Using the WIDS/WIPS to approximate the location and then following through by using the portable device is a common method of locating rogues and other devices in a WLAN enterprise. No matter which method you choose, you will most likely encounter a situation that requires finding the physical location of a device.

FIGURE 10.23 Mobile tracking tool



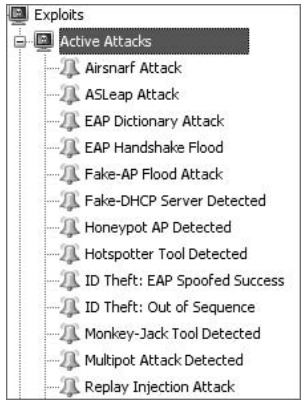
WIDS/WIPS Analysis

As you have learned, WLAN security monitoring using a distributed WIDS/WIPS solution is capable of collecting information continuously. Because the information gathered from multiple sensors can be extensive, the task of analyzing all the collected data can be overwhelming. Every WIDS/WIPS solution uses a variety of software modules or software engines to simplify the task of analyzing massive amounts of collected data.

Signature Analysis

WIDS/WIPS solutions use *signature analysis* to analyze frame patterns or "signatures" of known wireless intrusions and WLAN attacks. The WIDS/WIPS has a programmed database of hundreds of threat signatures of known WLAN attacks. As shown in Figure 10.24, threat signatures can include man-in-the-middle attacks, DoS attacks, flood attacks, and many more. WIDS/WIPS signatures are based on Layer 1 and Layer 2 attacks. The WIDS/WIPS utilizes some sort of signature analysis engine that processes 802.11 frames and RF data. Automatic signature learning systems require extensive logging of complex network activity and historic data mining that can impact performance. Most WIDS/WIPS solutions use manual signature detection, which is comparable to most virus protection systems where the signature database is updated automatically as new signatures are discovered. WIDS/WIPS vendors are constantly updating their signature databases as new attacks emerge. Usually, the systems also have the capability of creating custom signatures. Custom signatures are useful to WLAN administrators who want to monitor for a behavior or attack that could be specific to their WLAN environment.

FIGURE 10.24 Attack signatures



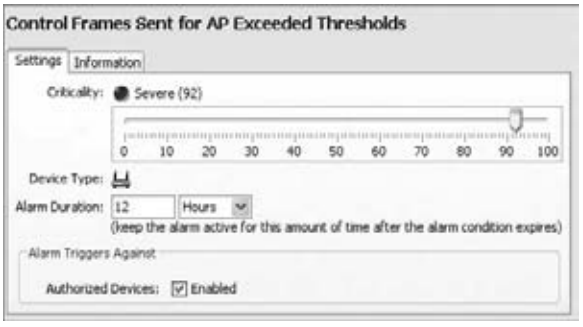
Behavioral Analysis

Many WIDS/WIPS solutions also utilize *behavioral analysis* to recognize any patterns that deviate from normal WLAN activity. Behavioral analysis identifies abnormal network behavior based on historical metrics. Because historical normal WLAN behavior is the baseline, anomalies can be detected that would not necessarily be discovered by other intrusion detection techniques. Whereas the signature analysis identifies known threats, the anomalous behavior analysis recognizes new, unknown attacks or threats that have no signature.

Detection of anomalies can be based on various thresholds of 802.11 management, control and data frames, fragmentation thresholds, and many other variables. Behavior analysis helps detect *protocol fuzzing*, where an attacker sends malformed input to look for bugs and programming flaws in WLAN controller code or client station firmware. Attackers transmit malformed data by tampering with bits and fields of data in 802.11 frames. Protocol fuzzing attacks often identify driver vulnerabilities and find weaknesses that result in a buffer overflow attack.

As you have learned, known attacks can be easily identified by signature analysis. However, the greatest threat to WLAN security is a new attack that is not known and cannot be detected. An unknown threat used to exploit computer networks is known as a *zero day attack*. Very often, a zero day attack will create some sort of anomaly in 802.11 behavior that can be detected. As shown in Figure 10.25, behavior thresholds can be configured on the WIDS/WIPS that can trigger an alarm. Setting thresholds can often be difficult and time-consuming to achieve a balance in detecting possible zero day attacks versus triggering false positive alarms.

FIGURE 10.25 Behavior thresholds



Protocol Analysis

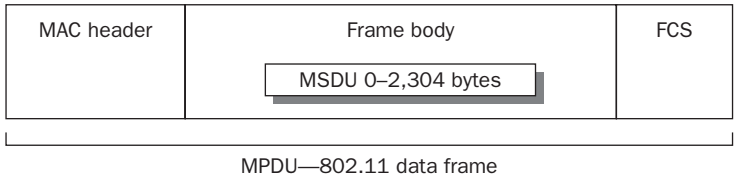
All WIDS/WIPS vendors use *protocol analysis* to dissect the MAC layer information from 802.11 frames. Protocol analysis may also be used to analyze Layer 3–7 information of 802.11 data frames that are not encrypted. In Chapter 9, "Wireless LAN Security

Auditing," you learned that standalone WLAN protocol analyzers are usually installed on a laptop and are used for security audits. Standalone WLAN protocol analyzers are also used for Layer 2 troubleshooting and WLAN performance analysis. The WildPackets OmniPeek software you have been using in the book's exercises is a standalone WLAN protocol analyzer. All standalone WLAN protocol analyzers have some security analysis capabilities, but some place a greater emphasis on security auditing and can effectively be used as a *mobile wireless intrusion detection system* solution. Two examples are Fluke Networks' AirMagnet Wi-Fi Analyzer and Motorola's AirDefense Mobile. Although rarely used, mobile WIDS analyzers can also be integrated with a distributed WIDS/WIPS, effectively acting as software-based sensors.

An enterprise WIDS/WIPS solution provides for distributed protocol analysis, with each hardware sensor acting as a listening device. Distributed protocol analysis is mainly used to monitor all the 802.11 frame exchanges that occur at Layer 2. That information can be leveraged for both security reasons and for WLAN performance analysis. Attacks can be detected at Layer 2 by reading the headers and trailers of all of the frames captured with a distributed protocol analyzer.

An in-depth discussion of 802.11 protocol analysis is beyond the scope of this book; however, a quick discussion of the 802.11 frame format is necessary. The technical name for an 802.11 data frame is a *MAC Protocol Data Unit (MPDU)*. The 802.11 frame, as shown in Figure 10.26, contains a Layer 2 MAC header, a frame body, and a trailer, which is a 32-bit CRC known as the *frame check sequence (FCS)*. The Layer 2 header contains MAC addresses and the duration value. The frame body contains the *MAC Service Data Unit (MSDU)*, which is the Layer 3–7 payload.

FIGURE 10.26 MAC Protocol Data Unit



The IEEE 802.11-2007 standard defines three major frame types:

Management 802.11 management frames are used by wireless stations to join and leave the basic service set (BSS). Another name for an 802.11 management frame is a *Management MAC Protocol Data Unit (MMPDU)*. Management frames do not carry any upper-layer information. There is no MSDU encapsulated in the MMPDU frame body, which carries only Layer 2 information fields and information elements. Information fields are fixed-length mandatory fields in the body of a management frame. Information elements are variable in length and are optional. Examples of management frames are beacons, probe requests, and association request frames.

Control 802.11 control frames assist with the delivery of the data frames. Control frames must be able to be heard by all stations; therefore, they must be transmitted at one of the basic rates. Control frames are also used to clear the channel, acquire the channel, and provide unicast frame acknowledgments. They contain only header information. Control frames do not have a frame body. Examples of control frames are acknowledgments, request-to-send, and clear-to-send frames.

Data Most 802.11 data frames carry the actual data that is passed down from the higher-layer protocols. The Layer 3–7 MSDU payload is normally encrypted for data privacy reasons.

Most WIDSs/WIPSs have the capability to monitor 802.11 frame exchanges in real time just like a standalone WLAN protocol analyzer. Enterprise WIDSs/WIPSs also usually have the ability to use sensors for *remote packet capture*. As shown in Figure 10.27, an individual sensor is configured to capture on a single channel and then mirror the captured 802.11 traffic to a remote IP address. The remote IP address is typically a desktop computer with standalone WLAN protocol analyzer software used to view the remote packet capture.

FIGURE 10.27 Remote packet capture

Spectrum Analysis

Always remember that 802.11 devices operate at both Layers 1 and 2. The Layer 1 physical medium is the uncontrolled, unlicensed, and unbounded RF spectrum. Traditionally, WIDS/WIPS solutions have mostly been used strictly to monitor Layer 2 communications and have mostly ignored Layer 1 for security monitoring. As you learned in Chapter 8, DoS attacks can occur at Layer 1. Any continuous transmitter will cause a DoS. RF jamming devices can be used by an attacker to cause an intentional Layer 1 DoS attack. Denial of service at Layer 1 usually occurs as an unintentional result of transmissions from non-802.11 devices. Video cameras, baby monitors, cordless phones, and microwave ovens are all potential sources of interference. Unintentional interference may cause a continuous DoS, but the disruption of service is often sporadic. This disruption of service will upset the performance of Wi-Fi networks used for data applications but can completely disrupt VoWiFi communications within a WLAN. At the very least, unintentional interference will result in retransmissions that negatively affect WLAN performance. The majority of unintentional interfering devices transmit in the 2.4

GHz ISM frequency band. The 5 GHz UNII bands are less susceptible to unintentional interference. RF interference often is undetected by traditional WIDS/WIPS sensors and cannot be properly classified.

Included on the CD that accompanies this book is a white paper titled "Protecting Wi-Fi Networks from Hidden Layer 1 Security Threats," authored by Neil Diener of Cisco Systems and David Coleman of AirSpy Networks. This white paper is highly recommended extra reading and should be considered as suggested study material for the CWSP exam.

Although wireless intrusion prevention systems are outstanding products that can mitigate most rogue attacks, some rogue devices will go undetected. The radio cards inside the WIPS sensors typically monitor the 2.4 GHz ISM band and the 5 GHz UNII frequencies. Older legacy wireless networking equipment exists that transmits in the 900 MHz ISM band, and these devices will not be detected. The radio cards inside the WIPS sensors is use only *direct sequencing spread spectrum (DSSS)* and *orthogonal frequency division multiplexing (OFDM)* technologies. Wireless networking equipment exists that uses *frequency hopping spread spectrum (FHSS)* transmissions in the 2.4 GHz ISM band and will go undetected by traditional WIDS/WIPS sensors. The only tool that will detect with 100 percent certainty either a 900 MHz or a frequency hopping rogue access point is a spectrum analyzer capable of operating in those frequencies.

A spectrum analyzer is a frequency domain measurement and troubleshooting tool. A spectrum analyzer can help identify and locate an interfering transmitter. Spectrum analyzer hardware can cost upward of $40,000 U.S. dollars, thereby making them cost-prohibitive for many smaller and medium-sized businesses. The good news is that several companies have standalone solutions, both hardware and software based, that are designed specifically for 802.11 spectrum analysis and are drastically less expensive. As shown in Figure 10.28, WLAN spectrum analysis is most often achieved with a standalone

FIGURE 10.28 WLAN spectrum analyzer

software-based solution installed on a laptop that works with special PCMCIA cards or USB adapters.

One of the most important capabilities of a spectrum analyzer is the ability not only to detect RF energy but also to classify the sources of the interference. The better spectrum analyzers use *RF signature analysis* to identify and classify interfering RF transmitters, such as Bluetooth, microwave ovens, wireless cameras, jammers, and so on.

In the past, a major oversight in many WIDS/WIPS solutions was that they were unable to detect previously discussed Layer 1 security threats. However, in recent years, enterprise WIPSs have begun to operate as *distributed spectrum analysis systems (DSAS)*. The advantage of any distributed solution is that they run 24/7 and can be administered remotely. Ideally, the best DSAS solution would use sensors with a special spectrum analyzer cardbus that solely monitors Layer 1. The downside is that a spectrum analyzer cardbus effectively doubles the costs of WIPS sensors that already are using 802.11 radios. Several enterprise WIPS vendors have begun to use the 802.11 radio chipsets to perform a lower-grade of distributed spectrum analysis. The spectrum analysis capabilities of an 802.11 radio may not be as robust, but the costs are drastically less. A good DSAS is capable of RF signature analysis and can also physically pinpoint sources of RF interference using the location tracking capabilities discussed earlier in this chapter.

EXERCISE 10.1

Spectrum Analysis

In this exercise, you will use a demo program of Fluke Networks' AirMagnet Spectrum XT to view sources of interference and simulate spectrum analysis.

1. Browse to `www.airmagnet.com/cwsp/sybex` and request your copy of Spectrum XT. You will receive an email with instructions on how to download the software and the spectrum capture file.
2. Install the Spectrum XT software.
3. Access and run the XT software from the Programs menu.
4. By default, XT will load its default capture file.
5. Notice that the 2.4 GHz frequency space is very crowded with interfering devices.
6. Continue to maneuver through the program and familiarize yourself with the spectrum analyzer's features and capabilities.

Forensic Analysis

Enterprise WIDS/WIPS solutions may also provide *forensic analysis* that allows an administrator to retrace the actions of any single WLAN device down to the minute.

With forensic analysis, investigating an event takes minutes instead of potentially hours. Administrators can rewind and review minute-by-minute records of connectivity and communication within a WLAN. As shown in Figure 10.29, the WIPS records and stores hundreds of data points per WLAN device, per connection, per minute. This allows an organization to view months of historical data on any suspicious WLAN device as well as all authorized devices. Information such as channel activity, signal characteristics, device activity, and traffic flow and attacks can all be viewed historically.

FIGURE 10.29 Forensic analysis

Performance Analysis

A very useful by-product of WIDS/WIPS deployment is that you are able to collect a large amount of data for analysis for performance monitoring. Although the main purpose of an enterprise WIDS/WIPS is security monitoring, information collected by the WIPS can also be used for *performance analysis*. Since everything WLAN devices transmit is visible to the sensors, the Layer 2 information gathered can be used to determine the performance level of a WLAN. The WIPS can detect hidden nodes, excessive Layer 2 retransmissions, excessive wired to wireless traffic, excessive roaming, and many other events and traffic types that lower the capacity performance of a WLAN.

Knowing how the WLAN functions on a regular basis can help reduce problem-solving time greatly. Performance analysis can be used to define performance baselines used to establish expected performance standards or levels. Baselining involves determining how the WLAN is functioning in terms of performance. An administrator must take several samples of traffic at various times. These samples should be taken at both peak and off-peak times and over a long enough period to capture adequately an idea of what is normal

for the WLAN. The baseline should include normal use conditions as well as peak and off off-peak captures. Using captures from longer periods will allow you to better understand normal use of the network and have a more accurate baseline. Since the WIDS/WIPS is collecting information all day, every day, the sampling for a baseline is more accurate and more inclusive. Once a baseline has been established for the WIDS/WIPS, performance thresholds can be configured to send alerts when performance drops to detrimental levels. Performance monitoring allows an administrator to act on potential network issues before the users notice any performance problems. Performance monitoring also aids in the planning for any necessary expansion of the WLAN. If an administrator knows how well the WLAN functions with the current number of APs and stations running the current applications, the impact of adding more users and devices can be more accurately predicted.

Monitoring

With the vast amount of data that can be collected, it is of great importance to have the WIDS/WIPS properly tuned for your environment. Alarm policies can be configured to define thresholds for security and performance. Custom alarm threat thresholds can be configured to match the WLAN's security and performance requirements. Alarm notifications can also be triggered to alert you about attacks. You can then evaluate the alarms and take the proper actions.

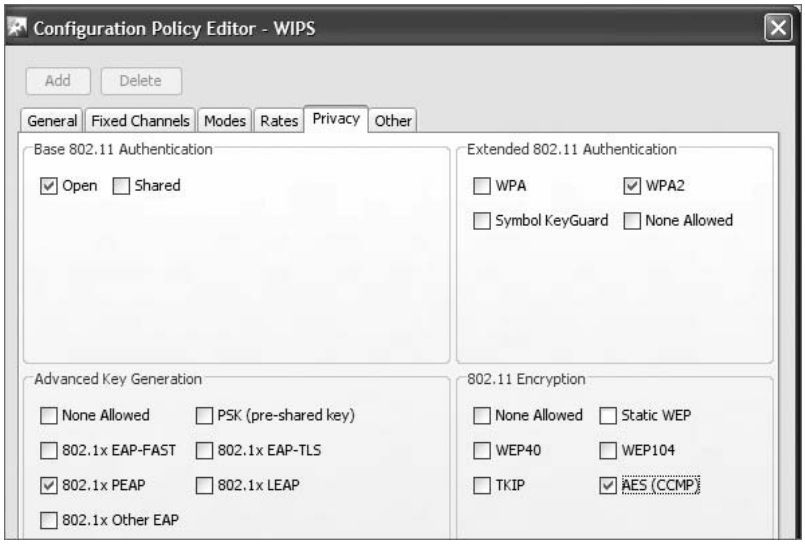
Policy Enforcement

Enterprise WIDS/WIPS solutions allow administrators to define, monitor, and enforce wireless LAN policies in the areas of security, performance, usage, and vendor types. Organizations can minimize vulnerability by ensuring that WLAN devices are using the proper security protocols. Improper configuration of WLAN devices is one of the most common causes for wireless security breaches.

Security policies must be defined to set thresholds for acceptable network operations and performance. As shown in Figure 10.30, you can define a security policy that requires all client stations use an 802.1X/PEAP solution for authentication and CCMP/AES for encryption. If an end-user configures a client station that is not using PEAP and CCMP, the WIPS will generate a policy-based alarm. Defining security policies ensures that all devices are properly configured with the mandated level of protection.

Security policies need to be set for both access point and client station configuration thresholds. Policies should be defined for authorized APs and their respective configuration parameters, such as Vendor ID, authentication modes, and allowed encryption modes. Define allowable channels of operation and normal activity hours of operation for each AP. Performance thresholds can also be defined for minimum signal

FIGURE 10.30 Security policy



strength from a client station associating with an AP to identify potential attacks from outside the building.

The defined security policies form the baseline for how the WLAN should operate. The thresholds and configuration parameters should be adjusted over time to tighten or loosen the security baseline to meet real-world requirements. For example, normal activity hours for a particular AP could be scaled back due to working hour changes. The security policy should also be changed to reflect the new hours of operation. No one security policy fits all environments or situations. There are always trade-offs between security and usability.

The WIPS can also be used for policy enforcement. Once again, you can define a security policy that requires all client stations use an 802.1X/PEAP solution for authentication and CCMP/AES for encryption. If an end-user configures a client station that is not using PEAP and CCMP, the WIPS will generate a policy-based alarm. However, the security policy can also be set to trigger an automatic response in addition to the alarm. The WIPS can use spoofed deauthentication frames against the misconfigured client, similar to rogue containment measures. In this way, authorized devices are not able to place their traffic at risk by communicating without the use of required authentication or encryption methods. A policy is only as good as its ability to be enforced uniformly. An alarm will alert you to an unsecure environment or device, but does not take steps to enforce the policy. A WIPS offers the additional protection of

preventing devices from communicating outside of policy by terminating noncompliant devices connections. This approach does have the potential to disrupt business and should be properly weighed against potential security problems when making the decision to terminate noncompliant connections. Many users of WIPSs in larger enterprise deployments with 24/7 staffing prefer to receive notifications of noncompliant device communications and manually remediate the problem to avoid business interruption.

Prior to implementing actions to enforce policy, it is of great importance that any written organizational security policy be consulted, followed, and or updated and required. Policy violation reporting and policy enforcement may be dictated by outside organizations based on industry and governmental regulations. You can find a more detailed discussion about policies and regulations in Chapter 13, "Wireless Security Policies."

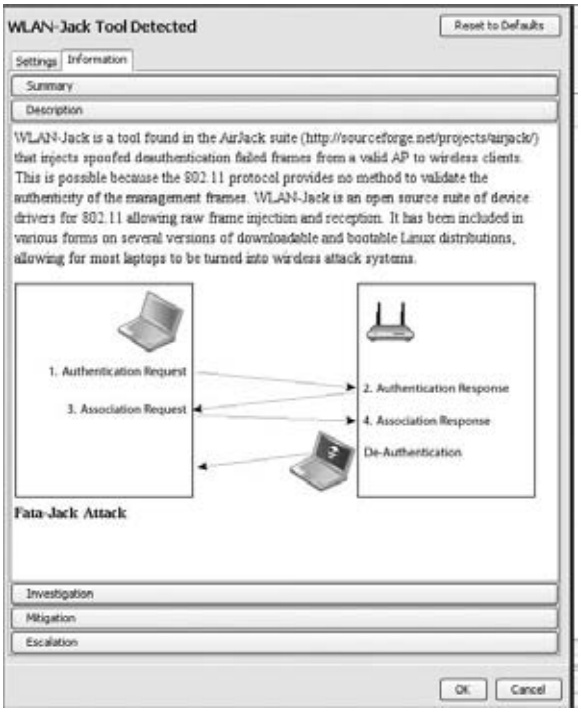
Alarms and Notification

In a congested WLAN environment or in an area with very little traffic, any 802.11-based device that transmits a signal can be heard by the WIDS/WIPS sensors. The WIDS/WIPS will detect all 802.11 transmissions and then, if necessary, generate the appropriate alarms. Depending on the configured threshold, the alarms can be triggered by signature analysis, spectrum analysis, behavioral analysis, or performance analysis. Alarms can also be policy based, as we discussed in the previous section. Practical questions then arise once the alarms have been triggered:

- What do I do with all of this information?
- What do these alarms mean?
- Do I need to be informed about every device detected?
- Who is going to respond to the alarms?
- Am I under attack?
- Is this normal or acceptable behavior?
- Are any or all of these detected devices mine?
- Are my devices safe?

As shown in Figure 10.31, the triggered alarms will often have a detailed description of the attack or performance problem. The WIPS alarm may also have suggested mitigation actions. The detailed description and recommended actions will often help you answer the questions we just listed.

FIGURE 10.31 WIDS/WIPS alarm



As we discussed earlier, WIDS and WIPS solutions are able to discover and classify devices as well as conduct behavioral analysis. Event alerts or alarms are used to indicate that a device or particular behavior has been detected by the system. Different behaviors will trigger different alarms. If a user turns on a new client device within hearing range of a sensor, an unauthorized device alarm will be triggered. If that user then connects to an authorized AP without their new client device first being authorized, a rogue station alarm will be triggered. What happens beyond that depends on the vendor of the WIDS/WIPS and the customization done to the system. A WIPS can proactively begin to protect the network using rogue station containment.

Users, contractors, and visitors often have the credentials to connect and do so using their own devices. This will trigger alarms within the WIDS/WIPS based on the classification of their device as unauthorized and the behavior analysis of the device showing it as associated with an authorized AP. Any device detected and any behavior detected can be used to trigger alarms and possible automatic responses.

Alerts or alarms can be classified just as devices can be classified. Events that trigger alarms are not always indications of security threats or vulnerabilities. Some events are

normal behavior, such as protection mode in use by an 802.11g access point or including its SSID in the beacon frames it transmits. The alarms can be broken into several categories:

- Behavioral
- Exploits
- Performance
- Policy Compliance
- Reconnaissance
- Rogue Activity
- Performance
- Vulnerabilities

WIDS/WIPS alarms are usually set to a threat-criticality level the vendor has determined to be what most users want. However, you may wish to make some alarms more or less important than the preset threat levels. Within the categories, alarms or alerts can be given custom threat levels from "everything is fine" to "we are under attack." These levels include the following:

Safe No immediate threat

Minor Potential problem alarms that may worsen if ignored

Major Potentially serious alarms that require priority attention

Critical Serious alarms that require immediate attention

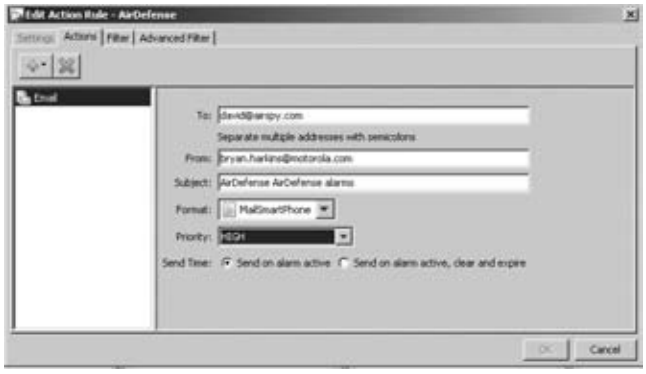
Severe Serious alarms that may have catastrophic effects

Tuning the alerts or alarms to threat levels is an important and possibly time-consuming task when deploying a WIDS/WIPS. However, spending the time up front to calibrate alarm thresholds properly will make the alerts more meaningful. The intended use of a WIDS/WIPS along with vendor-specific options will dictate how you should tune the alarm thresholds. Alarms can be disabled or have their threat levels lowered if they are not of importance.

Keeping a record of everything that is detected is a sound practice for forensic or even legal reasons. However, you may not want to receive a notification about everything the system detects. As shown in Figure 10.32, an alarm can be configured also to trigger notifications. These notifications can be sent from the system in several forms:

- Email
- SMS
- Syslog
- Smart Phone

FIGURE 10.32 Alarm notifications



The notifications should be configured to trigger only if an alarm is of specific importance to you. You will want to be alerted to the fact that a rogue is on the network or an attack is occurring. However, you would not want to know every time a WLAN device is detected unless a no-wireless zone is being enforced. Typically, alarms with a threat level of critical or severe are also configured for notification. It should be noted that any AP or client that is initially classified as unauthorized should still be investigated as soon as time permits.

False Positives

The physical radio frequency medium used for 802.11 communications is both harsh and unpredictable. RF behaviors, such as reflections and multipath, often create a hostile environment that results in corrupted 802.11 frames and Layer 2 retransmissions. WLAN problems, such as adjacent cell interference, low SNR, and hidden nodes, can also lead to corrupted data frames. Because the RF environment is at worst unstable and at best fluctuating, not every WIDS/WIPS alarm is going to be perfectly accurate. In other words, a certain amount of false positive alarms are to be expected. A *false positive*, also known as a false detection or false alarm, is a result that is erroneously positive when the situation is actually normal. A false positive is simply another way of saying "mistake." All intrusion detection systems, both wired and wireless, will have some occurrence of false positives. A false positive WIDS/WIPS alarm indicates that a WLAN attack is occurring when in fact the threat does not exist. False positive alarms can be time consuming for you to verify or invalidate. Even worse, false positives are often ignored due to their volume, thus increasing the possibility that a real attack alarm will also be ignored.

Corrupted frames are the leading cause of false positives. However, improper configuration of the WIPS or misinterpretation of alarms by administrators can also lead to false positive alarms. Proper classification of all devices as either authorized devices or neighbor devices is important. If devices are not properly classified, many alarms will be triggered. As mentioned earlier in this chapter, setting alarm thresholds can often be

difficult and time consuming to achieve a balance in detecting possible attacks versus triggering false positive alarms. Some inaccurate reporting of events, seen as false positives, are unavoidable. However, properly setting alarm thresholds that are fine-tuned to the on-site RF environment can greatly reduce the number of false positives. A reduction in false positives will save time and improve the security of the WLAN.

Reports

Enterprise WIDS/WIPS solutions usually offer extensive report generation capabilities. Reports can be created manually or can be scheduled to be created automatically. Viewing and saving these reports is part of maintaining a secure and healthy wireless environment. When properly created, reports are useful tools in problem analysis and resolution. Security issues that may require disciplinary and or legal action are better supported with documentation. The reports can also be used to validate expenditure issues with upper management with regard to network security and development requirements.

The report software engine of the WIDS/WIPS will have many predefined reports that cover compliance, security, and performance. Additionally, the WIPS administrator will usually have the option to create custom reports that address the individual needs of a specific WLAN that is being monitored.

Examples of two WIPS-generated reports are included on the CD that comes with this book. The reports are titled `Security_Rogue_Detail_report.pdf` and `Vulnerability_Assessment_Report.pdf`.

802.11n

Consumers and businesses have long anticipated the ratification of the 802.11n-2009 amendment, which defines the use of *High Throughput (HT)* radios that have the potential to support data rates as high as 600 Mbps. 802.11n technology uses both PHY and MAC layer enhancements to achieve these high data rates. However, new issues arise in regard to security when 802.11n technology is deployed.

All 802.11n radio transmissions use a physical layer header with training symbols that provide the initial synchronization with receiving 802.11 radios. 802.11n supports three frame formats:

Legacy This format uses the legacy PHY header that is used by 802.11a and 802.11g radios.

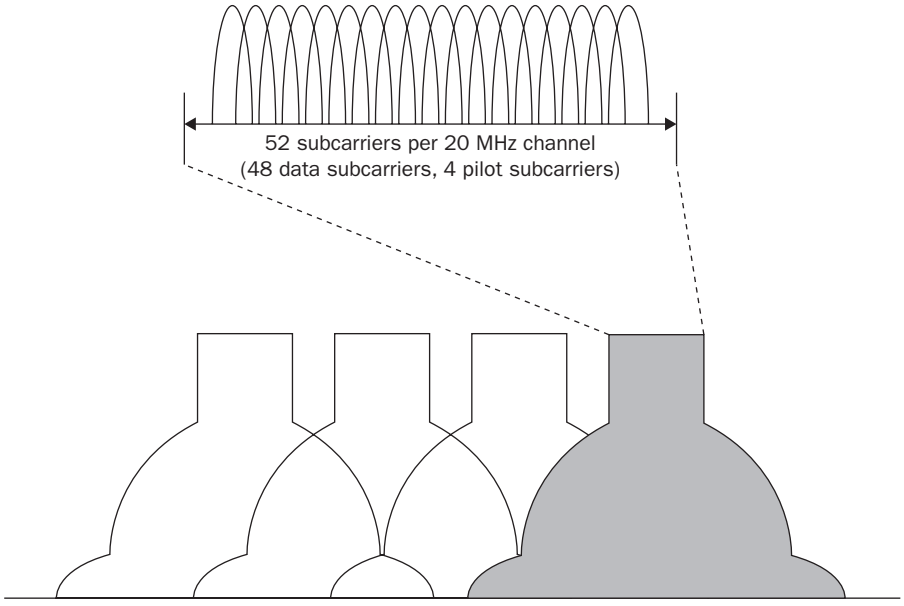
Mixed Format This format uses a PHY header that can be interpreted by both legacy 802.11a/g radios and 802.11n High Throughput (HT) radios.

HT Greenfield The Greenfield PHY header is not backward compatible with legacy 802.11a/g radios and can only be interpreted by 802.11n HT radios.

Most of the current WIPS sensors only have 802.11a/g radios. An 802.11a/g sensor will be able to detect an 802.11n transmitter using a 20 MHz channel and using either the mixed or non-HT frame formats. However, a legacy 802.11a/g sensor will not be able to decipher any transmissions using the HT Greenfield frame format. An attacker could potentially install a rogue 802.11n AP that is only transmitting using the HT Greenfield frame format. The HT Greenfield PHY header cannot be detected by a WIPS that is using legacy 802.11a/g sensors. The solution to this problem is to upgrade the WIPS with new sensors that also have 802.11n HT radios. The downside is that the initial upgrade to 802.11n sensors will be costly.

Non-HT radios (802.11a and 802.11g radios) use 20 MHz OFDM channels. As shown in Figure 10.33, each channel consists of 52 subcarriers. Forty-eight of the subcarriers transmit data, while four of the subcarriers are used as pilot tones for dynamic calibration between the transmitter and receiver.

FIGURE 10.33 20 MHz non-HT (802.11a/g) channel



A unique optional capability of HT radios (802.11n) is to transmit on 40 MHz OFDM channels. As shown in Figure 10.34, the 40 MHz HT channels use 114 OFDM subcarriers. One hundred and eight of the subcarriers transmit data, while six of the subcarriers are used as pilot tones for dynamic calibration between the transmitter and receiver. As shown in Figure 10.35, the 40 MHz channels used by HT radios are essentially two 20 MHz OFDM channels that are bonded together. Each 40 MHz channel consists of a primary and secondary 20 MHz channel. The primary and secondary 20 MHz channels must be adjacent 20 MHz channels in the frequency in which they operate.

FIGURE 10.34 40 MHz HT (802.11n) channel

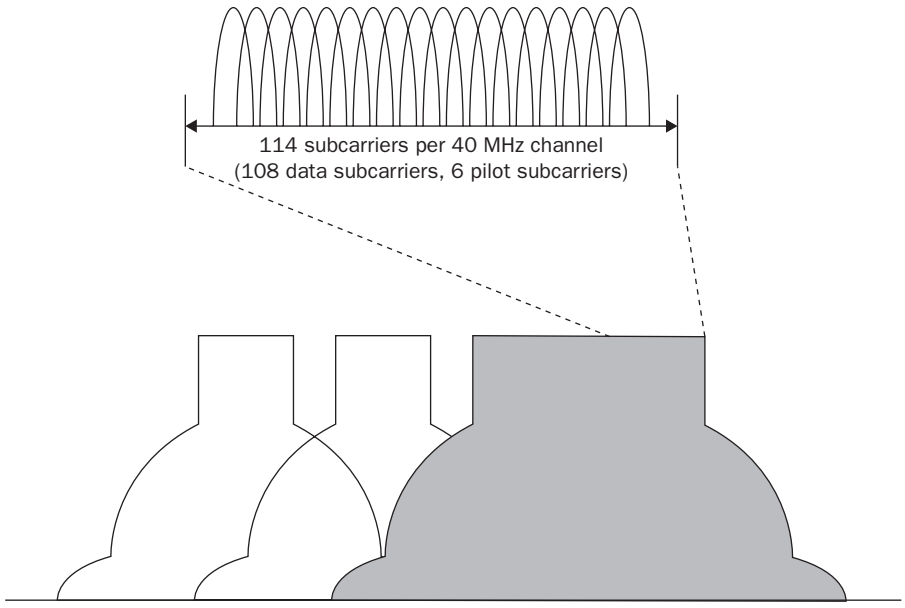
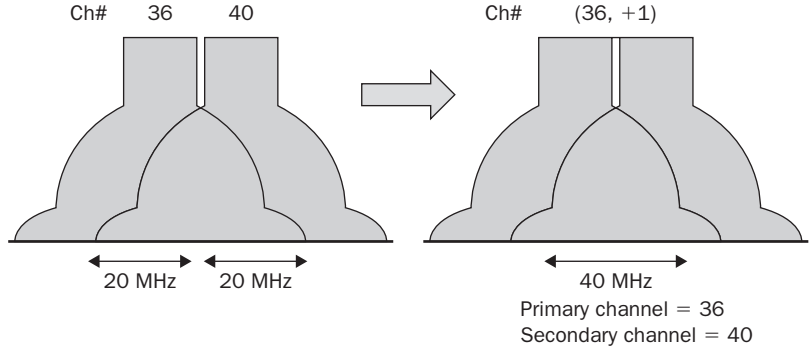


FIGURE 10.35 Channel bonding



All 802.11n access points are configured to operate as a 20/40 basic service set. A 20/40 BSS allows legacy 20 MHz 802.11a/b/g client stations and 20/40 MHz–capable 802.11n stations to operate within the same cell at the same time. 802.11n radios that are 20/40 capable can use 40 MHz transmissions when communicating with one another; however, they would need to use 20 MHz transmissions when communicating with the legacy

802.11 a/b/g stations. To maintain backward compatibility, the 40 MHz capable 802.11n stations will communicate on the primary 20 MHz channel when communicating to legacy 802.11 a/b/g stations.

An 802.11a/g sensor will be able to detect an 802.11n transmitter using a legacy 20 MHz channel. Older sensors will also be able to detect a 40 MHz 802.11n transmitter as long as it is communicating on the 20 MHz primary bonded channel. However, a legacy 802.11a/g sensor will not be able to decipher any full 40 MHz channel transmissions. A WIPS sensor capable of spectrum analysis could detect the 40 MHz channel but could not decipher the 40 MHz transmissions unless the sensor had an HT 802.11n radio.

An 802.11n deployment effectively doubles the amount of channels that must be monitored for IDS purposes. The WIPS solution must listen for attacks on both the 20 MHz and 40 MHz OFDM channels. Some WLAN vendors use an integrated WIPS solution where access points perform off-channel scanning and are used as part-time WIPS sensors. Access points spending too much time listening off-channel will cause latency/jitter issues with VoWiFi solutions. Because more channels must be monitoring, the potential of unheard attacks increases. Too little time spent listening off-channel can also expose the WLAN to potential unheard attacks. As you have already learned, if an integrated WIPS solution is being used, it is a highly recommend practice to convert a number of controller-based APs into full-time WIPS sensors that are constantly scanning all channels. The need for full-time scanning sensors is even more important because both 20 MHz and 40 MHz channels must be monitored frequently.

As new technologies are deployed, new attacks always follow. Currently, there is already a denial-of-service (DoS) attack that exploits 802.11n Block ACK frames. There will probably be more new Layer 2 DoS attacks against 802.11n deployments in the future. The answer to this problem is to make sure that the deployed WIPS can detect these new attacks and to update the WIPS signature files on a regular basis.

A white paper from Fluke Networks titled "Guide to Deploying 802.11n Wireless LANs" authored by David Coleman of AirSpy Networks is included on the CD that comes with this book. The white paper offers a general overview about the basics of 802.11n technology.

Proprietary WIPS

As you have already learned, most WIDS vendors prefer to call their products a wireless intrusion prevention system (WIPS). The reason that they refer to their products as prevention systems is that they are all capable of mitigating attacks from rogue access points and rogue clients. Currently, the main attack mitigated by a WIPS is rogue devices. In the future, other wireless attacks might be mitigated as well. In the meantime, several WIPS vendors are using proprietary methods to mitigate some WLAN attacks.

Cloaking

One example of proprietary mitigation is the WEP Cloaking solution used by Motorola's AirDefense WIPS. As you learned in previous chapters, WEP encryption can be easily cracked with freely available cracking software tools. Tools such as Aircrack-ng use reinjection methods to speed up an attack when capturing WEP encrypted frames.

Ideally, an enterprise deployment should have long ago upgraded to WPA2 security using CCMP/AES dynamic encryption. However, due to cost restraints, many organizations still use static WEP encryption on a lot of legacy devices, such as wireless barcode scanners. WEP Cloaking is a solution designed to protect legacy devices using WEP encryption from the twenty-three known WEP attack tools. If WEP Cloaking is enabled, the WIPS sensors transmit altered WEP frames, which are designed to confuse WEP attack tools. The sensors inject the altered WEP frames into the environment. Once configured for cloaking, sensors intelligently analyze local traffic and inject carefully timed cloaking frames. These cloaking frames appear to be legitimate WEP traffic to an attacker. Authorized users using the proper WEP key will ignore the cloaking frames because the ICV integrity test will fail. However, an attacker sniffing traffic cannot distinguish cloaking frames from the legitimate frames. When statistical WEP cracking tools are run on the captured data, key cracking should fail.

Once again note that the cloaking solution is propriety and that upgrading to dynamic CCMP/AES encryption is highly recommended when funds are available. A proprietary solution such as WEP Cloaking will also not meet certain industry and compliance standards that may require the use of strong Advanced Encryption Standard (AES) cryptography.

Management Frame Protection

For several years Cisco Systems has used proprietary *management frame protection (MFP)* to defend against several Layer 2 denial-of-service attacks. As you learned in Chapter 8, the two most common Layer 2 DoS attacks occur when deauthentication or disassociation management frames are spoofed. When Cisco's management frame protection is enabled, an AP adds a message integrity check (MIC) to each management frame it transmits. Any attempt to copy, alter, or replay the frame invalidates the MIC. Certain 802.11 management frames are protected with either CCMP/AES or TKIP/RC4 in a similar method, which is already used for 802.11 data frames. Parts of the management frame header are copied into the encrypted payload component of each frame for extra protection. The three management frames protected by Cisco MFP are:

- Disassociation
- Deauthentication
- QoS (WMM) action frames

Because Cisco's implementation is indeed proprietary, in order to be protected, client stations will need to support Cisco Compatible Extensions (CCX) version 5 or higher. Cisco's MFP implementation is effectively a pre-standard implementation of the IEEE 802.11w-2009 amendment.

You can find more information about the Cisco Compatible Extensions Program at `www.cisco.com/web/partners/pr46/pr147/partners_pgm_concept_home.html`.

802.11w

The IEEE 802.11-2007 standard addresses security of data frames, but WLANs are still vulnerable to attacks because management frames are unprotected. At the time of this writing, the IEEE ratified the 802.11w-2009 amendment, which defines standardized management frame protection.

Disassociation frames can be sent by either an AP or a client station. Disassociation is a notification, not a request. In the past, disassociation could not be refused by the receiving station. 802.11w allows the receiving STA to refuse disassociation when management frame protection (MFP) is negotiated and the message integrity check fails. Deauthentication frames can be sent by either an AP or a client station. Deauthentication is a notification, not a request. In the past, deauthentication could not be refused by the receiving station. 802.11w allows the receiving STA to refuse deauthentication when management frame protection is negotiated and the message integrity check fails.

The 802.11w draft amendment defines a *robust management frame* as a management frame that can be protected by the management frame protection service. The robust management frames include robust action frames, disassociation frames, and deauthentication frames. The majority of action frames are considered robust, including QoS action frames, radio measurement action frames, Block ACKs, and many more.

As you learned in Chapter 5, TKIP/RC4 and CCMP/AES provide protection against replay attacks against 802.11 data frames. However, only CCMP/AES is supported for protection of robust management frames. Replay protection is provided for robust management frames for STAs that use CCMP and *Broadcast/Multicast Integrity Protocol (BIP)*. BIP provides message integrity and access control for group-addressed robust management frames. Now that it has been ratified, the 802.11w-2009 amendment should help put an end to deauthentication attacks and disassociation attacks as well as Layer 2 DoS attacks that involve action frames. Although 802.11w does address these two popular DoS attacks, 802.11w will not address many other Layer 2 DoS attacks.

Numerous Layer 2 DoS attacks exist, including association floods, EAPOL floods, PS-Poll floods, and virtual carrier attacks. 802.11w does not address these types of Layer 2 DoS attacks. Luckily, any good wireless intrusion detection system will be able to alert an administrator immediately to a Layer 2 DoS attack. Please understand that 802.11w compliance will eventually prevent some of the popular Layer 2 DoS attacks that currently exist, but it is doubtful that all Layer 2 DoS attacks will ever be circumvented.

Real World Scenario

How Will 802.11w Affect Rogue Mitigation?

As you have previously learned, most WIPS solutions use a wireless rogue containment that uses spoofed deauthentication frames. Rogue containment is accomplished wirelessly when the WIPS' sensors become active and begin transmitting deauthentication frames that spoof the MAC addresses of the rogue access points, rogue ad hoc networks, and rogue clients. The WIPS is using a known Layer 2 denial-of-service attack as a countermeasure. The 802.11w-2009 amendment defines mechanisms that protects deauthentication frames. Therefore, wireless rogue containment based on management frames protected by 802.11w will not work against 802.11w rogue devices. As 802.11w compliant devices become more widely available, WIPS vendors will have to rely on other methods for rogue mitigation and prevention. Port suppression will become a more important method of rogue deterrence. Other WIPS vendors may rely more on rogue *tarpitting* methods. Tarpitting is a method used to get rogue devices to associate to a WIPS sensor. The rogue client is kept busy by the sensor and is stuck in a wireless tar pit where the rogue client cannot do any damage. WIPS vendors will most likely also develop new wireless rogue containment methods based on management frames that are not protected by 802.11w. There are multiple Layer 2 DoS attacks that are not protected by 802.11w, which might also be used as countermeasures against rogue devices.

Summary

As part of maintaining a secure and healthy WLAN environment, regular security monitoring and auditing is a requirement. Steps should be taken to ensure that all the devices on WLANs are legitimate and are operating within written security guidelines. Both Layer 1 and Layer 2 should be monitored as part of a complete WLAN security monitoring solution. Distributed WIDS monitoring offers numerous detection and analysis capabilities. Distributed WIPS monitoring offers protection against rogue devices as well as enforcement of predefined security policies.

Exam Essentials

Explain the difference between a WIDS and a WIPS WIDS solutions offer monitoring and analysis capabilities, while WIPS solutions can also offer mitigation against some attacks.

Define the components of a WIDS/WIPS architecture Understand the distributed architecture that includes a server, sensors, and management consoles. Mobile monitoring devices can also be integrated into a distributed architecture.

Explain the difference between an overlay, integrated, and integration-enabled WIDS/WIPS An overall WIPS is installed on top of a preexisting WLAN. An integrated solution uses the existing WLAN infrastructure. Integration-enabled is a hybrid of the other two solutions.

Define the various types of sensors Sensors can be standalone devices or access points that operate as either a part-time sensor or full-time sensor. Sensors are usually hardware based and can use either a single radio or multiple radios.

Understand the importance of device classification Explain the difference between authorized, unauthorized, rogue, and neighbor devices.

Explain rogue detection and mitigation Be able to explain the multiple ways that a WIPS can determine if a rogue device is connected to the wired infrastructure. Understand how rogue devices are mitigated using either wireless rogue containment or wired-side port suppression.

Describe WIDS/WIPS analysis Outline the differences between signature, behavioral, protocol, spectrum, forensic, and performance analysis.

Understand WIDS/WIPS monitoring capabilities Explain the importance of alarm thresholds and policy enforcement. Understand that false positives are a reality.

Explain 802.11n security monitoring concerns Understand that eventually WIPS sensors will need to be upgraded to properly monitor 802.11n WLANs. New attacks may surface that specifically target 802.11n devices.

Explain management frame protection Understand that some MFP solutions are currently proprietary. 802.11w will eventually standardize management frame protection, but not all Layer 2 DoS attacks will be prevented.

Key Terms

Before you take the exam, be certain you are familiar with the following terms:

Angle of Arrival (AoA)

auto-classification

behavioral analysis

Broadcast/Multicast Integrity Protocol (BIP)

direct sequencing spread spectrum (DSSS)

distributed spectrum analysis systems (DSAS)

false positive

frequency hopping spread spectrum (FHSS)

full-time sensors

High Throughput (HT)

independent basic service set (IBSS)

integrated

integrated-enabled

location configuration information (LCI)

location tracking

MAC Protocol Data Unit (MPDU)

MAC Service Data Unit (MSDU)

management frame protection (MFP)

Management MAC Protocol Data Unit (MMPDU)

mobile wireless intrusion detection system

off-channel scanning

orthogonal frequency division multiplexing (OFDM)

overlay

part-time sensors

performance analysis

port suppression

protocol analysis

protocol fuzzing

radio resource measurement (RRM)

real time location systems (RTLS)

received signal strength indicator (RSSI)

remote packet capture

RF calibration

RF fingerprinting

RF signature analysis

RF triangulation

robust management frame

rogue containment

secure-sockets-layer (SSL)

sensors

signature analysis

Simple Network Management Protocol (SNMP)

software defined radio (SDR)

standalone sensors

Time Difference of Arrival (TDoA)

time to live (TTL)

WIDS/WIPS server

wireless intrusion detection system (WIDS)

wireless intrusion prevention system (WIPS)

zero day attack

Review Questions

1. Which of these tools will best detect frequency hopping rogue devices? (Choose all that apply.)
   - **A.** Standalone spectrum analyzer
   - **B.** DSAS
   - **C.** Distributed Layer 2 WIPS
   - **D.** Mobile Layer 2 WIPS
   - **E.** Layer 2 WIPS

2. Name the labels that a WIPS uses to classify an 802.11 device. (Choose all that apply.)
   - **A.** Authorized
   - **B.** Unauthorized
   - **C.** Enabled
   - **D.** Disabled
   - **E.** Rogue
   - **F.** Neighbor

3. The ACME Corporation has recently replaced all of their older lightweight access points with HT (802.11n) access points. The WLAN controller has integrated WIPS. The controller-based APs will be used to provide access to clients. The APs will also work as part-time sensors using off-channel scanning for IDS purposes. What are some of the potential problems? (Choose all that apply.)
   - **A.** The access points cannot monitor 40 MHz channel transmissions during off-channel scanning.
   - **B.** VoWiFi communications will be disrupted by increased off-channel scanning.
   - **C.** Too much off-channel scanning creates increases in latency.
   - **D.** More channels must be monitored.
   - **E.** Too little time spent listening off-channel can expose the WLAN to potential unheard attacks.

4. A WIDS/WIPS consists of which of the following components? (Choose all that apply.)
   - **A.** WIDS/WIPS server
   - **B.** Midspan injector
   - **C.** Hardware sensors
   - **D.** Management console
   - **E.** Software sensors

5. As defined by the 802.11w-2009 amendment, which 802.11 management frames will be safeguarded by management frame protection (MFP) mechanisms? (Choose all that apply.)
   - **A.** Beacon frame
   - **B.** Deauthentication frame
   - **C.** PS-Poll frame
   - **D.** Null function frame
   - **E.** QoS action frame
   - **F.** Measurement request action frame

6. What type of WLAN attacks might be detected by a distributed WIDS/WIPS solution using a behavioral analysis software engine? (Choose all that apply.)
   - **A.** EAP flood attack
   - **B.** Deauthentication attack
   - **C.** Protocol fuzzing
   - **D.** Fake AP attack
   - **E.** CTS flood attack
   - **F.** Zero day attack

7. Management has asked Cathy, the WLAN administrator, to devise a plan for rogue mitigation for the ACME Company corporate headquarters that are located in a heavily populated area. What are the best recommendations Kathy can make? (Choose all that apply.)
   - **A.** Automatic wireless rogue containment for all devices classified as unauthorized
   - **B.** Automatic wireless rogue containment for all devices classified as rogue
   - **C.** Automatic wireless rogue containment for all devices classified as ad hoc
   - **D.** Wired-side port suppression
   - **E.** RF rogue containment using frequency jamming

8. Which method of device location tracking compares the target device's RSSI values with a database of RSSI values of the reference points?
   - **A.** RF triangulation
   - **B.** RF calibration
   - **C.** RF positioning
   - **D.** RF fingerprinting
   - **E.** TDOA

9. The ACME Company currently has a WLAN at one location using 100 autonomous APs with 1,500 VoWiFi phones communicating over the WLAN. ACME wants to add a WIPS security monitoring solution within the next six months. ACME also has a requirement that the WIPS operate 24/7 even if the WLAN is not operational. Costs and security monitoring are all concerns when choosing the proper WIPS solution. Which of these recommendations would best meet ACME's cost and security needs?

A. Install an overlay WIPS to monitor the current WLAN using autonomous APs.

B. Replace the autonomous APs with a WLAN controller solution using an integrated WIPS. The controller-based APs will operate as part-time sensors.

C. Replace the autonomous APs with a WLAN controller solution using an integrated WIPS. A number of controller-based APs will operate as full-time sensors.

D. Replace the autonomous APs with a WLAN controller solution. Install an overlay WIPS to monitor the controller-based-APs.

E. Replace the autonomous APs with a WLAN controller solution using an integrated WIPS using a WNMS for centralized monitoring.

10. What type of WLAN attacks might be detected by a distributed WIDS/WIPS solution using a signature analysis software engine? (Choose all that apply.)

A. PS-Poll flood

B. Deauthentication attack

C. Protocol fuzzing

D. Virtual carrier attack

E. CTS flood attack

F. Zero day attack

11. The ACME company plans on installing a new WLAN with 100 autonomous APs with 1,500 VoWiFi phones communicating over the WLAN. ACME expects to add 100 more APs in the next six months because coverage expansion plans. ACME wants to add a WIPS security monitoring solution within the next six months. Costs, performance, and security monitoring are all concerns when choosing the proper WIPS solution. Rogue mitigation is also an important objective. Which of these recommendations would best meet ACME's cost, performance, security, and rogue mitigation objectives?

A. Install an autonomous AP solution. Install an overlay WIPS to monitor the current WLAN using autonomous APs.

B. Install a WLAN controller solution using an integrated WIPS. The controller-based APs will operate as part-time sensors.

C. Install a WLAN controller solution using an integrated WIPS. A number of controller-based APs will operate as full-time sensors.

D. Install a WLAN controller solution. Install an overlay WIPS to monitor the controller-based APs.

12. Which of these WIDS/WIPS software modules allows an organization to view months of historical data on any suspicious WLAN device as well as all authorized devices?

A. Spectrum analysis

B. Protocol analysis

C. Forensic analysis

D. Signature analysis

13. What is the recommended ratio of WIPS sensors providing security monitoring to access points that are providing access for WLAN clients?
    - **A.** 1:2
    - **B.** 1:3
    - **C.** 1:4
    - **D.** 1:5
    - **E.** Depends on the customer's needs

14. Bob has been investigating numerous false positive alarms from the newly installed integrated WIPS solution using controller-based APs as part-time sensors. What can Bob do to reduce the number of false positives? (Choose all that apply.)
    - **A.** Lower alarm threat thresholds
    - **B.** Raise alarm threat thresholds
    - **C.** Convert some of the controller-based APs to full-time sensors
    - **D.** Disable behavioral analysis
    - **E.** Properly classify all authorized devices

15. The ACME Company currently has a WLAN with three locations. Two locations are using WLAN controllers with 90 controller-based APs at each location. A third location is using 100 autonomous APs from a different vendor. ACME wants to add a WIPS security monitoring solution within the next six months. Costs, performance, and centralized security monitoring are all concerns when choosing the proper WIPS solution. Which of these recommendations would best meet ACME's cost, performance, and security objectives?
    - **A.** Install an overlay WIPS to monitor the WLAN using autonomous APs. Use the integrated WIPS capabilities of the WLAN controllers at the other two locations.
    - **B.** Replace the autonomous APs with a WLAN controller solution at the third location. Use the integrated WIPS capabilities of the WLAN controllers at all three locations.
    - **C.** Replace the autonomous APs with a WLAN controller solution using an integrated WIPS. A number of controller-based APs will operate as full-time sensors.
    - **D.** Install an overlay WIPS to monitor the location using autonomous APs and the other locations using WLAN controllers.
    - **E.** Install standalone sensors at the location with the autonomous APs. Use the integrated WIPS capabilities of the WLAN controllers at the other two locations. Install a WNMS solution for centralized management and monitoring.

16. Why does RF fingerprinting offer more accurate device location information than simple triangulation?
    - **A.** RF fingerprinting uses known RSSI reference points in addition to measured device RSSI values.
    - **B.** RF fingerprinting uses RSSI values combined with RFID tags to find other devices.
    - **C.** Triangulation uses known signal measurement points in addition to RSSI values.
    - **D.** RF fingerprinting uses more sensors to locate devices by using a greater number of RSSI values.

17. Brooke is using an integrated WIDS/WIPS solution with controller-based APs as part-time sensors to protect the VoWiFi devices and the corporate WLAN. Brooke has not been receiving any information from the WIDS/WIPS about VoWiFi device traffic in the office, although several people are using VoWiFi phones and wireless laptops. What is the most likely cause of this problem?
    A. The VoWiFi phones are transmitting on 5 GHz channels and sensors are only scanning 2.4 GHz channels.
    B. The VoWiFi phones are transmitting on 2.4 GHz channels and sensors are only scanning 5 GHz channels.
    C. The WIPS has detected SIP traffic.
    D. The controller-based APs are busy performing wireless rogue containment.

18. What are some of the methods used by WIPS vendors to determine if a rogue device is connected to the wired network infrastructure? (Choose all that apply.)
    A. TTL packet analysis
    B. RF triangulation
    C. Signature analysis
    D. Behavioral analysis
    E. MAC table analysis
    F. Proprietary analysis

19. What are some of the methods used by WIPS vendors to determine if a Layer 3 rogue device is connected to the wired network infrastructure? (Choose all that apply.)
    A. Sensor associates with a suspected rogue device and sends traffic back to the WIPS.
    B. Sensor deauthenticates rogue clients from the suspected rogue AP and captures the association frames from the rogue clients.
    C. The WIPS looks for decremented MAC addresses.
    D. The WIPS looks for spoofed MAC addresses.

20. Which of these alarms should be configured to send an automatic notification to the WIPS administrator's phone and/or email account? (Choose all that apply.)
    A. Man-in-the-middle attack detected
    B. Unauthorized client detected
    C. Rogue AP detected
    D. Unauthorized AP detected

Answers to Review Questions

1. A, B. The radio cards inside the WIDS/WIPS sensors currently use only DSSS and OFDM technologies. Wireless networking equipment exists that uses frequency hopping spread spectrum (FHSS) transmissions in the 2.4 GHz ISM and will go undetected by Layer 2 WIPS/WIDS sensors. The proper tool to detect a frequency hopping rogue access point is a spectrum analyzer. Some WIDS/WIPS vendors have begun to offer Layer 1 distributed spectrum analysis system (DSAS) solutions.

2. A, B, E, F. Most WIDS/WIPS solutions categorize 802.11 radios into four or more classifications. An authorized device refers to any client station or access point that is an authorized member of the company's wireless network. An unauthorized device is any new 802.11 radio that has been detected but not classified as a rogue. A neighbor device refers to any client station or access point that is detected by the WIPS and whose identity is known. This type of device initially is detected as an unauthorized device. Typically, the neighbor device label is then manually assigned by an administrator. A rogue device refers to any client station or access point that is considered a potential threat. An AP is classified as a rogue if the WIPS determines that the AP is connected to the wired network.

3. B, C, D, E. An 802.11n deployment effectively doubles the amount of channels that must be monitored for IDS purposes. The WIPS solution must listen for attacks on both the 20 MHz and 40 MHz OFDM channels. Too much time spent listening off-channel will cause latency issues with VoWiFi solutions. Because more channels must be monitored, the potential of unheard attacks increases. Too little time spent listening off-channel can expose the WLAN to potential unheard attacks.

4. A, C, D, E. The typical wireless intrusion detection system is a client/server model that consists of three components:

   WIDS Server A software or hardware server acting as a central point of management.

   Management Consoles Software-based management consoles that connect back to a WIDS server as clients. These consoles can be used for 24/7 monitoring of wireless networks. More than one console can be configured.

   Sensors Hardware or software-based sensors placed strategically to listen to and capture all 802.11 communications.

5. B, E, F. The 802.11w-2009 amendment defines protection for robust management frames. The robust management frames include robust action frames, disassociation frames, and deauthentication frames. The majority of action frames are considered robust, including QoS action frames, radio measurement action frames, Block ACKs, and many more. A beacon is an 802.11 management frame that is not considered robust. A PS-Poll frame is an 802.11 control frame. A null function frame is a type of 802.11 data frame.

6. C, F. Many WIDS/WIPS solutions also utilize behavioral analysis to recognize any patterns that deviate from normal WLAN activity. Behavioral analysis identifies abnormal network behavior based on historical metrics. Behavior analysis helps detect protocol fuzzing where an attacker sends malformed input to look for bugs and programming flaws in

WLAN controller code or client station firmware. Very often, a zero day attack will create some sort of anomaly in 802.11 behavior that can be detected. An unknown threat used to exploit computer networks is known as a zero day attack. EAP floods, CTS floods, Fake AP, and deauthentication attacks are all known attacks with specific signatures that can be detected by signature analysis.

7. B, C, D. The answer to this question depends on the policy of the corporation. Defining a policy on how rogue APs are dealt with as well as a policy forbidding employees to install their own Wi-Fi devices is mandatory. Wireless rogue containment should be used very carefully. Rogue devices can be manually terminated using wireless rogue containment or a WIPS can be configured to automatically terminate any devices that are classified as rogue. Using a deauthentication countermeasure against all unauthorized devices is usually not a good idea because the WIPS may accidentally terminate legitimate APs and clients from neighboring businesses. Improper use of wireless rogue containment capabilities can create legal problems. Some organizations choose to implement wireless rogue containment manually. Any device that has been classified as rogue is a device that has been determined by the WIPS to be connected to the corporate backbone and probably should be wirelessly contained automatically. Automatic wireless rogue containment of ad hoc WLANs is usually recommended. The wired-side termination method of rogue mitigation uses the Simple Network Management Protocol (SNMP) for *port suppression*. Most WIPS can determine that the rogue access point is connected to the wired infrastructure and may be able to use SNMP to disable the managed switch port that is connected to the rogue access point.

8. D. RF fingerprinting is a method that compares the target's detected RSSI values with the RSSI values of the known reference points. If the target and the known reference point have similar RSSI values, they are located close to each other. RF fingerprinting relies on building up a database of actual measurements as they relate to particular locations. The method used to document RSSI reference points on a map is known as RF calibration. RF triangulation is a way of using received signals detected by sensors that are in known locations to find devices that are in unknown locations. TDoA uses the variation of arrival times of the same transmitted signal at three or more sensors. The speed of travel of the radio frequency is a known factor, and each of the synchronized TDoA sensors report the time of arrival of the signal from the transmitting device.

9. A. The best answer in terms of cost and security is to install an overlay WIPS to monitor the current WLAN using autonomous APs. Overlay WIDS/WIPS servers typically use a wider range of attack signatures to recognize potential threats and collect more information for WLAN health analysis. Because overlay solutions increase hardware and deployment costs, answer C might be a correct answer; however, ACME has a requirement that the WIPS operate 24/7 even if the WLAN is not operational. One advantage of the overlay model is that if the WLAN goes down, the WIDS/WIPS monitoring continues because the overlay solution is independent of the WLAN infrastructure.

10. A, B, D, E. WIDS/WIPS solutions use signature analysis to analyze frame patterns or "signatures" of known wireless intrusions and WLAN attacks. The WIDS/WIPS has a programmed database of hundreds of threat signatures of known WLAN attacks. PS-Poll floods, CTS floods, virtual carrier attacks, and deauthentication attacks are all known attacks with specific signatures that can be detected by signature analysis. Protocol fuzzing and zero day attacks might be detected by behavioral analysis.

11. C. The best answer in terms of cost and security is to install a WLAN controller solution using an integrated WIPS. A number of controller-based APs must operate as full-time sensors. Part-time sensors may suspend off-channel scanning if a VoWiFi phone is associated with the access point, because off-channel scanning is notorious for causing "choppy audio" during an active voice call from a VoWiFi device associated to a controller-based AP. If the off-channel scanning is suspended due to VoWiFi communications, WLAN security monitoring is also suspended. A time slicing AP/sensor must go off-channel for an extended period of time to contain a rogue device, and the AP is not on its home channel providing access to clients. Note that most WLAN controller companies have a configuration setting that prevents a time slicing AP/sensor from performing wireless rogue containment when clients are associated. If clients are associated with all the APs, a device is not available for proper wireless rogue containment.

12. C. Enterprise WIDS/WIPS may provide forensic analysis that allows an administrator to retrace the actions of any single WLAN device down to the minute. You can rewind and review minute-by-minute records of connectivity and communications within a WLAN. The WIPS records and stores hundreds of data points per WLAN device, per connection, per minute. This allows an organization to view months of historical data. Information such as channel activity, signal characteristics, device activity, and traffic flow and attacks can all be viewed historically.

13. E. The answer often depends on the budget and the value of what network resources are being protected by WLAN security monitoring. The best answer is that you can never have too many sensors. When WLAN security monitoring is deployed, the more sensors the better. Every WLAN vendor has their own sensor deployment recommendations and guidelines, but a ratio of one sensor for every three-to-five access points is highly recommended. When WLAN security monitoring is an extremely high priority and cost is not an issue, the more sensor devices the better. WIDS/WIPS deployments at military bases often follow a ratio of one sensor for every two APs or may even deploy with a 1:1 ratio.

14. A, E. Corrupted frames are the leading cause of false positives, but improper configuration of the WIPS or misinterpretation of alarms by administrators can also lead to false positive alarms. Proper classification of all devices as either authorized or neighbor devices is important. If devices are not properly classified, many alarms will be triggered. Setting alarm thresholds can often be difficult and time-consuming to achieve a balance in detecting possible attacks versus triggering false positive alarms. Some inaccurate reporting of events, seen as false positives, are unavoidable. However, properly setting alarm thresholds that are fine-tuned to the on-site RF environment can greatly reduce the number of false positives. When an integrated WIPS using controller-based APs is deployed, it is always a highly recommended practice to convert a number of the controller-based APs into full-time sensors. However, using full-time sensors does not necessarily decrease false positives.

15. E. The best answer in terms of cost and security is to install standalone sensors at the location with the autonomous APs. The integrated WIPS capabilities of the WLAN controllers at the other two locations can be utilized and a wireless network management system (WNMS) can be used for centralized management and security monitoring. WNMS servers are used as a central point of management for multiple WLAN controllers in a large-scale WLAN enterprise. The current WNMS servers that are used to manage multiple WLAN controllers from a single vendor may also be used to manage other vendors' WLAN infrastructure, including autonomous APs. An enterprise WIDS/WIPS may be configured to work together with a wireless network management system (WNMS).

16. A. RF fingerprinting compares RSSI values collected with measured RSSI values from known points to better pinpoint the location of the device being tracked and can do so with fewer sensors. However, RF fingerprinting solutions are more costly and require more time to set up and calibrate. Recalibration is required should the RF environment change.

17. C. Controller-based APs configured as part-time sensors use off-channel scanning for security and performance monitoring purposes. Part-time sensors may suspend the off-channel scanning if VoWiFi communications are occurring. Most WLAN controller vendors have an option that suspends off-channel scanning if any voice protocols, such as Session Initiation Protocol (SIP) or SpectraLink Radio Protocol (SRP), are detected. If the off-channel scanning is suspended due to VoWiFi communications, the WLAN security and performance monitoring is also suspended.

18. A, E, F. Given that an AP acts as a Layer 2 bridge, a WIPS solution builds a MAC table that correlates both the wired-side MAC address and wireless-side MAC address (BSSID) of the access point. This correlated MAC table can then be compared to the database of authorized devices. Any unauthorized device that is detected by both a sensor on the wireless side and by SNMP on the wired side will then be classified as rogue AP. Another method often used to determine if a device is connected to the wired backbone is by looking at ARP requests from a wired device, such as a core router, and by analyzing MAC tables. The WIDS/WIPS solution will look at the wired/wireless MAC tables. Any unauthorized BSSID transmitting an ARP request with the source address of the wired router will be classified as a rogue AP. Another method for possibly determining if there is a potential rogue device connected to the wired network is to examine time-to-live (TTL) values of IP packets. Wi-Fi routers will lower the TTL value of a packet when it flows through the device. WIDS/WIPS vendors may also use proprietary rogue detection and classification.

19. A, C. One method of classifying Layer 3 rogue devices is to have a nearby sensor associate with an unauthorized suspect rogue AP. The sensor then sends traffic, such as a ping, back to the WIPS server. If the traffic reaches the server on the wired side, the suspected rogue AP is confirmed to be on the internal network and then classified as a rogue. However, very often a rogue Wi-Fi router will have configured security such as WEP or WPA. A sensor will not be able to associate with the rogue Wi-Fi router because the sensor does not know the rogue Wi-Fi router security settings. The majority of the WLAN vendors that manufacture home Wi-Fi routers use MAC addresses that are one bit apart on the wireless and wired interfaces. Methods of Layer 2 rogue detection can be augmented by looking for wired MAC addresses one bit higher or one bit lower than the BSSID detected by a sensor.

20. A, C. As the administrator, you should configure automatic notifications to trigger only if an alarm is of specific importance. You will want to be alerted to the fact that a rogue is on the network or an attack is occurring. However, you would not want to know every time a WLAN device is detected unless a no-wireless zone was being enforced. Typically, alarms with a threat level of critical or severe are also configured for notification. It should be noted that any AP or client that is initially classified as unauthorized should still be investigated as soon as time permits.

Chapter 11

VPNs, Remote Access, and Guest Access Services

IN THIS CHAPTER, YOU WILL LEARN ABOUT THE FOLLOWING:

- ✓ **VPN Technology in 802.11 WLAN Architecture**
  - VPN 101
  - Client software
  - WLAN controllers: VPN server for client access
  - VPN client security at public hotspots
  - Controller-to-Controller VPNs and Site-to-Site VPNs
  - VPNs used to protect bridge links
- ✓ **Remote access**
  - Remote AP
  - RAP tunneling
  - RAP bridging
  - RAP split tunnel
  - Branch offices: virtual branch networking
- ✓ **Hotspots/public access networks**
  - Captive portal
  - Features
  - User-based authentication methods
  - Segmentation

In this chapter, you will learn some of the ways that VPNs are being used in conjunction with wireless LAN controllers to extend the WLAN to remote branch offices, home offices, or just about anywhere a road warrior might need to access the corporate network. You will also learn about remote access points and how controller vendors are integrating VPNs into APs to provide secure remote access from a single device. Finally, you will learn how captive portals are used to provide guest access at hotspots and on corporate networks.

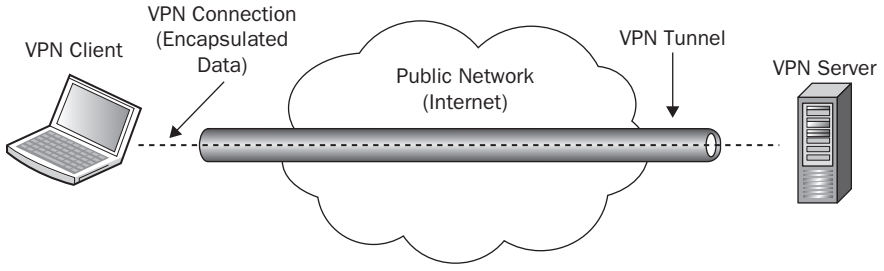
VPN Technology in 802.11 WLAN Architecture

Virtual private networks are used in many ways with wireless LANs. In Chapter 2, "Legacy 802.11 Security," you learned how VPNs were used in legacy 802.11 networks. PPTP and L2TP/IPsec VPNs were often used to secure the communications between the wireless client and the enterprise's core network. The VPN technology provided a higher level of security than what was available at that time on the earlier wireless LANs. An IPsec VPN uses Layer 3 encryption; therefore, the data payload that is encrypted is Layer 4–7 information. In the past, VPNs were used to provide data privacy for WLAN clients because strong Layer 2 encryption solutions did not exist. WPA/WPA2 solutions can now provide Layer 2 encryption using either TKIP or CCMP; therefore, using VPNs for client-based WLAN security is no longer necessary or recommended in the enterprise. Note that VPN technology did not become obsolete, only its use for securing the client's wireless communications on the enterprise network. VPNs are still used to provide client-based security at remote WLAN locations. Furthermore, VPNs are still used for data privacy between WLAN architecture devices such as controllers, bridges, and remote access points. This section will explain some of the ways that VPNs are currently being used with WLANs to extend the WLAN and provide security.

VPN 101

Before discussing the ways that VPNs are being used, it is important to make sure that we review what a VPN is, what it does, how it works, and the components that are configured to construct one. By now you know that a VPN is a virtual private network. But what does that really mean? As shown in Figure 11.1, VPN is essentially a private network that is created or extended across a public network. In order for a VPN to work, two computers or devices communicate to establish what is known as the VPN tunnel. Typically, a VPN client initiates the connection by trying to communicate with the VPN server.

FIGURE 11.1 VPN components



The VPN client can be a computer, router, WLAN controller, or even an AP, which you will learn about later in this chapter. When the client and the server are able to communicate with each other, the client will attempt to authenticate with the server by sending its credentials. The server will take the client's credentials and validate them. If the client's credentials are valid, the server and client will create the VPN tunnel between them. Any data that is sent from the VPN client to the VPN server is encapsulated in the VPN tunnel. The client and the server also agree on if and how the data will be encrypted. Prior to the data being encapsulated in the tunnel, the data is encrypted to make sure that, as it travels through the tunnel, it cannot be compromised. Since the underlying premise of a VPN is that the data is traveling across an insecure public network, security is one of the primary reasons for implementing a VPN.

When the client and server build the tunnel, it is their responsibility to route the data across the public network between the two devices. They take the data from the local network, encrypt and encapsulate it, and then send it to the other device, where it is unencapsulated and decrypted, and then placed on the local network of the other device.

Real World Scenario

VPN Analogy

To understand the concepts of VPNs and encapsulation, imagine a company that has two buildings in a city where the buildings are separated by a distance of two kilometers. Since these buildings are very large, and many people travel between the buildings, the company decides to purchase buses to transport people back and forth between the buildings. The driver of the bus is responsible for driving from the pickup point of the first building to the drop-off point of the second building. The route the driver takes may vary depending on traffic. The employees in the first building know that if they go to the pickup point and board the bus, when they exit the bus they will be at the drop-off location of the second building; just as when the data arrives at the VPN client it will be tunneled and arrive at the VPN server.

The employees are given directions instructing them to get on the bus at the pickup point and to get off the bus at the drop-off point. The employees would not have to understand the route that they were taking through the city. The employees were essentially encapsulated and secured in the climate-controlled bus as they traveled between the offices.

In a VPN network, the client and server provide the transportation just as the bus did. The city streets make up the many routes that the bus could take, just as the Internet has many routes that the packets can take. The passengers travel inside the bus just as the data is transmitted inside the packets. The packet is directed through the network just as the bus is directed through the city.

Now that you are familiar with the basic workings of a VPN, it is time to review how VPNs are implemented. There are two typical ways of installing and configuring a VPN: site-to-site, also known as network-to-network, and client-to-server also known as client-to-network.

The site-to-site installation is typically used when a company has two or more locations. Often specialty VPN devices or routers with VPN software are configured at each location to provide a continuous connection between the two locations. This type of configuration makes both networks appear as if they are one large network. Site-to-site VPNs can be used to connect multiple networks, with each VPN extending the network to a new location.

The client-to-server installation is normally used when one of the locations is permanent and the other is not, or when there is no need for a continuous connection. This is typical when a company has people who want to work from home and need access to the corporate

network, or when people are traveling and need access to the corporate network. In this configuration, a VPN server is configured and installed on the company's network, and the remote user has the VPN client. The client could be an appliance; for example, someone working from home may have a home router/VPN client that is configured to connect automatically to the corporate network. The client could also be specialty software installed on the person's laptop computer, or the dial-up software that is built into the operating system of the laptop. When the traveling user needs to connect to the corporate network, he or she simply initiates the VPN client and types in his or her login credentials. The VPN server then validates the user and, if the credentials are correct, allows them to have access to the corporate network.

VPN Client

As mentioned earlier, one of the key components of a client-to-server VPN is the *VPN client*. Whether the VPN client is software running on a personal computer or a hardware device, the client needs to be configured properly in order to establish the VPN connection. The information that needs to be entered on the client is:

- The network address of the VPN server to which the client is connecting
- The proper credentials to authenticate with the VPN server
- The proper security parameters

In order for the client to connect to the VPN server, the server must have an IP address that can be reached by the client. This is often referred to as a publicly available address. The VPN server can either be directly connected to the Internet using this IP address, or more likely, the Internet firewall will forward the VPN traffic to the VPN server. The server address is typically an IP address or a URL. The next setting that is needed by the client is the VPN type. Since security is important, the security will typically be L2TP over IPsec. A shared secret key, sometimes referred to as a preshared key for authentication, will also be needed. This shared secret key needs to match the one entered on the VPN server in order for the authentication process to continue. Once the key is validated, then a username and password is used for authentication.

If the client is a personal computer, typically all the information is entered when creating the VPN connection, or all the information except for the username and password is entered. If the client is a hardware device, then all these settings are entered into the device. When the device is connected to the network, it will automatically attempt to connect and authenticate with the VPN server.

WLAN Controllers: VPN Server for Client Access

In the early days of VPNs, the VPN server was often a dedicated hardware device designed and configured to function solely as a VPN server. Prior to the widespread acceptance of WPA/WPA2, VPNs were used for client-based WLAN security. The VPN server was

usually a standalone device and the WLAN infrastructure was usually autonomous APs. Layer 2 WEP static encryption was also often used as an overlay on top of an IPsec VPN tunnel. WPA/WPA2 provides a higher level of security along with less overhead and easier configuration on both the client and server. Since WPA/WPA2 is a superior technology for 802.11 wireless networking, it is the preferred method of providing client-based security in the enterprise. There are still valid reasons for some companies to use VPN technology to secure their wireless clients. VPNs can still be used with older client devices that do not support the newer security protocols.

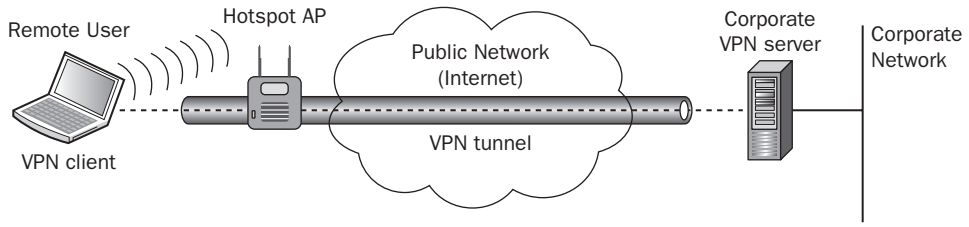
A VPN server does not have to be a standalone server. A VPN server can be integrated into many different types of devices. Some of the WLAN controller vendors have integrated VPN serving capabilities into their controllers. The VPN server that is integrated within a WLAN controller can be used to provide VPN tunnels for WLAN clients. However, it should be noted that the integrated VPN servers found in WLAN controllers are normally used for other architectural VPN solutions that will be discussed later in this chapter.

VPN Client Security at Public Hotspots

So having just stated that you should not use VPNs to secure your WLAN clients because there are better methods, we are now going to tell you that VPNs are not dead and at times should be used for client-based security. Yes, there is some rhyme and reason to this statement, and no, we are not going back on our previous statement. If you think back, we stated that VPNs are a good way of providing security to wireless users when the wireless network does not provide a high level of security. In the enterprise environment, a robust security network (RSN) will use 802.1X/EAP for authentication and TKIP or CCMP for dynamic encryption. The insecure WLAN environments where we still highly recommend that you use VPNs for client-based security are public access WLANs and hotspots that do not provide security. Because most hotspots do not provide Layer 2 security, it is imperative that end-users provide their own security. VPN technology is mandatory for remote access when end-users connect to public access WLANs. Since no encryption is used at public access WLANs, a VPN solution is needed to provide for data privacy.

Most public networks and hotspots do not provide a high level of security. Many provide simple captive-portal authentication, verifying your identity and that you are a valid user on their network. Captive-portal authentication is a very weak authentication method and, more importantly, does not provide any data privacy. To secure the 802.11 data transmissions, you need to encrypt it. Since the public network or hotspot provider is not providing encryption, it is necessary for you to protect your own data. The easiest and best way of securing your data on a public network is to use a VPN. Figure 11.2 illustrates a VPN established between a client personal computer and a VPN server. In this illustration, the client is connected to the Internet through a public hotspot.

FIGURE 11.2 VPN established from a public hotspot



Many organizations already have VPN servers installed to provide secure access to the enterprise network for people who work from home and/or travel. A VPN server is indifferent to how a VPN client connects to it. Therefore, you can use the same VPN client software to connect to the corporate VPN server no matter how you connect to the Internet: wired, 802.11 wireless, or even through a cellular modem. As long as the VPN client can communicate with the VPN server, it will be able to establish a VPN connection. Note that we are assuming that there are no firewalls or filters blocking the VPN packets between the VPN client and VPN server. The VPN encryption provides data privacy for the WLAN environment as well as providing for data privacy across the Internet.

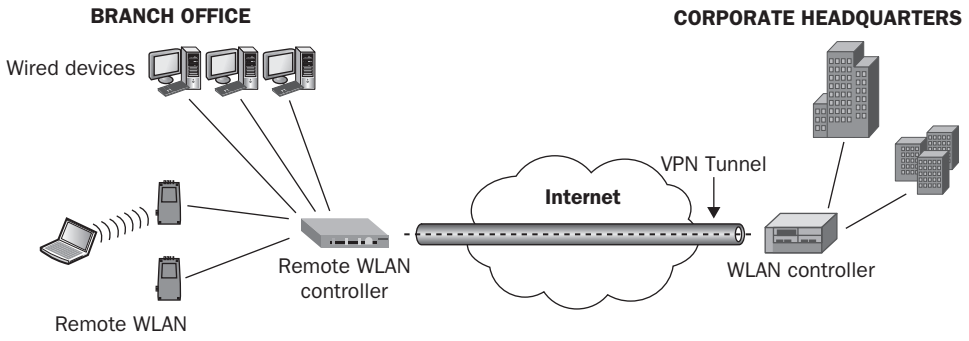
Controller-to-Controller VPNs and Site-to-Site VPNs

Over the past ten years, wireless networking has increasingly become a commonplace technology to connect users to the organizations core network. A key reason for this is its ease of installation and flexibility. Another important transition that has occurred is the need for companies to provide connectivity for most, if not all, employees. In the past, it was sufficient for people to perform their daily job tasks on their computer—in some cases a computer that was shared between employees—and then to upload or transmit the data to the corporate headquarters at the end of the day, or even the end of the week. This is typically no longer the case. With the proliferation of email as an integral work tool along with the need to have quicker access to information, Internet access and access to the corporate network is vital to most employees

With corporate and Internet access so important, companies have obviously sought to provide these capabilities in a cost-effective manner. It is impractical and cost prohibitive for most organizations to install dedicated links between their locations. Organizations have found VPNs to be an efficient and cost-effective way of providing secure site-to-site networking. Remote locations can inexpensively connect to the Internet using a cable modem or DSL connection, and then establish a VPN between the locations.

For scaling purposes, WLAN controllers are often deployed at both corporate headquarters as well as at branch offices. Any data communications across the Internet between WLAN controllers should be protected with a site-to-site VPN. Any user traffic that is being forwarded from a remote location to corporate headquarters requires the data privacy that the encryption from a site-to-site VPN can provide. Most WLAN controllers offer the VPN capabilities needed to provide for a site-to-site VPN. As shown in Figure 11.3, a branch office WLAN controller with VPN capabilities can tunnel WLAN client traffic and bridged wired-side traffic back to the corporate network.

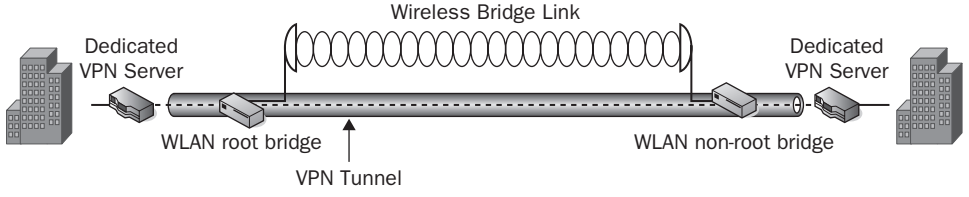
FIGURE 11.3 Site-to-site VPN with WLAN controllers



VPNs Used to Protect Bridge Links

Another use of VPNs is to provide security for 802.11 WLAN bridges links. In addition to using 802.11 wireless technology to provide client access, 802.11 technology is used to create bridged networks between two or more locations. As discussed in the *CWNA: Certified Wireless Network Administrator Official Study Guide: (Exam PW0-104)*, by David D. Coleman and David A. Westcott (Sybex, 2009), point-to-point (PTP) or point-to-multipoint (PTMP) connections can be created to connect wired networks wirelessly. WLAN bridging is most often used to provide wireless backhaul links between buildings. WLAN bridge links can cover many kilometers if properly and legally deployed. As with any 802.11 wireless network, the wireless backhaul communication needs to be protected with encryption. When WLAN bridges are deployed for wireless backhaul communications, VPN technology can be used to provide the necessary level of data privacy. Depending on the bridging equipment used, VPN capabilities may be integrated into the bridges, or you may need to use other devices or software to provide the VPN. Figure 11.4 shows an example of a point-to-point wireless bridge network using dedicated VPN devices. A site-to-site VPN tunnel is used to provide encryption of the 802.11 communications between the two WLAN bridges.

FIGURE 11.4 WLAN bridging and VPN security



Remote Access

As we have been discussing in this chapter, secure remote access has become an important component of many enterprise networks. A user might access corporate resources across the Internet using a client-based VPN solution. However, that method does not push the corporate WLAN to remote locations. WLAN vendors offer several methods to scale the WLAN across the Internet to remote locations. The most common method is to use controller-to-controller links, which can then be used to extend the corporate WLAN to remote sites. We have already discussed how communications between WLAN controllers should be secured with a site-to-site VPN across the Internet. Another method that is growing in popularity is to use single access points as a remote solution across a WAN link to extend the corporate WLAN.

Remote AP

As computers and networks become a more critical component in everyday business, companies need to identify ways of securely connecting satellite office locations and remote employees to the corporate network. This has historically been done with either dedicated private WAN links or VPN connections through the Internet. Over the past ten years, the expansion of wireless networking has made computing more flexible and has expanded the capabilities of the network. Because of the increased freedom provided by wireless networking, in addition to wanting secure access from the remote locations to the corporate network, many of these remote locations either require or want their network to be a wireless one. So now, in addition to providing and securing the WAN connection to the remote site, the IT staff must also provide a secure WLAN.

As mentioned earlier in this chapter, VPNs are often used to provide secure access to the enterprise network from a remote location. In the past, if the remote location needed continuous connectivity to the organization's network, it was common for the organization to purchase dedicated VPN appliances to provide this connectivity. If the remote location needed periodic access to the organization's network, or if the remote location was not a fixed location, such as a traveling user, VPN access was often handled using dial-up software.

With the added need for a WLAN, locations that used VPN appliances also had to purchase and install APs. The home user could purchase an AP for their house, but traveling users were typically limited to the network that was available at their hotel.

Although VPNs are a great way of providing secure connectivity, they also add an additional layer of complexity and often an additional device, possibly from a different vendor, that the IT staff must support. In most instances, these VPN appliances are standalone devices that have to be managed and updated individually. When a WLAN is also needed, it is common to install autonomous APs. These autonomous APs also have to be managed and updated individually. These APs typically are not configured with the

same authentication and encryption protocols that are provided on the enterprise WLAN, and the client must use a different method to connect to the WLAN.

To solve many of these problems, a new classification of AP has been created, referred to as a *remote access point (RAP)*. A RAP provides both VPN connectivity back to the enterprise network, and it also provides wireless networking. The remote AP has VPN client software integrated into it. Typically, the IT department will configure the RAP with the necessary VPN parameters and then give it or ship it to the remote user or remote site. The RAP is then plugged into the wired LAN at the remote site. When the RAP boots up, using DHCP it will obtain an IP address, subnet mask, and default gateway. At that point, the RAP should be able to communicate on the local LAN and out to the Internet. Then, using the integrated VPN client capabilities, the remote AP establishes a VPN tunnel between itself and a VPN server back at corporate headquarters. Once the VPN tunnel is established, the RAP will communicate through the VPN to the WLAN controller, from which the RAP will download its WLAN configuration. This information is used by the RAP to configure the SSID, security settings, radio channel, and RF power settings, along with various other AP settings. The VPN server may be a standalone VPN server, or it is often integrated within a WLAN controller that exists back at corporate headquarters. In either case, the WLAN profiles used by the remote APs originate from the WLAN controller.

Some remote access points can even be shipped directly to the end-user without being preconfigured. When the end-user receives the RAP, they first need to connect it to a wired Internet connection. Then the user must wirelessly connect to the RAP. When the user connects to the AP, they are prompted to enter some basic information provided to them by the IT department. Using this information, the RAP will automatically connect to the enterprise network and download its configuration.

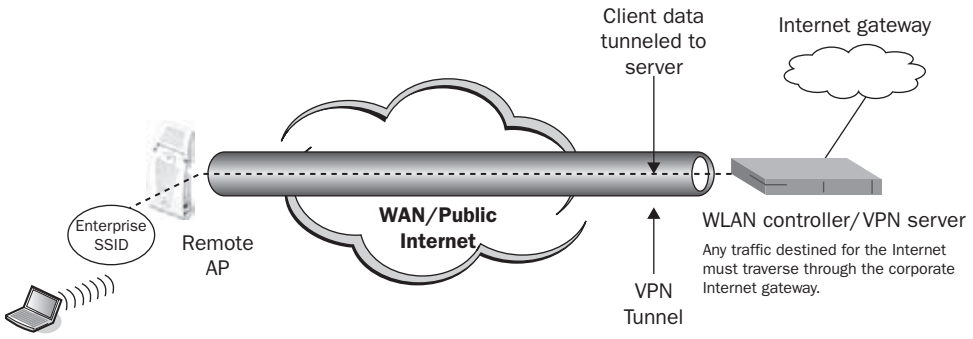
RAPs provide many benefits that to an organization. Since the RAP is communicating to the WLAN controller, once the VPN is established network settings and changes can be made at the controller and pushed to the RAP. The RAP does not have to be managed individually. It is treated just like any other AP that tunnels to a WLAN controller. This also allows the RAP to provide the same SSIDs, VLANS, authentication, and encryption protocols, providing a much higher level of security at the remote site than is typically available. Since the RAP can be configured to advertise the same networks as any other AP within the enterprise, the logon process for the organization can be identical no matter where the user connects. Because access throughout the organization will be identical, users will be familiar and comfortable with connecting to the WLAN, no matter what their location.

Another benefit of remote APs is the ability to configure them in multiple networking modes: tunneling, bridging, and split tunneling. This flexibility allows organizations to customize the RAP to best meet their networking and security needs. These modes can be configured per SSID, so a single RAP could have an employee SSID configured with tunneling and a guest SSID configured with bridging. The following sections explain these networking modes.

RAP Tunneling

Tunneling is a traditional configuration for a VPN. When the wireless radio of the RAP receives data from a wireless client, the data is automatically forwarded to the VPN client that is integrated into the RAP. The remote AP then forwards the WLAN traffic through a secure VPN tunnel back to the corporate enterprise network where a VPN server resides. Organizations that want more control of the data will typically configure *remote AP tunneling* on the remote AP. Forcing all data back to the enterprise network can allow the organization to perform content filtering on the traffic, or to make sure that all data is scanned for viruses. As shown in Figure 11.5, any traffic destined for the Internet must go through the VPN tunnel and use the Internet gateway at corporate headquarters.

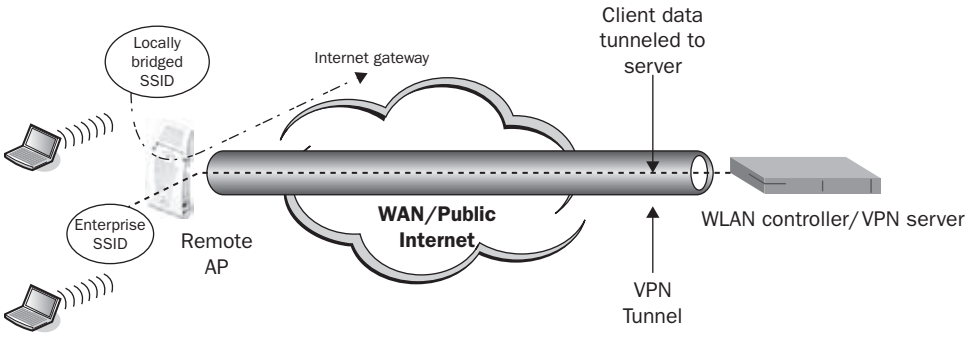
FIGURE 11.5 Remote AP tunneling



RAP Bridging

Although the main purpose of the RAP is to provide the enterprise user with a secure connection back to the organization's core network, remote APs are also often used to provide guest access to a separate gateway to the Internet. A remote location, such as a satellite classroom for a university or training company, may need to provide secure access for the local staff, but also guest access for students who just need to access the Internet. To provide both these services, the RAP would first be configured in tunneling mode with an enterprise SSID and 802.1X/EAP enabled. Any WLAN traffic used with this SSID is routed back through the VPN tunnel, as described in the previous section. The remote AP would then be configured with a second SSID. This second SSID would provide access to the students or guest users. This second SSID would be configured with authentication to ensure that only valid students or guests were able to access it. The second SSID is a locally bridged SSID that only sends traffic to a local Internet gateway. In this mode, any wireless traffic from users connecting to the second SSID would be routed directly to a gateway to the Internet. Any users connecting to the enterprise SSID would still have their traffic tunneled back to corporate headquarters. The enterprise SSID originates from a corporate WLAN controller whereas the second SSID is unique to the local remote AP. Figure 11.6 shows a RAP that is configured for both RAP tunneling and *remote AP bridging*.

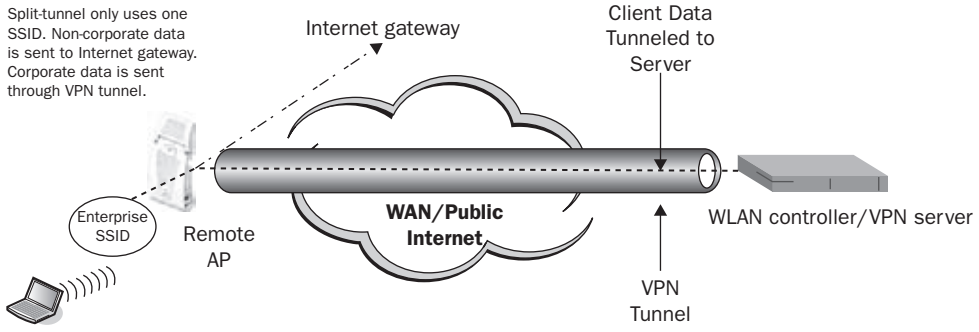
FIGURE 11.6 Remote AP, locally bridged SSID



RAP Split Tunneling

Many people are already familiar with the concept of split-tunnel VPNs and many remote AP solutions can also provide a split-tunnel solution. When a remote AP is configured for tunneling, all of the user data is tunneled back to the enterprise network. If a user is connected to the RAP, no matter where they are connecting from, even their Internet traffic must be sent to the enterprise network before it is forwarded to the Internet. Some extremely security-conscious companies like this configuration because they can monitor and filter all the traffic on their network. Most organizations would rather not have traffic destined for the Internet traverse the enterprise network. If a remote AP is configured in *remote AP split-tunneling* mode, the enterprise SSID would be configured to require an 802.1X/EAP logon for the employees. After the employees are logged on, the RAP analyzes their traffic as it is received. A firewall policy enforced on the RAP ensures that any traffic that is destined for the enterprise network would be sent through the VPN tunnel. Any traffic that is destined for the Internet would be sent directly to the Internet gateway. Figure 11.7 shows a RAP that is configured for split-tunnel VPN. Depending on the destination of the traffic, some of the data is tunneled back to the enterprise WLAN controller and some of the data is routed to a gateway to the Internet.

FIGURE 11.7 Remote AP split-tunnel VPN



How does a remote AP using a split-tunnel solution differ from a remote AP using a locally bridged SSID? A remote AP that uses a split tunnel needs only one SSID for wireless user connectivity. The split tunnel can provide access either to the Internet gateway or back through the VPN tunnel with the single SSID. The bridging mode solution described earlier requires two separate SSIDs. One enterprise SSID routes traffic through the VPN tunnel, and a second locally bridged SSID provides a route to the Internet gateway.

Virtual Branch Office Networking

To perform their jobs properly, remote employees and off-site locations typically require the same technologies as the rest of the organization's in-house employees, such as secure access to real-time data applications, email, voice, and video. Some of the wireless controller companies have realized the need for organizations to provide the same level of connectivity and wireless networking to their remote users that they provide to the users at their main offices. Using the RAP technology discussed earlier in this chapter, organizations are able to extend these services securely to these off-site offices and homes, creating what is referred to *virtual branch offices*.

Some of the vendors have designed their controllers so that, not only can the controller provide the necessary wireless services at the remote location but, with VPN services integrated into the controller, these services can be provided in one device. Additionally, the wireless controller vendors offer numerous controller models, allowing organizations the flexibility to purchase controllers large or small enough to meet their specific needs.

Hotspots/Public Access Networks

The term *hotspot* typically refers to a free or pay-for-use wireless network that is provided as a service by a business. When people think of hotspots, they typically associate them with cafes, bookstores, or a hospitality-type business such as a hotel or convention center. A companion network to the hotspot is the *guest network*. Although hotspots and guest networks are essentially the same, the difference between them has to do with the reason for installing them and the target audience.

A hotspot provider is typically providing the service either as a pay-for-use service or to attract business. Travelers often frequent restaurants or cafes that are known to provide free Internet access. Many of these establishments benefit from the increased business generated by offering the hotspot.

A guest network is typically provided by businesses as a convenience to visitors. These guest networks allow Internet access to visitors, such as contractors, students, or salespeople. Many organizations understand the need and importance for their visitors to be able to access the Internet, especially to access email. Therefore, many organizations provide WLAN guest access with a unique SSID and user VLAN. Firewalls are also often used to further restrict the guest user capabilities and even the bandwidth that is available to guests. Guest networks are a courtesy and these filters prevent abuse of the guest services.

One of the problems with a guest network is restricting access to a select group of people. At a hotspot, access should be limited to paid customers. On a corporate guest network, access is limited to invited guests. Providing users with encryption keys is not practical because it can be cumbersome to change the keys frequently. The keys could also be easily shared with other users, compromising the security of the network. Having users configure an 802.1X/EAP client is also not practical due to the difficulty of the task, and the guest user may not have enough technical capability to configure all of the necessary settings. Because of the ease of use and the ability to provide different levels of authentication, captive portal is the most widely used method for providing guest access. Captive portal solutions are usually integrated as a feature within an autonomous AP or WLAN controller; however, standalone captive portal solutions also exist.

Captive Portal

Most hotspots and guest networks are secured by a *captive portal*. A captive portal is essentially the integration of a firewall with an authentication web page. Although captive portals are often associated with hotspots and wireless guest networks, the technology is not specifically affiliated with wireless networks. When a user connects to the guest network, whether wired or wireless, any packets that the user transmits are intercepted and blocked from accessing a gateway to the network resources until the user has authenticated through the captive portal. To authenticate, the user must launch a web browser. After the browser is launched and the user attempts to go to a website, no matter what web page the user attempts to browse, the user is redirected to a logon prompt which is the captive portal logon web page. Figure 11.8 shows the logon section of a captive portal web page at a hotel. This hotel chain provides guests with an access code when they register for their room. The guest can log on to the network by either entering this access code, or if they are a frequent traveler, they can sign in using their frequent traveler Username/Account number and Password/PIN code.

FIGURE 11.8 Hotel captive portal logon screen

Features

Captive portal are available as standalone software solutions, however, most WLAN controllers and some autonomous APs offer captive portal capabilities. When configuring a captive portal, you have available many options and features to customize it. Vendors that support captive portals provide the ability to customize the captive portal page. You can typically personalize the page by adding graphics, such as a company logo; inserting an acceptable use policy; and configuring the logon requirements.

Authenticating to a captive portal typically requires the user to enter a username and password. This username and password are verified, and if they are valid, the user is then allowed to access other resources, such as the Internet. Most hotspots and corporate guest networks are configured this way. Since a username and password are required, when the user is redirected to the captive portal, the user most likely be redirected to an HTTPS page. This will ensure that the exchange of the username and password are secure. A captive portal turns a Web browser into an authentication device. Captive portals can redirect unauthenticated users to a login page using an IP redirect, DNS redirection or redirection by HTTP. The most common method is redirection by HTTP.

Not all captive portal pages require a username and password for authentication. Some organizations configure the captive portal only to require the user to enter their email address in order to connect to the network. In fact, many of these captive portals do not even verify that an email address was entered. In many instances the user can type anything and it will be accepted. So, if it doesn't matter what was typed, why not just use an open SSID? The benefit of a captive portal over an open SSID is that most networks with captive portals have an acceptable use policy. When the user connects to the captive portal, the acceptable use policy or a link to it is usually displayed on the captive portal page, along

with a statement such as "Logging in as a registered user indicates that you have read and accepted the Acceptable Use Policy." This disclaimer, along with the acceptable use policy, may provide the organization with some legal protection if the user did something illegal while connected to the network. This disclaimer can also give the organization the right to disconnect the user from the network if they violate the rules of the acceptable use policy.

Segmentation

When an access point is configured to be used as a hotspot, its sole purpose is usually to provide access to guest users. When an AP is configured in an organization to provide wireless access, the access point is often configured with two or more SSIDs. The AP is often configured with the organization's primary SSID, which allows employees access to the corporate network, and also with the guest SSID that allows guest access to the Internet. When an AP is configured with multiple SSIDs, and those SSIDs provide different levels of access, *segmentation* is often recommended so that the traffic from the two wireless networks is placed on separate VLANS. This is especially true if one of the wireless networks provides guest access.

When configuring the guest wireless LAN, create a separate SSID and VLAN that will only transport the guest traffic. The guest network will be configured to completely restrict access to the organizations internal network, have limited access to the Internet, and often have bandwidth filters to prevent excessive use of the network. Creating separate VLANs should make it easier to create and manage the firewall policies that control the guest traffic.

User-Based Authentication Methods

When a user logs on to a captive portal, the username and password needs to be authenticated to make sure that it is valid. This is usually done by either a RADIUS server or an internal database on an autonomous AP or WLAN controller. If the captive portal is part of a paid hotspot service, when the user signs up for the service, a username and password are created in the database and a RADIUS server is used to validate the users when they log on to the wireless network. The signup process for the user is integrated with a credit card entry system and is fully automated.

Unfortunately, the captive portal network that provides guest access usually does not have an automated registration window. In addition to not having an automated registration window, the person who manages the user database is often unwilling to add interim guest accounts to the corporate database. Due to these obstacles, many vendors who provide captive portals also incorporate an internal database in the AP or controller that allows the wireless administrator to create guest user accounts. Some vendors have even created special administration accounts with limited capabilities. These special administration accounts can be used to assign a security guard or receptionist the ability to create the guest accounts. The security guard or receptionist can create accounts for a limited period of time, with the account automatically being deleted when the expiration date and time is reached.

Summary

In this chapter, you learned about the different VPN technologies and how VPNs are used to provide security for wireless networking. We discussed the configuration parameters for VPNs along with their uses with hotspots, site-to-site networks, and wireless bridge links. VPNs are rarely used for client-based security in the enterprise. VPNs should always be used for client-based security when clients are using public access WLANs and hotspots.

A new classification of access points known as remote APs combines the capabilities of a VPN with the functionality of a wireless AP. Remote APs are used to extend the organizations wireless network securely to remote locations, creating virtual branch offices. RAPs can support both employee and guest networking. The user traffic can be forwarded to the enterprise network or directly to the Internet using one of three different modes: tunneling, bridging, or split tunneling.

Hotspots and public access networks provide Internet access to guests and visitors. Hotspots are typically commercially based, either as paid-for services or as part of a paid service. Guest networks are usually created by businesses as a courtesy, providing access to visitors. A captive portal is used to authenticate users onto both of these guest networks. A captive portal provides authentication but does not provide encryption. Guest networks are often segmented, and firewalls typically limit the capabilities and bandwidth that guests are allowed.

Exam Essentials

Understand the fundamentals of VPNs. Be able to explain the different components and functions of a VPN, including the client and server.

Explain the different ways that VPNs are used. Explain how VPNs are used to provide security at public hotspots, site-to-site network connections between controllers, and wireless bridge links.

Describe remote AP technology and configuration. Describe what a RAP is and how it functions. Know the three networking modes: tunneling, bridging, and split tunneling.

Understand hotspots and public access networks. Describe how guest access is provided through hotspots and guest networks. Explain the features and benefits of captive portal.

Key Terms

captive portal
guest network
hotspot
remote access point (RAP)
remote AP bridging
remote AP split tunneling
remote AP tunneling
segmentation
virtual branch office
virtual private network (VPN)
VPN client
VPN tunnel

Review Questions

1. Which of these solutions is an example of a site-to-site VPN in use? (Choose all that apply.)
   - **A.** Laptop with VPN client software
   - **B.** IPsec VPN tunnel between two 802.11 bridges
   - **C.** IPsec VPN tunnel between two WLAN controllers
   - **D.** Remote AP
2. Which of the following settings would John need to configure on his client to establish an L2TP VPN? (Choose all that apply.)
   - **A.** IP address of VPN server
   - **B.** VPN type
   - **C.** Shared secret key
   - **D.** Username
   - **E.** Password
3. When Ben travels for business, he often connects to hotspots for Internet access. During his travels, which is the most common encryption that is provided by the hotspot?
   - **A.** WEP
   - **B.** IPsec
   - **C.** AES
   - **D.** 3DES
   - **E.** None
4. When Amelia received her RAP from the IT department, what settings did they configure on it?
   - **A.** SSID, channel, and power
   - **B.** Local IP Address, Mask, and Gateway
   - **C.** VPN Client Settings
   - **D.** Client authentication and encryption security
   - **E.** None of the above
5. Which of the following is true regarding a remote access point? (Choose all that apply.)
   - **A.** It provides VPN connectivity to the controller.
   - **B.** It functions as an access point.
   - **C.** The controller will download the AP settings to it.
   - **D.** It can support 802.1X/EAP clients.
   - **E.** It can support captive portal clients.

6. When Irene is traveling and connecting to her remote AP, all of her data is first sent to the corporate controller and then forwarded to the corporate network or out to an Internet gateway. The remote AP is configured using which mode?
   - **A.** Bridging
   - **B.** Routing
   - **C.** Gateway
   - **D.** Tunneling
   - **E.** Split tunneling

7. T.J. has a remote AP that is advertising both an Employee SSID and a Guest SSID. When the guest users connect to the RAP, their data is routed directly to an Internet gateway. To provide this functionality for the Guest SSID, the remote AP is configured using which mode?
   - **A.** Bridging
   - **B.** Routing
   - **C.** Gateway
   - **D.** Tunneling
   - **E.** Split tunneling

8. When Lucas is connected to the corporate SSID using his remote AP, data that is destined for the Internet is sent directly to an Internet gateway, but any data that is destined for the corporate network is carried over the VPN back to the corporate network. The remote AP is configured using which mode?
   - **A.** Bridging
   - **B.** Routing
   - **C.** Gateway
   - **D.** Tunneling
   - **E.** Split tunneling

9. A captive portal is essentially a combination of which of the following? (Choose all that apply.)
   - **A.** Firewall
   - **B.** Wireless AP
   - **C.** Authentication server
   - **D.** Authenticator
   - **E.** Authentication web page

10. Which of the following are typically affiliated with a captive portal? (Choose all that apply.)
    A. HTTPS
    B. Username
    C. Password
    D. Authentication
    E. Encryption

11. It was once common for companies to use VPNs or client-based WLAN security in the enterprise. Which technology is now recommended for client-based WLAN security?
    A. WEP
    B. 802.3af
    C. WPA/WPA2
    D. RAP

12. Which of these solutions are examples of a client-server VPN solution in use? (Choose all that apply.)
    A. Laptop with VPN client software
    B. IPsec VPN tunnel between two 802.11 bridges
    C. IPsec VPN tunnel between two WLAN controllers
    D. Remote AP

13. Remote APs can be configured in which of the following modes? (Choose all that apply.)
    A. Bridging
    B. Routing
    C. Gateway
    D. Tunneling
    E. Split tunneling

14. Elizabeth wants to ensure that all user traffic traverses the corporate network where it is analyzed for viruses. To achieve this, the RAP needs to be configured for which mode?
    A. Bridging
    B. Routing
    C. Gateway
    D. Tunneling
    E. Split tunneling

15. A captive portal can control access to which of the following networks?

- **A.** Wired Ethernet
- **B.** 802.11 wireless
- **C.** Cellular data network
- **D.** Fiber-optic network
- **E.** All of the above

16. Which of the following are common VPN protocols? (Choose all that apply.)

- **A.** PPP
- **B.** PPTP
- **C.** L2TP
- **D.** IPsec
- **E.** 802.11i

17. Which of the following statements can be true for captive portals? (Choose all that apply.)

- **A.** They authenticate the user.
- **B.** They always require a password.
- **C.** The user data is not encrypted.
- **D.** The user can be authenticated using a RADIUS server.
- **E.** They always require a username.

18. What is the easiest and best way of securing your data on a public network?

- **A.** WEP
- **B.** WPA2-PSK
- **C.** 802.1X/EAP
- **D.** Open SSID
- **E.** VPN
- **F.** Captive portal

19. Which of the following security features are often implemented to provide guest access? (Choose all that apply.)

- **A.** RADIUS authentication
- **B.** VLAN segmentation
- **C.** SSID segmentation
- **D.** Encryption
- **E.** Captive portal

20. What features and benefits are provided by a RAP? (Choose all that apply.)

- **A.** The VPN configuration is configured on the device and does not require the end-user to enter any information such as username and password.
- **B.** When the RAP has established the VPN, the controller can push changes to the RAP.
- **C.** The RAP can be configured individually.
- **D.** The RAP can be configured as part of a group of APs.
- **E.** The RAP can provide the same services as a local AP.

Answers to Review Questions

1. B, C. For scaling purposes, WLAN controllers are often deployed at corporate headquarters as well as at branch offices. Any data communications across the Internet between WLAN controllers should be protected with a site-to-site VPN. A site-to-site VPN tunnel is also often used to provide encryption of the 802.11 communications between the two WLAN bridges.

2. A, B, C, D, E. When configuring a VPN client, it is necessary to enter the IP address of the VPN server, the VPN type, and the shared secret key. A username and password is also needed to log onto the VPN server.

3. E. Hotspots typically use captive portals to provide authentication, but most do not provide encryption. WEP is a security technology. IPsec, AES, and 3DES are all encryption technologies. At a hotspot, a VPN solution is needed to provide data privacy.

4. C. The RAP is a VPN client device and needs to be programmed with the IP address of the VPN server, the VPN type, and the shared secret key. The Remote AP usually receives its original network information from the local DHCP server. The remote AP receives SSID, channel, and power settings after establishing the VPN tunnel and contacting the WLAN controller. Client authentication and encryption settings are specific to the SSID.

5. A, B, C, D, E. Once the RAP establishes its VPN tunnel back to the controller, it behaves just like any other controller based AP. The controller will download the SSID and radio parameters, which can include 802.1X/EAP and captive portal configurations.

6. D. When a RAP is configured for standard VPN tunneling, all of the data is sent to the controller through the VPN tunnel that is established between the RAP and the controller. Any traffic destined for the Internet must go through the VPN tunnel and use the Internet gateway at corporate headquarters.

7. A. The bridging mode remote AP solution typically has two separate SSIDs. One enterprise SSID routes traffic through the VPN tunnel and a second, locally bridged SSID provides a route to the Internet gateway.

8. E. A remote AP that uses a split tunnel only needs one SSID for wireless user connectivity. The split-tunnel can provide access either to the Internet gateway or back through the VPN tunnel with the single SSID. Depending on the destination of the traffic, some of the data is tunneled back to the enterprise WLAN controller and some of the data is routed to a gateway to the Internet.

9. A, E. A captive portal first prevents access to the network by blocking any unauthorized users. The captive portal will present an authentication web page to the user, and once the user has authenticated, the user will be granted access to the network.

10. A, B, C, D. Captive portals do not typically encrypt the data. The main purpose of a captive portal is to authenticate the user. Since a username and password exchange is required, HTTPS is usually used to secure the exchange.

11. C. Because WPA/WPA2 solutions can now provide Layer 2 encryption using either TKIP or CCMP, using VPNs for client-based WLAN security is no longer necessary or recommended in the enterprise.

12. A, D. Remote APs use VPNs to establish client-to-server connections from the RAP to a corporate VPN server that normally resides within the WLAN controller. Client-side VPNs are still considered mandatory when users access a public access WLAN or hotspot.

13. A, D, E. The three modes that are supported by remote APs are tunneling, bridging, and split tunneling.

14. D. When configured for tunneling, all RAP traffic is sent to the controller where it is then placed on the corporate network or forwarded back out to the Internet.

15. E. A captive portal can provide access to any Layer 2 network technology since it is a Layer 3 authentication technology.

16. B, C, D. The Point-to-Point Tunneling Protocol, Layer 2 Tunneling Protocol, and IP Security Protocol are often used to secure VPN communications. Most WLAN enterprise solutions use IPsec with L2TP.

17. A, C, D. A captive portal can be used to authenticate a user. They do not always require a username or password. Although it is not common or likely, the captive portal SSID can be encrypted with WEP, WPA-PSK, or WPA2-PSK. Depending on the vendor, the captive portal can authenticate against different servers, including a RADIUS server.

18. E. When connected to a public network, you do not have the ability to determine or change the settings on the AP, so WEP, WPA2-PSK, 802.1X/EAP, or captive portal would already be configured. WEP, WPA2-PSK, and 802.1X/EAP are not commonly used on a public network. Captive portal is typically used; however, it does not provide security. VPN is the only security method that you have control over.

19. A, B, C, E. When configuring guest access, it is common to use a captive portal with authentication to a RADIUS server. A separate SSID is typically created, with all the guest traffic being placed on a separate guest VLAN. Encryption is not typically implemented because it is more difficult for the guests to configure.

20. A, B, C, D, E. When installing a RAP, the end-user only needs to connect the RAP to a network that has Internet access, requiring no user interaction. When the RAP has connected to the wireless controller, changes can be made and downloaded to the RAP. The RAP can be managed individually or as part of a group, providing flexibility along with ease of management. The RAP is an AP connected to the controller through a VPN tunnel.

Chapter 12

WLAN Security Infrastructure

IN THIS CHAPTER, YOU WILL LEARN ABOUT THE FOLLOWING:

- ✓ **Overview of WLAN architectures and capabilities**
  - Integration service (IS)
  - Distribution system (DS)
  - Autonomous APs
  - WLAN controllers
  - Split MAC
  - Mesh
  - WLAN bridging
  - Cooperative control
  - Dynamic frequency selection
  - Dynamic RF
  - Location based access control
  - Hot standby/failover
- ✓ **Device management**
  - Protocols for management
  - CAPWAP and LWAPP
  - Wireless network management systems

- ✓ **RADIUS/LDAP servers**
  - Proxy services
  - Features and components
  - Integration
  - EAP type selection
  - Deployment architectures and scaling
  - RADIUS failover
  - Timer values
  - WAN traversal
  - Multi-factor authentication servers
- ✓ **Public Key Infrastructure**
- ✓ **Role-based access control**
- ✓ **Enterprise encryption gateways**

This chapter provides an overview of the many different WLAN architectures that are available today. In previous chapters, we discussed the authentication and encryption technologies used to provide 802.11 security. This chapter will discuss how the WLAN infrastructure, such as RADIUS, PKI, firewalls, ACLs, and other components, factor into WLAN security.

WLAN Architecture Capabilities Overview

WLANs today come in many different forms. The trend for the past several years has been focused on WLAN controller-based architectures, but it hasn't taken off in all environments and deployment scenarios. WLANs are deployed as mesh networks, as bridges used to enable wired-only machines wirelessly, as point-to-point units used as backhaul connections, and even more recently as remote site/office extension APs for small sites and telecommuters. There is even a new type of architecture gaining steam that is a hybrid approach to split-MAC and autonomous architectures.

IEEE 802.11 adoption has been on a rapid growth curve and is still experiencing phenomenal growth. Laptops are still replacing wired desktops. Office environments are being deployed with Wi-Fi as their primary access layer technology and are cutting back on switch ports. More and more new devices are emerging as Wi-Fi enabled, and, to the amazement of many, include cellular phones. Traditional PBX systems are being thrown out and replaced with small (in comparison), rack-mounted servers that service entire facilities full of Wi-Fi -based phones.

Combined with the fact that 802.11 technology is still relatively new, all these factors have contributed to incredible innovation and competing WLAN architecture developments that address various market verticals and customer operational models.

As speeds are increasing beyond 100 Mbps, introduced with 802.11n, wired Ethernet is having a hard time competing for budget dollars in comparison to the benefit of being mobile. For many, it is an elated feeling similar to cutting the leash and finally running free and working wherever you want. User expectations for a wireless network mirror the expectations of reliability of a wired connection along with the need to be secure at the same time.

Integration Service (IS)

The 802.11-2007 standard defines an *integration service (IS)* that enables delivery of MSDUs between the distribution system (DS) and a non-IEEE-802.11 LAN, via a portal. A simpler way of defining the integration service is to characterize it as a frame format

transfer method. The portal is usually either an access point or a WLAN controller. As mentioned earlier, the payload of a wireless 802.11 data frame is the layer 3–7 information known as the MSDU. The eventual destination of this payload is usually to a wired network infrastructure. Because the wired infrastructure is a different physical medium, an 802.11 data frame payload must be effectively transferred into an 802.3 Ethernet frame. For example, a VoWiFi phone sends an 802.11 data frame to an autonomous access point. The MSDU payload of the frame is a VoIP packet with a final destination of a VoIP server that resides at the 802.3 network core. The job of the integration service is to remove the 802.11 header and trailer and then encase the MSDU VoIP payload inside an 802.3 frame. The 802.3 frame is then sent on to the Ethernet network. The integration service performs the same actions in reverse when an 802.3 frame payload must be transferred into an 802.11 frame that is eventually transmitted by the access point radio.

It is beyond the scope of the 802.11-2007 standard to define how the integration service operates. Normally, the integration service transfers data frame payloads between an 802.11 and 802.3 medium. However, the integration service could transfer an MSDU between the 802.11 medium and some sort of other medium such as an 802.5 token ring. The integration service mechanism happens at the edge when autonomous APs are deployed. The integration service mechanism normally takes place inside a WLAN controller when lightweight APs are deployed.

Distribution System (DS)

The 802.11-2007 standard also defines a *distribution system (DS)* that is used to interconnect a set of basic service sets (BSSs) via integrated LANs to create an extended service set (ESS). Service sets are described in detail later in this chapter. Access points by their very nature are portal devices. Wireless traffic can be destined back onto the wireless medium or forwarded to the integration service. The DS consists of two main components:

Distribution System Medium (DSM) A logical physical medium used to connect access points is known as a *distribution system medium (DSM)*. The most common example is an 802.3 medium.

Distribution System Services (DSS) System services built inside an access point or WLAN controller usually in the form of software. The *distribution system services (DSS)* provide switchlike intelligence. These software services are used to manage client station associations, reassociations, and disassociations. Distribution system services also use the layer 2 addressing of the 802.11 MAC header to eventually forward the layer 3–7 information (MSDU) either to the integration service or to another wireless client station.

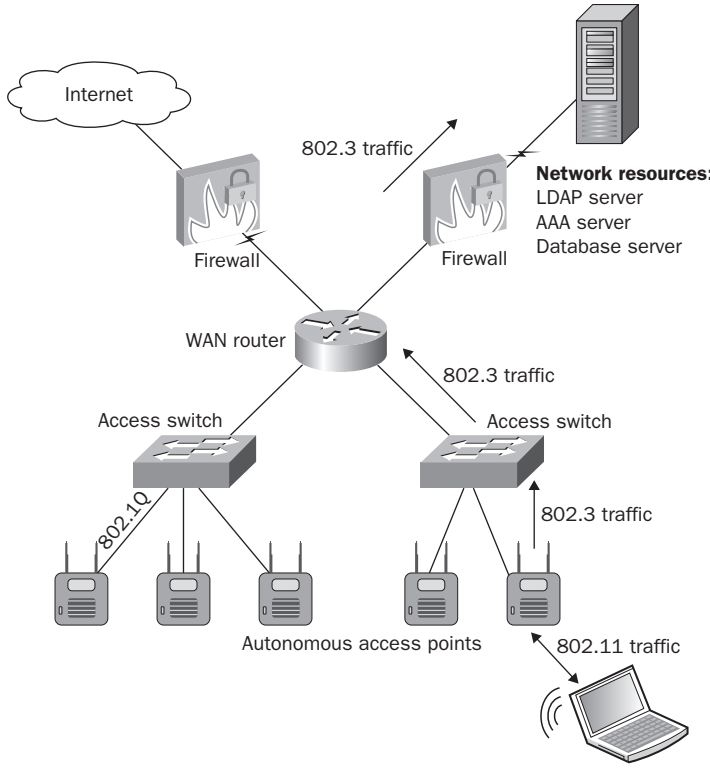
Autonomous APs

For many years, the conventional access point has been thought of as a portal device where all the "brains" and horsepower exist inside the access point (AP) on the edge of the network architecture. Because all the intelligence exists inside each individual access point, these APs are often referred to as *fat APs*, *standalone APs*, or *intelligent edge APs*. However, the most common industry term for the traditional access point is *autonomous AP*.

The 802.11-2007 standard defines operations starting with OSI Layer 1, the Physical layer, and ending with OSI Layer 2, the MAC sublayer of the DataLink layer. In an autonomous AP, all MAC-layer functionality is fully implemented into each autonomous AP—hence its name. It's not until we get into controller-based architectures that we start to split out the MAC-layer functionality between the AP and the WLAN controller. Therefore, in autonomous APs, all the functions specified in the IEEE 802.11-2007 standard are implemented locally on each autonomous AP, which includes encryption, decryption, 802.1X authenticator functionality, distribution system (DS) and integration service (IS) features, and more. All configuration settings exist in the autonomous access point itself, and therefore, management and configuration occurs at the access layer.

As shown in Figure 12.1, autonomous APs were deployed at the access layer and typically are powered by a Power-Over-Ethernet (PoE)-capable access layer switch. The integration service within an autonomous AP translates the 802.11 traffic into 802.3 traffic. Any traffic that originates from the WLAN was often segmented by a firewall that sat between the autonomous APs and network resources.

FIGURE 12.1 Autonomous access points



An autonomous AP is now being referred to in IETF RFC documents as *local-MAC AP*. Autonomous APs are the most traditional type of APs used since the inception of IEEE 802.11, including the prestandard devices. In a traditional autonomous model, each operated independently with little or no collaboration between adjacent autonomous APs.

Configuration and management of enterprise deployments with large autonomous AP populations is not an easy task. Using individual devices that are configured separately becomes quite an operational challenge without a sophisticated network management system in place. A wireless network management system (WNMS) has always been a bolt-on solution for autonomous APs regardless of whether the WNMS is from the same manufacturer or a third party.

An autonomous AP is essentially a bridge device from a wireless 802.11 medium to some other distribution system (DS) medium such as 802.3 Ethernet. It frankly doesn't matter what the DS architecture is, and it might even include 802.11 wireless DS, cellular, and more.

Wireless applications are becoming more demanding as user adoption and user expectation is increasing. That means that wireless devices need to do more, which may even include implementing a variety of application features or features of the DS system (which is typically an Ethernet network carrying IP traffic). Because of this, 802.1Q VLAN tagging; QoS features at both Layer 2 and Layer 3; PoE/802.3-2005 clause 33 (formerly 802.3af); its successor, 802.3at; embedded ACLs; and firewalls are all typically implemented in autonomous APs.

WLAN Controllers

As enterprise WLAN deployments began to grow larger in size, so did the administrative burden of managing and configuring individual autonomous APs. Therefore most vendors have moved to a more centralized WLAN architecture. This model uses a central WLAN controller that usually resides in the core of the network. In the centralized WLAN architecture, autonomous APs have been replaced with controller-based access points also known as thin APs. A *controller-based AP* has minimal intelligence, and functionally is just a radio card and an antenna. All the intelligence resides in a centralized *WLAN controller*, and all the AP configuration settings, such as channel and power, are distributed to the controller-based APs from the WLAN controller and stored in the RAM of the controller-based AP. The encryption and decryption capabilities might reside in the centralized WLAN controller or may still be handled by the controller-based APs, depending on the vendor. The distribution system service (DSS) and integration service (IS) that formally resided in an autonomous AP now resides in the centralized WLAN controller.

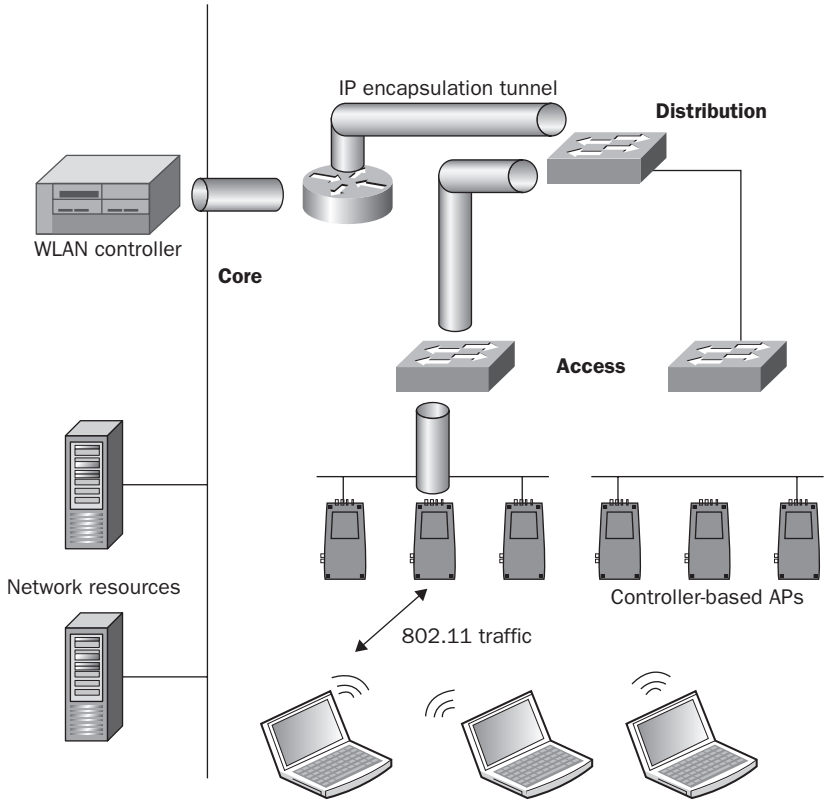
The controller is where all configuration changes are performed and the APs are merely extensions of this single focal point. Some of the 802.11-based (MAC-layer) functions were removed from the APs and placed on the controller. Some of these varied by vendor, but because other functions that were previously performed by an autonomous AP were removed, they were considered "lighter" and hence the name "lightweight APs or "thin APs." The CWNP program and this book use the term *controller-based access point*. The

CAPWAP specification (covered later in this chapter) refers to controller-based AP as a wireless termination point (WTP).

Controller-based APs, once powered on, phone home like E.T. to find a WLAN controller with which to form a bond. Once a controller-based AP contacts a WLAN controller, if out of sync, the AP will download the firmware matching the version of code the WLAN controller is running and also the AP's configuration template. Many WLAN vendors use proprietary protocols that can transfer configuration settings, update firmware, and maintain keep-alive traffic between the WLAN controller and the controller-based AP. The protocol may be a standalone management protocol used to administer the APs, or it may also be a protocol that is used for IP encapsulation of any 802.11 traffic.

Depending on the vendor, controller-based APs create an IP encapsulation tunnel back to the WLAN controller using protocols such as GRE, LWAPP, or CAPWAP. A key feature of most WLAN controllers is that the integration service (IS) and distribution system service (DSS) normally operate within the WLAN controller. In other words, all 802.11 traffic that is destined for wired-side network resources must first pass through the controller and be translated into 802.3 traffic by the integration service before being sent to the final wired destination. Therefore, as shown in Figure 12.2 controller-based access points must send their 802.11 frames to the WLAN controller over an 802.3 wired connection.

FIGURE 12.2 IP tunneling



The 802.11 frame format is complex and is designed for a wireless and not a wired medium. An 802.11 frame cannot travel through an Ethernet 802.3 network by itself. So how can an 802.11 frame traverse between a controller-based AP and a WLAN controller? The answer is inside an IP-encapsulated tunnel. Each 802.11 frame is encapsulated entirely within the body of an IP packet. Many WLAN vendors use *Generic Routing Encapsulation (GRE)*, which is a standards-based network tunneling protocol. WLAN vendors that do not use GRE may use other proprietary protocols for the IP tunneling.

GRE can encapsulate an entire 802.11 frame inside an IP tunnel, creating a virtual point-to-point link between the controller-based AP and the WLAN controller. GRE is only used for encapsulation of 802.11 traffic and is not used for management communications between the WLAN controller and the AP. For example, a separate management protocol would be needed for a WLAN controller to tell an AP to change operational parameters such as channel and power settings. However, some protocols such as LWAPP and CAPWAP can be used for encapsulation and management. LWAPP and CAPWAP are protocols used to encapsulate 802.11 traffic and can also be used by the WLAN controller can use to push configuration settings to the controller-based APs.

Tunneling enables several network benefits, such as a common ingress and egress point for all network traffic, along with VLAN abstraction, because regardless of which VLAN the actual controller-based access point resides on, the traffic can exit the controller on whichever VLAN the SSID designates. No longer is there a need for distributed ACLs or other mechanisms across the entire LAN switching and router fabric where a single form of traffic filtering can be done at the controller's edge. DHCP and ARP traffic can be inspected and controlled from the WLAN controller since all traffic from clients is entering the network from one common location.

Functions such as the 802.1X *authenticator* role reside at the controller, which helps limit the amount of overhead involved in 802.1X reauthentications to new APs. Clients can be more easily tracked by knowing where they roamed and from where they just left. Statistics can be gathered from the first association to a controller-based AP to the current time because the client is associated to the same WLAN system.

WLAN controller solutions didn't solve all our WLAN headaches. Rather, it created some new ones. The main complexities manifested in the form of multicast and QoS. As if multicast engineering wasn't tricky enough, it even got worse with WLAN controllers as clients moved between controllers and controller-based APs across LAN switches and controller-based APs on different VLANs. The same goes for QoS in that end-to-end marking became even more difficult because there was no longer a single mapping between the AP and the next hop switch port. The IP encapsulation tunnel now needs to be factored into the network packetization, and there are cases where Layer 2–based 802.1Q priority bits (or legacy 802.1p) are lost in the process, thus forcing QoS to rely almost exclusively on Layer 3 markings. That means that only Layer 3–capable switches must be deployed in some environments, or QoS is nonexistent between those Ethernet hops.

Another issue involves Ethernet traffic traversal between wireless clients and their destination. There is a new word that seems to have entered the Wi-Fi dictionary called *tromboning*. As air passes through the trombone musical instrument, it travels a long distance before it finally exits the end of the instrument. WLAN controllers are typically

placed at the core of a wired network and the controller-based APs are placed at the access layer. In rare cases, the AP may even reside across a WAN link. Consider the case when a wireless STA is talking to another STA that is associated with the same AP or even the same access layer switch connected to an adjacent AP in another part of the coverage area. Each and every 802.11 frame is encapsulated in an IP packet and sent all the way back to the WLAN controller, where it is then sent along to its destination. Although this feature may simplify the network design at one level, it serves to increase not only latency but also network design complexity in other areas such as multicast and QoS, as mentioned earlier.

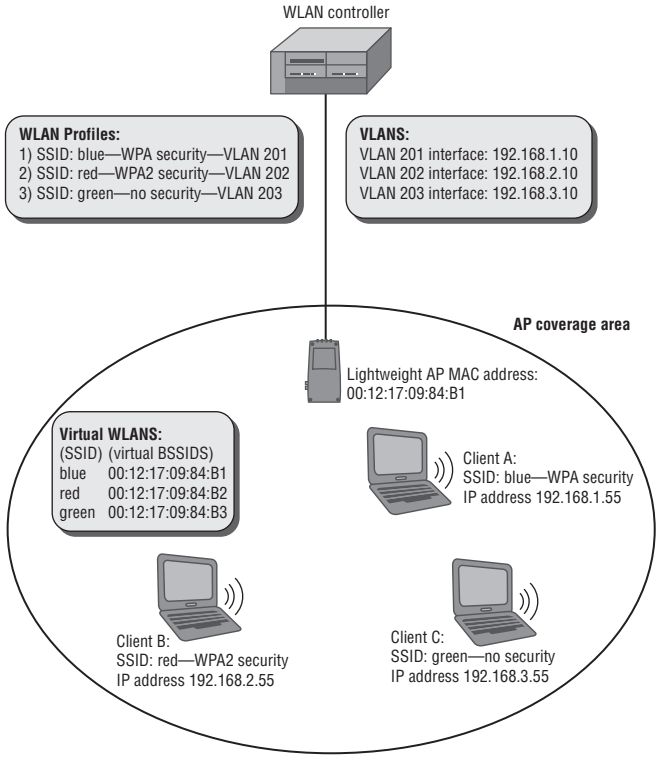
WLAN controllers are often referred to as *wireless switches* because they are indeed an Ethernet-managed switch that can process and route data at the Data-Link layer (Layer 2) of the OSI model. Many of the WLAN controllers are multilayer switches that can also route traffic at the Network layer (Layer 3). However, the phrase *wireless switch* does not adequately describe the many capabilities of a WLAN controller. With that in mind, WLAN controllers do fully support the creation of VLANs and 802.1Q VLAN tagging. Multiple wireless user VLANs can be created on the WLAN controller. The ability to create user VLANs is one of the main benefits of a WLAN controller, because they can provide for segmentation and security. VLANs may be assigned statically to WLAN profiles or may be assigned using RADIUS attributes. Some WLAN controllers may also offer some basic routing capabilities.

WLAN controllers also support virtual WLANs, which are often called *WLAN profiles*. Different groups of 802.11 clients exist in a virtual WLAN within the same physical contention domain. The WLAN profile is a set of configuration parameters that are configured on the WLAN controller. As shown in Figure 12.3, the WLAN profile parameters can include the WLAN logical name (SSID), WLAN security settings, user VLAN assignment, and QoS parameters. WLAN profiles often work together with role-based access control (RBAC) mechanisms. When a user connects to a virtual WLAN, users are assigned to specific roles.

FIGURE 12.3 WLAN profile

Every WLAN has a logical name (SSID), and each WLAN BSS has a unique Layer 2 identifier, the *basic service set identifier (BSSID)*. The BSSID is typically the MAC address of the access point's radio card. WLAN controllers have the capability of creating multiple virtual BSSIDs. As you just learned, the WLAN controller allows for the creation of virtual WLANs, each with a unique logical identifier (SSID) that is also assigned to a specific virtual local area network (VLAN). Because the BSSID is the MAC address of the AP, and because the WLAN controller can support many virtual WLANs on the same physical AP, each virtual WLAN is typically linked with a unique *virtual BSSID*. As shown in Figure 12.4, the virtual BSSIDs are usually increments of the original MAC address of the lightweight AP's radio. As you can see in Figure 12.4, within each controller-based AP's coverage area, multiple virtual WLANs can exist. Each virtual WLAN has a logical name (SSID) and a unique virtual Layer 2 identifier (BSSID), and each WLAN is mapped to a unique Layer 3 VLAN. In other words, multiple Layer 2/3 domains can exist within one Layer 1 contention domain. Try to envision multiple basic service sets (BSSs) that are linked to multiple-user VLANs yet all exist within the same coverage area of a single access point.

FIGURE 12.4 Virtual WLANs, virtual BSSIDs, and VLANs



Split MAC

The majority of WLAN controller vendors implement what is known as a *split MAC architecture*. With this type of WLAN architecture, some of the MAC services are handled by the WLAN controller, and some are handled by the controller-based access point.

You have already learned that 802.11 frames are tunneled between the controller-based APs and the WLAN controller. 802.11 data frames will almost always be tunneled to the controller because the controller's integration service transfers the Layer 3–7 MSDU payload of the 802.11 data frames into 802.3 frames that are sent off to network resources. Effectively, the WLAN controller is needed to provide a gateway to network resources for the payload of 802.11 data frames. 802.11 management and control frames do not have an upper-layer payload and therefore are never translated into 802.3 frames.

802.11 management and control frames do not necessarily need to be tunneled to the WLAN controller because the controller does not have to provide a gateway to network resources for these types of 802.11 frames. In a split-MAC architecture, many of the 802.11 management and control frame exchanges occur only between the client station and the controller-based access point and are not tunneled back to the WLAN controller. For example, beacons, probe responses, and ACKs may be generated by the lightweight AP instead of the controller. Note that most WLAN controller vendors implement split MAC architectures differently. The Internet Engineering Task Force (IETF) has proposed a set of standards for WLAN controller protocols called *Control and Provisioning of Wireless Access Points (CAPWAP)*. CAPWAP does define split MAC standards.

Mesh

Backhaul connections for APs can be expensive and an engineering burden more so in some environments than others. Outdoor and temporary network deployments not requiring peak AP network capacity or latency are huge beneficiaries of mesh technology.

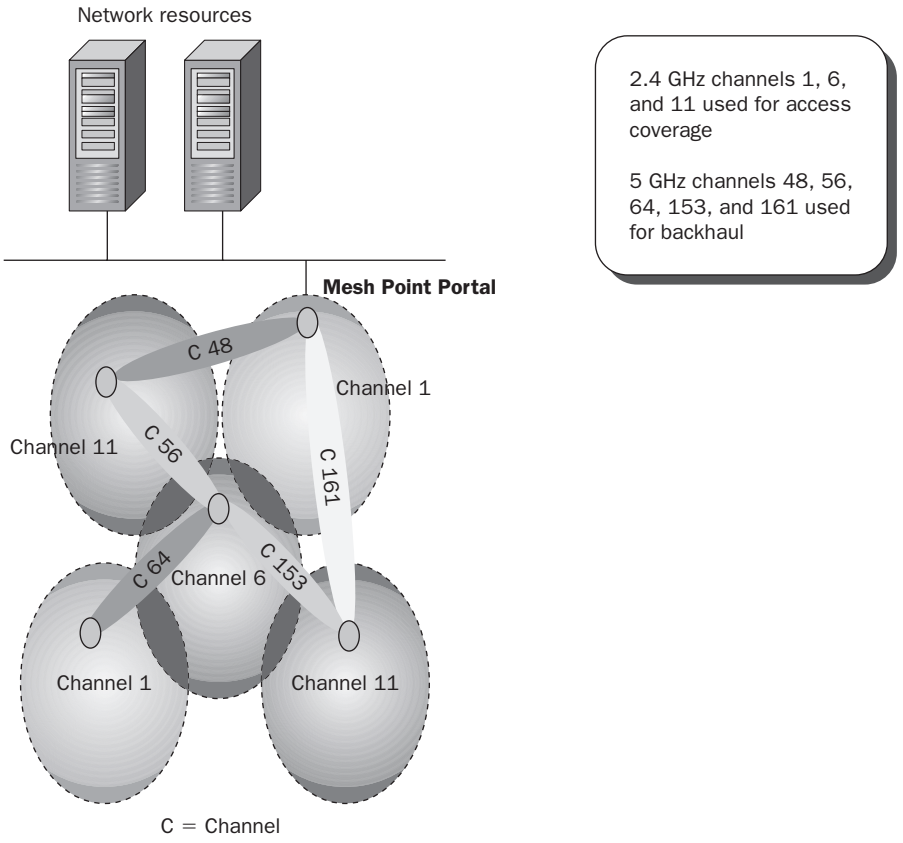
Although not all mesh networks are created equal, the basic concept is that a root AP, known as a *mesh point portal (MPP),* would have a connection to the wired network and an additional node AP, known as a mesh point (MP), which can form a repeater relationship with the mesh point portal to expand the RF coverage area of the network.

Other opportunities existed with mesh networks whereby backhaul redundancy could be possible. For example, if multiple MPPs existed and one of the backhaul connections went down, the network could readjust and forward traffic out of the still operating MPPs, similar in concept to that of routed IP networks.

Wireless mesh APs communicate with each other by using proprietary Layer 2 routing protocols, creating a self-forming and self-healing wireless infrastructure (a mesh) over which edge devices can communicate, as shown in Figure 12.5. A self-forming WLAN mesh network automatically connects access points upon installation and dynamically updates routes as more clients are added. Because interference may occur, a self-healing WLAN mesh network will automatically reroute data traffic in a Wi-Fi mesh cell.

Proprietary Layer 2 intelligent routing protocols determine the dynamic routes based on measurement of traffic, signal strength, hops, and other parameters.

FIGURE 12.5 Mesh architecture



Although a WLAN mesh network can be a mesh of repeater-like access points that all operate on one frequency, dual-band mesh APs are now much more common. With dual-band WLAN mesh APs, typically the 5 GHz radios are used for the mesh infrastructure and to provide backhaul while the 2.4 GHz radios are used to provide access to the client stations.

Some mesh networks operate over the same radio that is also serving traffic, which means that the usable real bandwidth of a single-radio mesh AP is cut in half to allow for maintenance overhead between mesh neighbors. Adding more single-radio mesh APs as a second, third, and even larger hop neighbor exacerbates the problem. Nodes near the root

mesh node can quickly become congested with network traffic contention from the large amount of mesh neighbors.

Other mesh networks use a dedicated backhaul radio ideally operating in a different RF band, such as 5 GHz, and then use the access radio in 2.4 GHz only. No longer does the access radio have to time-slice with the backhaul connection to the mesh neighbor. The backhaul radio does it all. The root mesh nodes can still quickly become congested, but this issue can often be resolved by limiting the number of hops to the nearest root mesh node to a maximum of three.

Although the 802.11s Task Group is currently working on standardizing WLAN mesh networking, all current vendor solutions are proprietary.

WLAN Bridging

When facilities are separated from each other and no physical network-capable wiring exists between them, wireless bridges are often employed. Monthly-based fees for Telco circuit costs can be mitigated with the one-time cost of a wireless point-to-point (PtP) bridge. Wireless bridges are also used between communication towers and can typically span many miles.

Bridge and backhaul links tend to have very different requirements than do typical AP functions that serve WLAN clients. The first difference is that APs typically serve in the access layer of a network. WLAN bridges operate in the distribution layer and are normally used to connect two or more wired networks together over a wireless link.

One side of the link is usually the *root bridge* and the other side is the *nonroot bridge*. The root bridge establishes the channel and beacons for the nonroot bridge to join. The nonroot bridge will then associate with the root bridge in a station-like fashion to establish the link. A point-to-multipoint (PtMP) bridge link connects multiple wired networks. The root bridge is the central bridge, and multiple nonroot bridges connect back to the root bridge.

Standard encryption protocols need not necessarily be followed if there are only two devices talking in a dedicated link. They can talk any kind of encryption gibberish they want, and often vendors try to distinguish themselves from others by employing a proprietary form of encryption. As you learned in earlier chapters, VPNs are often used for bridge security. An 802.1X/EAP solution can also be used for bridge security, with the root bridge assuming the authenticator role and the nonroot bridges assuming the supplicant role.

Cooperative Control

Over time one thing is for certain with technology; it gets smaller and faster and usually even cheaper. Regarding the size of an AP, a significant amount of computing power can now be yielded than previously possible. This has provided a new architecture opportunity for hardware vendors to resolve some of the challenges of split-MAC architectures while at the same time maintaining the benefits.

Hybrid WLAN architectures make use of the significant computing power available today in the form of an ultra-fat AP known as a *cooperative control access point (CC-AP)*. A CC-AP combines an autonomous access point with a suite of *cooperative control* protocols, without requiring a WLAN controller. These hybrid APs have pulled back a great deal of the 802.11 MAC layer functions and have even added embedded firewalls, RADIUS servers, and other advanced features for each AP. The cooperative control protocols enable multiple CC-APs to be organized into groups that share control information between CC-APs to provide functions such as Layer 2 roaming, Layer 3 roaming, cooperative RF management, security, and mesh networking. The best way to describe a cooperative control architecture is to think of it as an architecture that consists of groups of autonomous access points with WLAN controller intelligence and capabilities.

It has been said by industry insiders that several of the WLAN controller vendors would have taken this architectural approach initially if hardware processing power didn't also come with such a high cost. Therefore, economics played one of the biggest roles in forcing the MAC layer functions into a centralized controller. The same benefits can be achieved by smarter and more powerful APs coordinating among themselves without every single Ethernet frame tromboning all the way back to a controller.

This hybrid architecture still employs a server application that will allow for configuration functions to be coordinated for all the APs, but this server application need not have high-availability requirements. Once the APs download their configuration, they don't require communication to the server application to perform all their core duties. Statistics on clients, interface traffic, monitoring alerts, and other functions can be queued until the server application is restored.

WLAN controller vendors are now offering some features that approach this new architecture. They are offering hybrid APs that can switch traffic locally but still have a high dependency on a WLAN controller. When the WLAN controller is unavailable, some service degradation occurs.

Dynamic Frequency Selection

IEEE 802.11 WLANs are allowed to use the 5 GHz UNII bands, but there may be tenants that don't want to move out. It just so happens that in the 5 GHz UNII-2 and UNII-2E bands a form of radar used for military operations was used that may still be in operation. Therefore, to avoid interference with these systems, the FCC required the IEEE 802.11 working group to standardize a protocol that allows for *dynamic frequency selection (DFS)* in the 5 GHz bands.

802.11h became the protocol that eventually was standardized and has been rolled up into the IEEE Std. 802.11-2007 version. We still refer to it as 802.11h, likely because that was the amendment that made the changes to the 802.11 standard. In this amendment, there is a particular set of sequences that must be followed strictly in order to avoid radar, which includes silencing transmissions, scanning and selecting a new channel, and then eventually resuming normal operations.

Depending on the country of origin, not all of the 5 GHz channels are susceptible to being affected by radar and therefore DFS mechanisms are only mandated for certain 5

GHz channels. For example, in the United States, the FCC mandates the use of DFS in the 13 total channels available in the UNII-2 and UNII-2e frequency bands. The eight channels that reside in the UNII-1 and UNII-3 bands do not require DFS. Therefore, many 5 GHz WLANs are designed with a channel reuse pattern that excludes the DFS channels. From a security perspective, a hacker might create a DoS by manipulating 802.11h mechanisms causing client stations to unnecessarily change channels.

Dynamic RF

Several WLAN vendors saw a market opportunity to distinguish themselves and offer to solve one of the primary complexities of a WLAN deployment—that is, RF. This *black magic*, as the science of RF is sometimes called, was unfortunately understood by far too few designers of WLANs. To add insult to injury, many consultants and site survey companies didn't exactly win the confidence of customers, based on the end result of their WLAN deployments. Manufacturers then mounted their steed and rode into town to save the day.

About the time WLAN controllers started to develop as a new architecture, the concept of a "self-healing" and "self-optimizing" network took off in marketing literature from many vendors. The basic premise of this functionality is for APs to dynamically change channels in order to avoid interference and dynamically adjust power levels to minimize both interference with each other and at the same time ensure adequate coverage.

From a security perspective, a hacker might cause interference in a way that causes an AP to change channels or power, possibly to suboptimal settings.

Location-Based Access Control

Trapeze Networks recently introduced a new feature called *location-based access control (LBAC)*, which can be defined as location-aware security. Location tracking has been taking shape in WLAN design for quite some time now. Trapeze put this concept to work in their client authentication framework. LBAC allows you to prevent users, even valid users, from logging onto the WLAN from specified physical locations.

Wi-Fi networks that incorporate location tracking are constantly attempting to determine the location of wireless devices. Conveniently, when wireless STAs attempt to authenticate to a WLAN, the first thing they typically do is perform an active scan using 802.11 management frame probe requests. Usually, several are sent off for every channel. This allows every AP to hear the wireless STA and determine its approximate location. For companies that are concerned about hackers or wishing to deny access from wireless STAs located outside a specified area, LBAC is a great feature to enhance WLAN network security.

Hot Standby/Failover

From a security perspective, hot standby and failover solutions are important to avoid a denial-of-service that might be caused by a simple network failure. WLAN controllers often implement *Virtual Router Redundancy Protocol (VRRP)* to provide for a standby solution should a WLAN controller fail. APs are not an easy type of device to provide

failover for when external antennas are used. Fortunately, AP failure rates have historically tended to be quite low in normal operating environments.

Several AP vendors have developed software mechanisms in individual APs to maintain a heartbeat connection in a similar fashion to the way failover protocols like VRRP operate. When the heartbeat connection is lost, the standby AP will power up its radios to take over the same geographical coverage area the other AP was servicing.

Hot standby and failover features have been incorporated into controller products since their inception because of their critical role in the base operation of each individual AP. It's important to remember that in WLAN controller solutions, as mentioned earlier in this chapter, each 802.11 data frame essentially terminates at the controller where it is bridged onto the DS, which is typically a wired Ethernet network. Building a WLAN infrastructure with redundant WLAN controllers is highly recommended.

Device Management

Sound network design dictates placing network devices onto dedicated management VLANs or another out-of-band interface from regular network traffic. Enterprise network gear should allow for this functionality in order to keep infrastructure devices inaccessible to hackers or even to employees who are able to gain access to the network.

As the size of WLANs has grown over the years, so have the challenges of managing them. This includes managing the following:

- Firmware revisions
- Configurations and changes
- Monitoring and incident response
- Managing and filtering of device alerts and alarms
- Performance monitoring

Although WLAN controllers have certainly solved a great deal of these problems, not all networks can be converted exclusively to controller-based networks. At the same time, enterprises with a large number of sites still have many WLAN controllers to manage as well.

To make the job of managing these devices easier, standard network protocols for device management are typically included in most WLAN hardware and can be integrated with software-based management systems that can span even the largest of networks. The more a network management system (NMS) or a wireless network management system (WNMS) is incorporated in network designs, the less time is spent performing mundane tasks to support the network. Without exception, every time an NMS or WNMS is properly implemented, user satisfaction with the network is higher, while the cost of operating the network is lower. Equally important is incorporating the deployment of the WNMS into an

operational environment with the support staff. Developing processes and procedures around these systems and making them a part of the support staff's daily work are also critical.

Protocols for Management

There are many different types of protocols used for managing network devices. *Simple Network Management Protocol (SNMP)* has been around for quite some time and has undergone several revisions. In addition to SNMP, most devices can be configured using a command-line interface (CLI) or a graphical user interface (GUI).

The following protocols are common for managing WLANS. Some of these protocols are based upon de jure standards and some are based upon de facto standards. Either way, they provide the basis for WLAN management and administration.

SNMP

Simple Network Management Protocol (SNMP) is an Application layer protocol (OSI Layer 7) used to communicate directly with network devices. SNMP allows for pulling information from devices as well as pushing information to a central SNMP server based on certain, often user-configurable thresholds on network devices. A push from a device might include a message pertaining to an interface reset, a high number of errors, high network or CPU utilization, security alarms, and many other critical factors related to the healthy operations and status of devices.

SNMP is an IETF specification. You can find more information at `www.ietf.org/wg/concluded/snmpv3.html`. Additional information can also be found in RFC 3411 through 3418 for SNMP version 3.

Components

An SNMP management system contains:

- Several (potentially many) nodes, each with an SNMP entity (a.k.a. agent) containing *command responder* and *notification originator* applications, which have access to management instrumentation
- At least one SNMP entity containing command generator and/or notification receiver applications (traditionally called a manager)
- A management protocol used to convey management information between the SNMP entities

Structure of Management Information

Management information is structured as a collection of managed objects contained in a database called a *management information base (MIB)*.

The MIB consists of the following definitions: modules, objects, and traps. Module definitions are used when describing information modules. Object definitions are used when describing the managed objects. Trap definitions are notifications used for unsolicited transmissions of MIB information typically to an NMS.

All SNMP-capable devices have a MIB, and in that MIB should reside the configuration and status of the device. However, vendors aren't usually totally complete with their MIBs and SNMP implementations. Often you will find that certain pieces of critical information are not accessible via SNMP and therefore traps cannot be implemented using that information.

Versions and Differences

SNMP has undergone numerous revisions over the years. This section is not intended to be a complete history of SNMP, but rather an overview to guide you in knowing the differences between the different versions. Additionally, this section will help you properly implement different versions into your network designs by understanding the strengths and how to address the weaknesses.

SNMPv1

Version 1 of SNMP hit the scene in 1988. Like many other initial protocol introductions, SNMPv1 did not get it perfect the first time. SNMPv1 was designed to work over a wide range of protocols in use at the time—including IP, UDP, CLNS, AppleTalk, and IPX—but it is most commonly used with UDP.

SNMPv1 used a *community string*, which had to be known by a remote agent. Since SNMPv1 did not implement any encryption, it was subject to packet sniffing to discover the cleartext community string. Therefore, SNMPv1 was heavily criticized as being insecure. Protocol efficiency was also lacking for this initial protocol introduction. Each MIB object had to be retrieved one by one in an iterative style, which was very inefficient.

SNMPv2

When SNMPv2 was released, several areas of SNMPv1 were addressed, including performance, security, and manager-to-manager communications. Protocol performance became more efficient with the introduction of new functions such as GETBULK, which solved the iterative method of extracting larger amounts of data from MIBs.

Security was improved by the specification of a new party-based security system. Critics accused the party-based system of being too complex and therefore the system was not widely accepted.

SNMPv2c was created next and it is referred to as a *community-based* version, and defined in RFC 1901 through 1908. The community string from SNMPv1 was adopted in SNMPv2c, which essentially dropped any security improvements to the protocol. SNMPv2c does not implement encryption and is subject to packet sniffing of the cleartext community string.

SNMPv3

A great deal of security benefits were added to SNMPv3, including:

- Authentication performed using SHA or MD5.
- Privacy—SNMPv3 uses DES 56-bit encryption based on the CBC-DES (DES-56) standard.
- Access control—Users and groups are used, each with different levels of privileges. Usernames and passwords replace community strings.

Although these features are optional, usually the main driver behind adopting SNMPv3 is to gain these security benefits. It is also optional to have secure authentication but disable encryption.

Even with these features, most network designers still feel it is best to implement the SNMP agents only on secure management interfaces. Specifically, VLAN segmentation and firewall filtering is usually performed on all SNMP traffic to network devices. No sufficiently complex protocol is considered completely secure, and additional safeguards are always highly recommended.

If you intend to implement an NMS or WNMS using SNMP, we highly recommended that you implement SNMPv3. If the management network is highly secure, using older SNMP versions may be acceptable. However, you must consider that older SNMP versions may be deprecated in time. Therefore, it would be wise to implement the latest protocol versions while at the same time gaining the security and performance benefits of the newer protocols.

One of the most important security concerns is most vendor equipment defaults to SNMP being enabled, with default *read* and *write* community strings. This is an *enormous* security threat to the configuration and operation of your network, and should be one of the very first lock-down steps to securing network devices.

CLI-Based Management

Command-line interfaces (CLIs) are one of the most common methods used to configure and manage network devices. It seems the age-old debate of GUI versus CLI is still present to this day, and is not likely to change anytime soon. GUIs do a wonderful job of presenting information, but due to browser incompatibility, JavaScript errors, GUI software bugs, time delays, and more, GUIs still drive many people back to the command line.

CLIs tend to be the raw, unedited configuration of devices and provide the ability to make specific changes quickly to device configurations. Commands issued via a CLI can even be scripted, allowing initial device configuration and even re-configurations to be performed with a simple copy and paste into a CLI session.

CLIs can be accessed using several methods, which are dependent on the device being used. These commonly include the following:

- Serial and console ports
- Telnet
- SSH1/SSH2

Serial and Console Ports

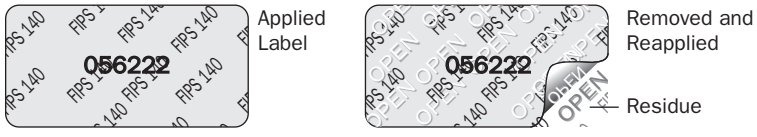
Serial or console port interfaces can vary from manufacturer to manufacturer and even from model to model. This is extremely frustrating to network engineers. Some of them use a standard DB-9 serial connector interface, while others use an RJ-11 or RJ-45 interface. Furthermore, the actual cable might be a proprietary pin-out (namely for the RJ-11 and RJ-45 connectors), a NULL-modem cable, a rollover cable, or a straight-through cable.

Baud rates, number of bits, flow control, parity, and other parameters also vary from device to device.

No matter what type of connector or cable you are using to manage your network device, serial or console ports should be locked down and require a user authentication mechanism. Although typically these can be thwarted by a password-recovery routine using instructions that can be readily found on the Internet, a user authentication mechanism will help deter hackers. Often, a device requires downtime in order to recover the password, and the impact of a service outage may be enough to alert staff of a physical break-in attempt to network devices. It is important to note that most password recovery routines require direct access to the device via the serial or console port. Securing network equipment in a locked data closet or computer room will help to prevent this type of attack from occurring.

Government regulations such as FIPS 140-2 may require that serial and console ports be secured with a tamper-evident label (TEL) to prevent unauthorized physical access to a WLAN infrastructure device such as a WLAN controller. TELs cannot be surreptitiously broken, removed, or reapplied without an obvious change in appearance. As shown in Figure 12.6, each TEL has a unique serial number to prevent replacement with similar labels.

FIGURE 12.6 Tamper-evident label



Telnet

Telnet is another protocol that is commonly used, but often can only be used after a serial port configuration or initial configuration from a factory default state is performed. The IP of the device typically needs to be enabled for it to be accessed and managed via the network interface.

Telnet is heavily criticized and usually prohibited from use by enterprise security policies due to its lack of encryption. Telnet is a completely unencrypted protocol and the payload of each packet can be inspected by packet sniffing. This includes the username and password during the login sequence. We recommend that you disable Telnet after the initial device configuration. Many companies have written policies mandating that Telnet be disabled.

Secure Shell

Secure Shell (SSH), is typically used as the secure alternative to Telnet. SSH implements authentication and encryption using public-key cryptography of all network traffic traversing between the host and user device. The features of Telnet for CLI-based management apply to SSH but include added security benefits. The standard TCP port 22 has been assigned for the SSH protocol. Most WLAN infrastructure devices now support the second version of the SSH protocol called SSH2. As a matter of policy, when

WLAN devices are managed via the CLI, an SSH2 capable terminal emulation program should be used. Figure 12.7 shows the configuration screen of the popular freeware program PuTTY, which supports SSH2.

FIGURE 12.7 PuTTY freeware SSH2 client

HTTPS

Hypertext Transfer Protocol Secure (HTTPS) is a combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encryption and secure identification. HTTPS is essentially an SSL session that uses the HTTP protocol, and is implemented on network devices for management via a graphical user interface (GUI). Not all users prefer CLI-based management methods, and GUIs are commonly used where a WNMS is used to manage WLAN infrastructure.

Because HTTP is transmitted in plaintext, it is susceptible to eavesdropping and man-in-the-middle attacks from modifications in transit. Some devices offer both HTTP and HTTPS, but it is important that minimal authentication be performed via HTTPS. If users of devices will be entered into the GUI, not using HTTPS is purely negligent if the device supports it.

CAPWAP and LWAPP

CAPWAP, as defined in RFC 5415, is a standards-based protocol commonly used for split-MAC architectures for controlling and provisioning of APs. CAPWAP is not restricted just to split-MAC architectures and may also be used in local-MAC mode of operation. However, its original intent is based on creating a standardized, interoperable protocol to enable communication between an *access controller (AC)* and a collection of *wireless termination points (WTPs)*.

When split-MAC architectures were being developed, Airespace proposed the Lightweight Access Point Protocol (LWAPP) as an IETF standard. LWAPP, a method to manage, control, and communicate with APs in a split-MAC architecture, is mostly associated with Airespace/Cisco product lines, since Cisco purchased Airespace.

> The CAPWAP Working Group selected the Lightweight Access Point Protocol (LWAPP) [LWAPP] to be used as the basis of the CAPWAP protocol specification.
>
> *IETF RFC 5415 CLAUSE 1.3*

CAPWAP is designed to be *independent* of OSI Layer 2 (L2) and assumes a network connection consisting of multiple WTPs communicating via the Internet Protocol (IP) to an AC. WTPs are considered a remote radio (RF) interface centrally controlled via an AC. CAPWAP defines either a split-MAC or local-MAC mode of operation.

In split-MAC mode, the distribution and integration services reside on the AC, and therefore all user data is tunneled between the WTP and the AC. However, IEEE 802.11 services, including the beacon frame generation and probe response frame generation are handled on the WTP.

In the local MAC mode, the integration service exists on the WTP, while the distribution service MAY reside on either the WTP or the AC. When it resides on the AC, station-generated frames are not forwarded to the AC in their native format, but encapsulated as 802.3 frames.

One important feature offered with CAPWAP is the optional support of encryption. The LWAPP protocol does not offer encryption and is therefore subject to inspection by sniffing. CAPWAP incorporates *Datagram Transport Layer Security (DTLS),* as defined in RFC 4347, as the security algorithm for the CAPWAP protocol. The concept of using DTLS for the CAPWAP protocol was part of the Secure Light Access Point Protocol (SLAPP) proposal promoted by Aruba Networks and Trapeze Networks. DTLS can be used to encrypt CAPWAP control traffic between a WLAN controller and the APs. DTLS can also be used to secure tunnel communications for data traffic.

Wireless Network Management System

A *wireless network management system (WNMS)* is thought of as a traditional NMS designed for the specific intricacies of wireless systems. The main purpose of a WNMS is to provide a central point of management. Both configuration settings and firmware upgrades can be pushed down to WLAN controllers and autonomous access points. Although centralized management is the main goal, a WNMS has other capabilities as well, such as including RF spectrum planning and management. A WNMS can also be used to monitor the WLAN architecture with alarms and notifications centralized and integrated into a management console. Other capabilities include network reporting, trending, capacity planning, and policy enforcement. A WNMS might also be able to perform some rogue AP detection, but by no means should a WNMS be considered a fully featured wireless intrusion detection system (WIDS).

WNMS products usually consist of a software-based solution that resides on a server-based platform, incorporating a wide range of network management protocols. Because a WNMS may need to work with many different vendor products, it is likely that many versions of management protocols are implemented, although SNMP is most commonly used as the management protocol.

WNMS products can provide a common configuration template that can be applied to different models from the same manufacturer and even different models from different

manufacturers. Configuration elements—such as SSIDs, authentication, encryption, IPs, RF channels, and other functions—are elements common to any AP even though the syntax and the method for configuring these elements may differ.

Although WLAN controllers provide many of the core features a WNMS provides, there are many environments where single autonomous APs still exist in large networks. Moreover, larger networks can be composed of many WLAN controllers, and a WNMS may provide the necessary management functions to monitor, alert, and manage the entire collection of network devices. Figure 12.8 shows the management console of AirWave, a popular WNMS solution that is capable of providing centralized management for WLAN controllers and autonomous APs from many different vendors.

FIGURE 12.8 Wireless network management system console

RADIUS/LDAP Servers

RADIUS was developed back in 1991 as an access server authentication and accounting application. It grew to be widely used by ISPs for dial-up users and later logically extended to VPN dial-up users. RADIUS developed critical mass and had the ability to extend, or rather *broker*, authentication to many different user databases. This includes LDAP, Active Directory, SQL databases, flat files, and native RADIUS users. In fact, multiples of each database type can be used and directed based on a realm attribute that specifies the home system where the user credentials belong.

In a push for IEEE 802.11 security methods to have maximum flexibility for supplicant authentications, RADIUS was a natural choice. In fact, many organizations already were maintaining a RADIUS infrastructure at least for dial-up users with a modem bank. The RADIUS server was typically already configured for authentication to the home-user database the enterprise was using.

What's more, RADIUS incorporates the use of attribute-value pairs (AVPs) that can return additional information in the authentication response to tell the authenticator of special treatment for the supplicant. For example, this might mean the VLAN on which the user should be placed or even the amount of bandwidth that user will be able to consume.

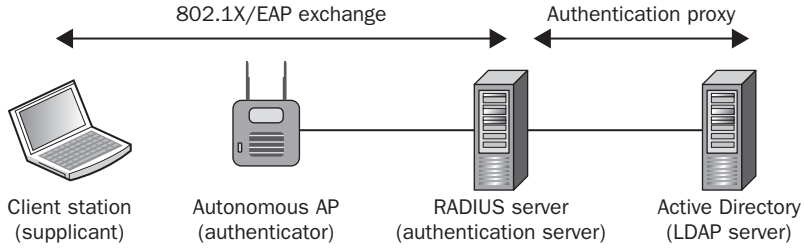
Proxy Services

To proxy an authentication would be to act as a middleman in the authentication transaction. Many authentication severs can be tiered and configured to proxy each other.

In fact, more often than not the authentication server in your WLAN infrastructure APs or WLAN controller configurations do not actually hold the user account credentials for the WLAN supplicant. In the case of EAP-PEAP, EAP-FAST, LEAP, and some others, the actual user credential database is typically Windows Active Directory or an LDAP server. Although the authentication server can maintain a native user database, a RADIUS server will usually proxy with an external user database to authenticate user credentials, as shown in Figure 12.9.

What makes RADIUS so powerful is that it is designed from the ground up to proxy authentications to many different end sources. Although a RADIUS server is most

FIGURE 12.9 Proxy authentication



commonly integrated with Active Directory, integration with Novell's eDirectory is also possible. Many enterprise RADIUS servers even allow an SQL database or flat files to be queried. A RADIUS servers should be able to communicate with any LDAP-compliant database.

Features and Components

As previously stated, RADIUS is a flexible protocol framework largely due to the extensibility of its primary, core components. We'll discuss these main architectural components and features next.

Attribute-Value Pairs

When a RADIUS server provides a successful response to an authentication, the ACCESS-ACCEPT response contains a series of *attribute-value pairs (AVPs)*. RADIUS AVPs are analogous to the concept of variables used in mathematics or software programming. The "attribute" has a name such as Tunnel-Type. There are several standard, reserved attributes, and each value has a unique numeric identifier as well. When a value of an AVP is included in the ACCESS-ACCEPT response, it is done so as a pair.

Vendor-Specific Attributes

Part of the extensibility of RADIUS is the built-in support for adding additional nonreserved AVPs that can be utilized by vendors, called *vendor-specific attributes (VSAs)*. This allows for configuration of these VSAs to be included in the RADIUS database that

would then be included with successful authentications. A standard RADIUS platform can therefore be used for a variety of vendor-specific, and potentially proprietary, features.

Dynamic VLAN Assignment

One of the most popular uses of RADIUS AVPs is in assigning users into VLANs dynamically based on the user's identity. Instead of segmenting users to different WLANs that are mapped to a single user VLAN, all the users can be associated to a single SSID and be dynamically assigned to different VLANs. The main benefit of this solution is that existing ACLs or firewalls between VLANs can be extended to the WLAN clients.

Assuming the AP (or WLAN controller) has access to the VLAN that's assigned, the user will be placed on that VLAN after authentication. As a designer of a network employing this feature, you need to make sure that the AP (or WLAN controller) can actually place the clients into the VLAN that is dynamically assigned. If your network is large and spans many facilities that don't use consistent VLAN numbering, you may want to reconsider dynamically assigning users to VLANs.

Proxy of User Databases

When selecting a RADIUS server, it is important first to consider your user database sources. There may be one or more user databases, and you should confirm support for the exact database technology. For example, if you are an ISP or hotspot provider, the user database may reside in an SQL server, which may limit the available choices of RADIUS server products that are applicable to your design requirements. Support for more than one user database may also be an important criteria for your purchase decision. Usually one database is specified to be the primary over the others and configured in a priority search order.

Real World Scenario

Integrating Different User Databases

Entering the same user information into more than one database is possible. When this occurs, the search order can be paramount. For example, a company has just merged with another. Each division has its own Windows Active Directory domain. In the design of the new network, a single RADIUS server services both sets of users that reside in the two different Active Directory domains.

In Domain 1, a user named John Smith (username: jsmith) exists along with Jane Smith (username: jsmith) in Domain 2. In this case, the first user database in the priority search order would be used for all authentications for the username jsmith. If Jane was in the second domain in the priority search order, her authentication would fail every time because it would not match John Smith's password.

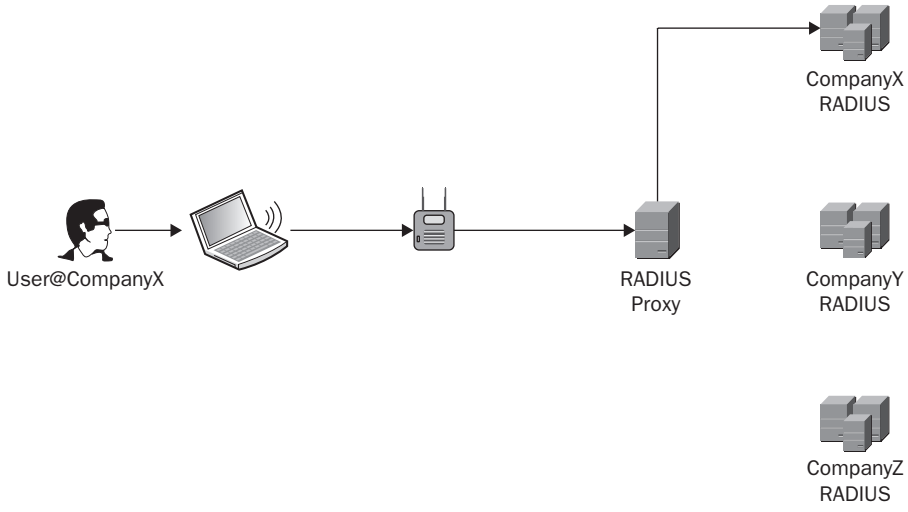
Proxy of a Proxy (Realm)

A RADIUS server can be a proxy to one or more centralized RADIUS servers. As you have already learned, a username can be in the form `DOMAIN/username` or `username@domain`. This is valuable information that can tell the first authentication server which final destination authentication server to request authentication from. In this case, *domain* is synonymous with the term *realm* as referred to previously.

For example, if an AP was configured in a regional office or subsidiary of a large enterprise, the AP might point to an authentication server located at that facility or perhaps in a nearby datacenter. If an employee with a common name, let's say Charles, from the parent company was traveling on a business trip and visiting the subsidiary's office, when Charles logged in with `CWNP/charles`, the authentication would know that it needed to contact the remote CWNP user account database server. In this situation, the first authentication server that the AP pointed to would have just performed a proxy authentication to the final authentication server where Charles's user account resided.

When a domain is used, we commonly refer to this as a *realm-based authentication*. As shown in Figure 12.10, the realm in this case is the domain being sent in the supplicant identity. Authentication of the user is directed to a RADIUS server for CompanyX based on the domain value supplied.

FIGURE 12.10 Realm-based authentication



Integration

RADIUS servers all have their own user databases as well as user grouping features commonly found in many user database systems. User groups may have general security policies defined for them, and when individual user accounts are placed into them,

they inherit the policy of the group. The reality is that most enterprises simply want the ability to authenticate against their existing user databases. Therefore, it is common to find that most enterprises do not use the built-in native user database functions within RADIUS servers. Depending on what user database technology an organization is already using, RADIUS would be used to interface to these systems.

LDAP

Lightweight Directory Access Protocol (LDAP) is an application protocol providing directory services detailed in RFC 4510. WLAN infrastructure from some manufacturers can integrate directly to LDAP systems in lieu of sending each supplicant authentication request to a RADIUS server. If a RADIUS server was still used, a RADIUS server could authenticate requests to an LDAP database.

LDAP databases can contain a wealth of information and can be configured with many attributes. For example, a user can be placed into one or more LDAP groups, thus inheriting the rights and privileges of each group to which the user belongs.

Active Directory

Microsoft introduced Active Directory with Windows Server 2000 and has continued to enhance it with subsequent releases of its server OS platforms. Active Directory is a hierarchical directory service that is based on LDAP. Active Directory also incorporates a DNS-naming component based on the Internet DNS structure. Security is considered very strong with recent offerings of Active Directory from its use of Kerberos.

Windows Active Directory has become popular in enterprise networks due to the popularity of Microsoft Windows at both the client and the server level. By far, most enterprises use Windows Server platforms as their network operating system, and Active Directory is the main component of that framework.

Active Directory provides a vast amount of capability for organizing and centralizing information and designing relationships for computers, users, printers, groups, security policies, and more. Because of this popularity, we have seen enterprise devices such as Cisco IOS routers, Novell NDS and NIS+, and all the major enterprise RADIUS platforms natively support Windows Active Directory.

SQL Databases

RADIUS servers allow integration with a variety of structured query language (SQL) database technologies. The interface is usually via an Open Database Connectivity (ODBC) or Java Database Connectivity (JDBC) interface in the same fashion that is done with any interface of this type.

EAP Type Selection

When 802.1X is configured on an AP or WLAN controller (authenticator), no configuration is possible to specify which EAP type is allowed or restricted. The

authenticator plays absolutely no role in the selection or restriction of the actual EAP type used. When 802.1X is configured on an authenticator, simply enabling this at the SSID level and pointing it to the IP and UDP port of the RADIUS server is all that is essentially needed for the authenticator's configuration. 802.1X/EAP type configuration is performed at the supplicant and authentication server. The authenticator is EAP agnostic.

First, the RADIUS server configuration will specify the EAP types that will be globally allowed, which in turn affects all 802.1X/EAP authentications. Selecting two strong EAP types and one horribly insecure EAP type leaves the door wide open for hackers. If an intruder was attempting to enter your house and the front door was made of one-foot-thick steel but the back door was simply a screen door with a simple hook latch, the intruder would be able to get in your house. This example is analogous to allowing weak EAP types on a WLAN authentication server.

WLAN supplicants negotiate the EAP type with the RADIUS server when the EAP transaction begins. If the RADIUS server proposes an EAP type not allowed on the client, the client is required to respond with an EAP-NAK frame telling the RADIUS server that the EAP type presented is not supported. Once that is performed, as long as the RADIUS server supports more than one EAP type, the RADIUS server will suggest another.

Deployment Architectures and Scaling

When deploying RADIUS servers, put careful thought into the architectural deployment model based on the number of sites, number of devices, and network delays that will affect authentication performance and local security policies. As with any type of network design, scaling and redundancy are important considerations when deploying RADIUS servers.

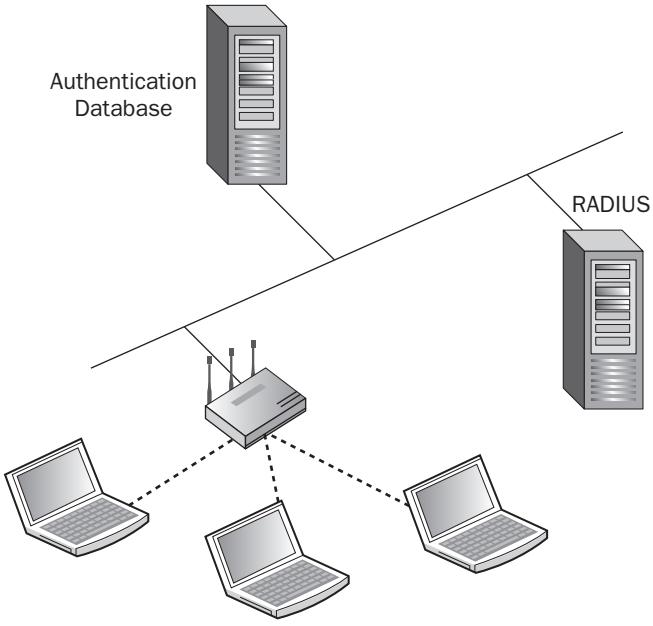
Single-Site Deployment

A single-site deployment is the simplest of all models. If your entire organization resides at a single location and is the hub of all communications, only a single RADIUS server or cluster of redundant servers is needed. Figure 12.11 depicts a single-site RADIUS deployment. Single-site deployments should be considered when:

- All WLAN users are located at a single site.
- A central authentication database handles all user authentication.
- One or more RADIUS servers proxy to the on-site authentication database. The RADIUS server manages WLAN authenticating users, and setting up secure WLAN connections.

The benefits of a single-site deployment is that the RADIUS server can proxy authentications against any type of back-end authentication database including NDS, Active Directory, LDAP, one-time passwords (OTP), and others. Some of the other deployment architectures may not be best suited for certain kinds of databases such as OTP.

FIGURE 12.11 Single-site deployment



Distributed Autonomous Sites

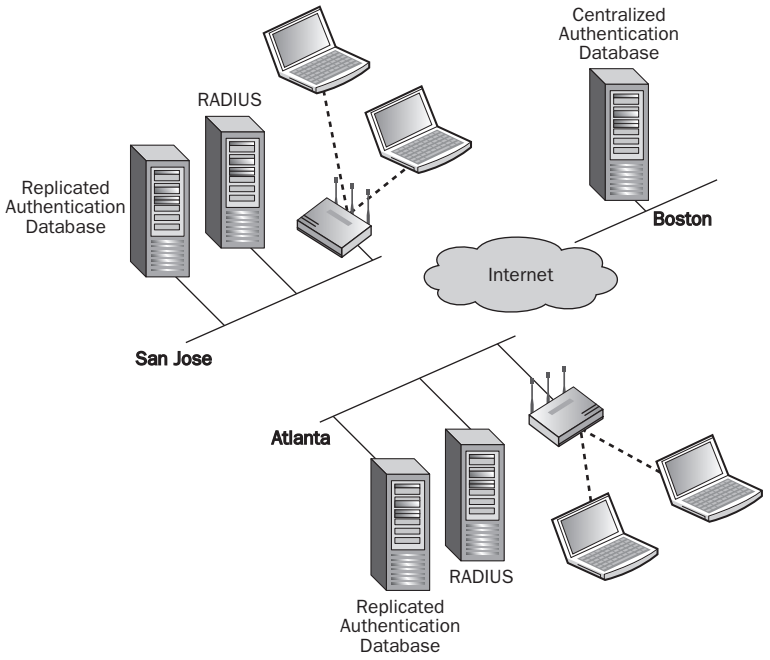
If an organization has WLANs at multiple locations or different cities, RADIUS can be scaled in a number of ways to support the multiple sites. As shown in Figure 12.12, a distributed autonomous sites scenario can replicate the authentication database from a central site to each autonomous site. All user authentications still occur locally.

A distributed autonomous sites scenario is defined by:

- Multiple WLANs existing at different locations
- The central authentication database is replicated to database servers at each autonomous site.
- Each remote site has one or more RADIUS servers that proxy to the on-site authentication database. The RADIUS server manages WLAN authenticating users, and setting up secure WLAN connections.

The main benefit to this scenario is that all of the wireless users authenticate against the local replicated authentication database and do not have to authenticate across a WAN link. If the WAN link goes down, the users can still successfully authenticate and access the wireless network. However, if the WAN link goes down, replication between the authentication databases cannot occur.

FIGURE 12.12 Distributed autonomous sites



Note that this scenario works best with authentication databases that can be easily replicated such as LDAP and Active Directory. One-time password (OTP) databases that use tokens, and SQL databases are not as easily replicated.

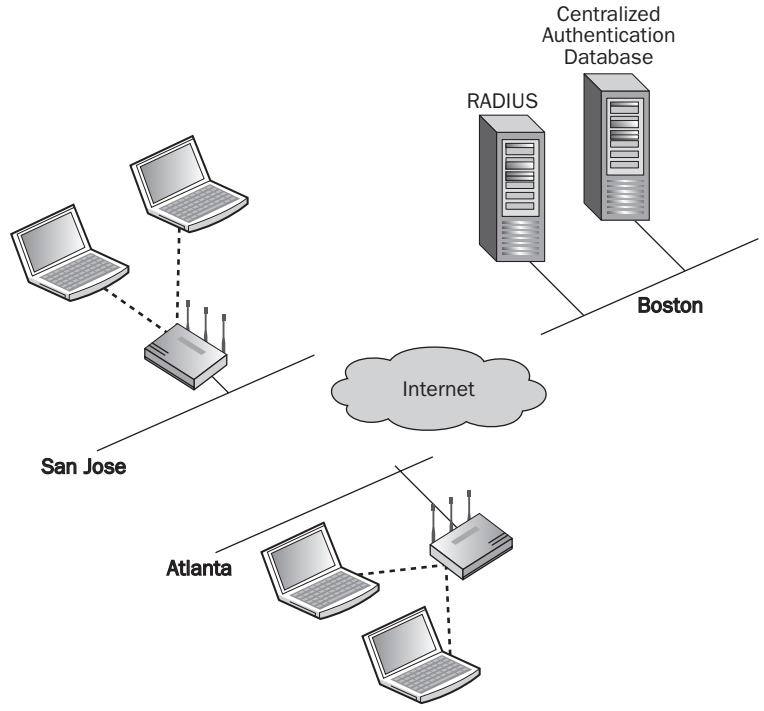
Distributed Sites, Centralized Authentication, and Security

Another approach to scaling RADIUS when multiple sites exist is to use a centralized authentication and security architecture. As shown in Figure 12.13, this scenario only uses an authentication database at a central site. All user authentication does not occur locally and must occur over a WAN link.

A distributed site, centralized authentication, and security architecture is defined by:

- Multiple WLANs existing at different locations
- The authentication database is located at a central site.
- One or more RADIUS servers are also located at the central site, and proxy to the central authentication database. The RADIUS server manages WLAN authenticating users, and setting up secure WLAN connections.

FIGURE 12.13 Distributed sites, centralized authentication, and security



The main benefit to this design is cost, because RADIUS servers and database servers are not deployed at the remote locations. The central RADIUS server can also proxy authentication against any database that is at the same location. This design may be more appropriate in situations where the authentication database cannot be easily replicated such as a token-based solution.

The biggest concern with this type of design is if the WAN link goes down, no new wireless user authentication can occur and the users would not be able to access the local wireless network. Performance bottlenecks can also occur that might affect latency. Timer values which will be discussed later in this chapter are a greater concern when users must authenticate to a database across a WAN link.

Distributed Sites and Security, Centralized Authentication

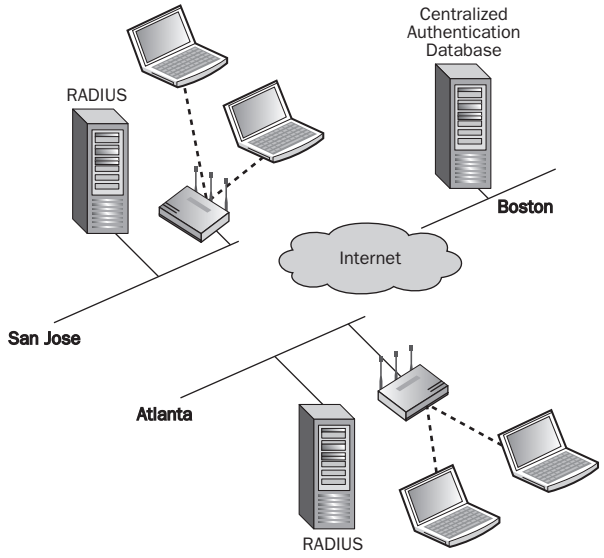
When multiple sites exist, this approach to scaling RADIUS is very similar to the previous model. However, some of the security workload is offloaded to the remote sites. As shown in Figure 12.14, this scenario also uses an authentication database at a central site. All user authentications do not occur locally and must occur over a WAN link.

A distributed sites and security, centralized authentication architecture is defined by:

- Multiple WLANS existing at different locations
- The authentication database is located at a central site.
- One or more RADIUS servers are located at the remote site and proxy the authentication request to the central authentication database. The RADIUS servers manage WLAN authenticating users, and setting up secure WLAN connections.

The design can be expensive, however it offers more flexibility. The biggest concern with this type of design is if the WAN link goes down, no new wireless user authentication

FIGURE 12.14 Distributed sites and security, centralized authentication



can occur and they would not be able to access the local wireless network. To prevent this from occurring, user accounts could be duplicated in the native databases of the local RADIUS server for a failover solution if the WAN link were to go down. This design is also appropriate in situations where the authentication database cannot be easily replicated, such as a token-based solution.

Large organizations with defined security policies fall into this category. For example, one location might house Human Resources staff, another Accounting staff, and yet another R&D staff. Each location should have the ability to control access and authentication at each facility.

For example, a user who works in a warehouse in Southern California would have access to the network at that location to perform his or her daily activities. If that user were to attempt a log in at another facility, perhaps where Accounting staff are located, that

individual or distributed site might deny access to the user. However, the same warehouse user might have access at corporate headquarters where centralized applications and training facilities are located.

The benefit of this model is that it is the most flexible. A centralized user database means that each user would have a single-user identity (username and password), but the enterprise would have the ability to limit individual users' rights at each location.

Built-in RADIUS Servers

Many WLAN vendors are embedding mini-RADIUS servers into their WLAN products. This can be particularly useful in small sites or perhaps in a remote site RADIUS-failover scenario with simple requirements. For example, a remote-office WLAN controller with a built-in RADIUS database can be used as a failover solution for authentication when a primary RADIUS server is not available because a WAN link goes down.

The embedded RADIUS servers that are incorporated into many of the WLAN APs and controllers are not as full featured as the dedicated RADIUS servers. Although each of the vendors offer different capabilities, features such as VLAN assignment and rate limiting are sometimes lacking.

RADIUS Failover

Complete loss of connectivity to a RADIUS server will result in no further user or device authentication. This typically will not affect currently associated and authenticated clients until their reauthentication or session timer expires. There is no standards-based specification or criteria for when an authenticator considers the RADIUS server to be "down." The methods for determining this might even vary from firmware to firmware.

When configuring a WLAN infrastructure device, there are often at least three RADIUS servers that can be configured. Multiple RADIUS servers may be deployed for redundancy purposes. The first server in the list is usually considered the primary server. When a RADIUS server is determined to be unavailable based on the method used by the WLAN infrastructure, it will move to the next server in the priority list.

Typically, a hold-down timer will be enacted that monitors the availability of that RADIUS server until it is considered stable in order to be sent authentication or accounting transactions again. Depending on the settings or logic of the authenticator functionality in the AP or WLAN controller, the original RADIUS server may not revert to the primary role automatically. It is possible that not until the second and possibly the third RADIUS server configured is also considered unavailable, the original one will be reinstated to the helm as the primary server.

Even if the other servers are geographically far away, resulting in added latency, this may not cause any other problem other than slowness of all RADIUS transactions as long as the network connection is still reliable. We highly recommend that you monitor for RADIUS failover events on your APs and WLAN controllers.

Timer Values

When two network applications communicate, in order to maintain the application state, programmers typically implement timer values to handle situations where one end of the link does not respond in a timely fashion. Without timer values, applications might be stuck in a state waiting for a response from the third packet exchange and not accept another inbound request from that station until it gets that response. Without some type of timer thresholds, applications could be sent into a tizzy.

802.1X authentications have several timer values that are important to consider. While not all WLAN vendor hardware/software supports overriding or managing these timers, this information still might save you some headaches in future troubleshooting sessions. When an 802.1X session is initiated, there is a unique session ID for that transaction. When a timer value expires, that particular session expires. Any response received after that session is abandoned and will be discarded.

EAP Timers

EAP timers affect the 802.1X/EAP authentication between the supplicant and the authenticator. Enterprise-grade APs and WLAN controllers should have the ability to adjust the EAP timer values that affect all 802.1X/EAP authentications for these devices.

EAP Request

The EAP Request timer specifies the time when the 802.1X state machine will abandon the current session when waiting for a response from the supplicant. Consider the case where an 802.1X authentication begins and progresses to the point where a low CPU-capable device has to perform a TLS tunnel before passing its identity—for example, with EAP-FAST, EAP-TTLS, and EAP-PEAP. The processing burden, in addition to whatever else that device might also be processing, might be enough to cause a response too long before the AP/authenticator abandons the current 802.1X session. Perhaps a virus scan was in process on the client device, or maybe its CPU is just simply too low powered. More capable laptop computers are not the usual culprits. Rather, the problem usually occurs with handheld computers, VoWiFi phones, or wireless application-specific devices.

We advise you to set this timer to the highest value to accommodate the slowest client and not for the fastest, most capable client. Usually these timers are global values that operate for all SSIDs. Default settings may suffice in most scenarios, but sometimes manufacturer products are set too aggressively, causing the timers to expire too quickly. More sophisticated client supplicants will allow modification of EAP request timer settings as well. As a general note, client supplicant settings should match the infrastructure settings.

EAP Identity Request

During the 802.1X/EAP process, depending on the EAP type, the client identity is requested. This may be seen in the form of a dialog box requesting user input. The EAP Identity Request timer affects how long before the 802.1X/EAP session will expire once

the maximum retry limit is exceeded. Typically, a setting that affects how many times the supplicant will reattempt the EAP Identity Request accompanies this timer, as shown in Figure 12.15.

FIGURE 12.15 Example EAP timer settings from a Cisco 4400 WLAN controller

```
EAP-Identity-Request Timeout (seconds)..... 10
EAP-Identity-Request Max Retries.......... 20
EAP Key-Index for Dynamic WEP............. 0
EAP Max-Login Ignore Identity Response..... enable
EAP-Request Timeout (seconds).............. 10
EAP-Request Max Retries.................... 20
EAPOL-Key Timeout (seconds)................ 1
EAPOL-Key Max Retries...................... 2
```

When using any type of authentication configuration requiring manual user input, such as a one-time password (OTP) or a PIN when using a smart card, a user acts relatively slowly. The time the 802.1X state machine waits for a response may need to be overridden in situations involving these types of EAP or authentication methods. It is interesting to see that even equipment from a single vendor, but with different models or product families, can vary from 1 to 30 seconds or more.

RADIUS Timers

RADIUS timers affect the interaction between the authenticator and the RADIUS server, and affect all 802.1X/EAP transactions.

RADIUS Authentication Retransmission Timeout

This is the timer value that the authenticator will wait for the RADIUS server transaction. Remember, the RADIUS server is typically configured as a proxy, and it will usually need to query another authentication database or a PKI infrastructure, as in the case of EAP-TLS. The default timer might not be long enough for this transaction to occur in all cases, which might cause an authenticator to fail over to a secondary RADIUS server if configured.

AP-Based Timers

AP-based timer values affect the operation of wireless client connections to APs. Session timers and inactivity timers are often configurable settings on access points and WLAN controllers.

Session Timeout

Whenever a wireless client associates with a WLAN, regardless of the authentication mechanism, a timer usually governs how long that client will continue to be allowed on the WLAN until it is forced to reauthenticate, and perhaps reassociate.

When a session timeout expires, it can be quite a disruptive event because the AP will typically send an 802.11 deauthentication frame to the wireless client. Should this client be

in the middle of an active phone call or other latency-sensitive or session-based application, this might really frustrate users.

Session timeouts are desirable predominantly when not in an RSN. RSN networks using strong EAP types typically will re-key at regular intervals or after a certain amount of traffic. Legacy 802.1X using dynamic WEP is a method that benefits from a session timeout value. This is because when enough WEP frames are recovered, the key for that pairwise association can be discovered, thereby losing data confidentiality. However, with a strong EAP type and when using WPA/WPA2, there is no current risk of traffic decryption. Therefore, when using these current methods, we recommend that you disable this feature altogether or place it at such a high value where any negative impact of it will be acceptable.

Inactivity Timer

When a client is associated with a WLAN and simply stops receiving or transmitting any wireless traffic, this is the timer that, once expired, will deauthenticate the client from the WLAN.

If a client were to run out of battery power and simply turn off, the AP need not continue to buffer traffic for it or maintain anything related to its state.

WAN Traversal

Network latency should always be a consideration when time-sensitive applications are deployed. Although this may seem trivial, the enterprise's centralized datacenter is the most likely location for any type of server because the datacenter is usually designed for high availability and provides both physical and network security.

802.11 authentications, or reauthentications for certain applications, can be very noticeable to end-users. Applications like voice and video are only two examples. When these authentications have to traverse a wide area network (WAN), there can be significant variance to response times. Consider the reality of ISP backbone design. Your local bandwidth contract with your circuit termination point isn't a guarantee of bandwidth you will receive. Your packets will traverse different backbone providers and network routers that are also servicing other circuits and traffic just like yours. There simply isn't a guaranteed amount of bandwidth for every second, 24 hours a day.

Put another way, ISPs oversubscribe their networks. That's undeniable. Otherwise, they simply wouldn't make any money. They are betting on the law of averages; that is, not every user is going to be consuming large amounts of bandwidth at the same time. Perhaps you may remember the first Victoria Secret fashion show simulcast online. Their video streaming servers became completely saturated and people became very frustrated. These kinds of events have a profound effect not only on the traffic to their servers, but can potentially impact all other network traffic traversing common backbone segments.

Therefore, if you are running or designing an authentication server to be run out of a remote facility over a WAN, pay careful attention to the round-trip traffic transmission times. You can't simply look at the average delays; you also need to look at the peak response times and consider that these might result in authentication timer expiration.

Transmission delays are only part of the equation. TCP and UDP behave quite differently, especially over networks you don't control. TCP will send retransmissions while UDP will not. Once a UDP frame is lost or corrupted in transit, it is indeed gone—that is, it will not be retransmitted.

An important consideration is that RADIUS uses UDP for its communication either over ports 1645 and 1646 (authentication and accounting, respectively) or 1812 and 1813.

Multifactor Authentication Servers

In Chapter 4, we discussed many EAP types as well as the option of using more than one authentication credential at the same time. For example, an OTP server and a smart card using a PIN value are two examples of multifactor authentication mechanisms that will need to communicate with multifactor authentication servers. These technologies are not directly part of an open standard but indeed utilize open standards to enable their features.

The main point you need to understand with multifactor authentication servers is that they must be integrated with your authentication server and/or user database technology. Each vendor has a different architectural model and even has its own tools to manage the secondary factor credential system (smart cards, OTPs, USB tokens, and so on). Discuss your existing authentication server and user database technology with the vendors to ensure interoperability.

Public Key Infrastructure (PKI)

A *public key infrastructure (PKI)* is an infrastructure system that allows the secure exchange of data over a public, unsecured network. PKIs can cover the scope of the entire Internet or operate within the confines of an enterprise network.

Digital certificates are used along with asymmetric encryption algorithms that accomplish an amazing feat. Asymmetric encryption allows for a message to be encrypted with one key and decrypted only with a related but different key. These keys are referred to as the public and private keys, respectively.

Consider two users named Alice and Bob, who need to exchange information with each other over a public, unsecured medium such as the Internet. Alice wants to send a message to Bob. PKI asymmetric encryption works by publishing and making readily available the public key for Alice and Bob, but for the context of our example, only Bob's public certificate is needed. This public key could be obtained directly from the intended recipient but may also be published elsewhere. The concept of the public key is that it needs indeed to be *public* and made accessible to anyone wishing to send encrypted data to the owner of that certificate.

In our example of Alice sending data to Bob, Alice first obtains the public certificate for Bob. Alice encrypts the message intended for Bob with Bob's public certificate. Once Bob receives the encrypted message, only Bob can decrypt it because only Bob has the private

key. This is the concept of asymmetric encryption in that the key used to encrypt can only be decrypted with a different but related key.

Certificates used in PKIs usually are issued by a *certificate authority (CA)*. CAs are analogous to notaries in the paper document world. They are used to *sign* documents that provide credibility to the validity of the document. It is like your friend vouching for the identity or trustworthiness of someone you may not know. Since you trust your friend and they are vouching for the other person, you also extend your trust. Just like humans need to have trust in the notary system, computers need to be able to trust certain entities themselves to serve as a trusted authority.

Using our same example, when Alice wants to send a message to Bob, Alice obtains the public digital certificate for Bob. Before Alice encrypts the message, she first looks to see if the certificate was signed and by whom. The CA who signed the certificate for Bob is included in this digital certificate, and Alice can contact the CA to see if that certificate is still valid (not revoked). When contacting the CA, the process also proves the validity of the public certificate. The name of the entity to which it belongs, the valid date range, and other factors are contained in this public certificate (see Figure 12.16). Once Alice is satisfied with the validity of Bob's certificate, she then proceeds with the normal process as originally described by encrypting the message with the public certificate and sending it to Bob, where only Bob can decrypt it with the private key. The factors contained in this public certificate include the following:

- Version number
- Serial number of the certificate
- Issuer algorithm information

FIGURE 12.16 Digital certificate

- Issuer of certificate
- Valid to/from date
- Subject's public key
- Public key algorithm information of the subject of the certificate
- Digital signature of the issuing authority
- X.509v3 optional extensions

The information embedded in the public certificate is also helpful for the person wishing to send a message. The sender may wish to use this information to discern whether they are indeed speaking to the correct party, as you learned in the topic of mutual authentication covered in Chapter 4. Consider our example of Alice and Bob again, if Bob wanted to send a response back to Alice, the process would start all over again but this time initiated by Bob.

Self-Signed Certificates

It is still possible to use certificates that are not signed by a CA. In this case, the certificate is presented to the user and an error message is typically presented that it is not issued by a trusted CA.

A self-signed certificate isn't purchased from a commercial CA such as VeriSign or Thawte. When using self-signed certificates, a conscious decision is made to avert the normal operational model of PKI, thereby placing the responsibility on the end-user whether or not to trust the source.

Self-signed certificates are commonly installed on network infrastructure devices by default. This allows for secure management out of the box for HTTPS, SSL, or other protocols using a digital certificate model. Self-signed certificates may be used in TLS-based EAP types as well. For you to be able to trust these sources, every self-signed certificate must be distributed and stored on each client device.

If you have complete control over these self-signed certificates and the private key is kept private, this approach can be very secure. The problem is the operational headache involved with the distribution of each self-signed certificate you would like to trust.

Enterprise PKI

After obtaining a self-signed certificate, you must install your own private or enterprise PKI. Windows Server operating systems come with a free CA software package that can integrate into Active Directory. The important part about the Active Directory integration is that, once a CA is created, you can *publish* this to Active Directory and thus automatically distribute the identity of this CA to the entire Active Directory and to your entire computer population as well.

Once your own CA is in place, you can create certificate-signing requests (CSRs), or you can manually create the certificates using the CA administrator utility and then issue them to your devices. For example, your entire intranet, network devices, and servers can be issued a certificate from your own CA, and all your network devices will automatically trust the signer of these certificates because it has been distributed to Active Directory.

Therefore, you can also use your own CA to issue certificates to your RADIUS servers and successfully perform mutual authentication based on these certificates. We recommend that you allow for every computer to reboot or log in again once the CA is published to Active Directory.

Role-Based Access Control

The 802.11-2007 standard only defines operations at Layers 1 and 2 of the OSI model. However, because an 802.11 WLAN is a portal to your preexisting network infrastructure, upper-layer design considerations still exist when deploying a WLAN. 802.1X/EAP is initially used to make sure only valid WLAN users are allowed onto network resources. However, there is no reason that all users need to access all network resources. Therefore a method is needed to segment users to certain network resources after they have been authenticated at Layer 2.

Role-based access control (RBAC) is an approach to restricting system access to authorized users. The majority of WLAN controller solutions have RBAC capabilities. The three main components of an RBAC approach are *users*, *roles*, and *permissions*. Separate roles can be created, such as the sales role or the marketing role. Individuals or groups of users are assigned to one of these roles. Permissions can be defined as Layer 2 permissions (MAC filters), Layer 3 permissions (access control lists), Layers 4–7 permissions (stateful firewall rules), and bandwidth permissions. All these permissions can also be time based. The permissions are mapped to the roles.

Once users are assigned to roles, they inherit the permissions of whatever roles they have been assigned. For example, users that associate with a "Guest" SSID are placed in a unique guest VLAN. The users then authenticate via a captive portal and are assigned a guest role. The guest role may have bandwidth permissions that restrict them to 100 kbps of bandwidth and allow them to use only ports 80 (HTTP), 25 (SMTP), and 110 (POP) during working hours. This scenario would restrict guest users who are accessing the Internet from hogging bandwidth and only allow them to view web pages and check email between 9 A.M. and 5 P.M. When used in a WLAN environment, role-based access control can provide granular wireless user management.

Role Assignment

Individual users or devices can be assigned to roles in a variety of methods including:

Pre-Authentication Role Assignment Users are assigned to a role prior to authentication. A common method of pre-authentication role assignment is to place users into specific roles based on simple Layer 2 association. For example, any users that associate to an SSID called GUEST get assigned to a specific role. Any users that associate to an SSID called CORPORATE are assigned to a different role. Each role has unique access restrictions.

Post-Authentication Role Assignment Users can be assigned to roles based on the user authentication method. For example, any user that authenticates using captive-portal

authentication is assigned to a role called GUEST. Any user that authenticates via 802.1X/EAP is assigned to a role called EMPLOYEE. Each role has unique access restrictions.

Server-Based Role-Assignment When a user authenticates using 802.1X/EAP, RADIUS attributes can be used to assign users into a specific role automatically. This is often referred to as server-based role derivation or server-based role assignment. One advantage of server-based role assignment is that all the users can associate to the same SSID but be assigned to unique roles. This method is often used to assign users from certain Active Directory groups into predefined roles created on a WLAN controller. Each role has unique access restrictions.

Built-in/Integrated Firewalls

Initially, the concept of a firewall built into the WLAN may not seem that spectacular. What is the big deal if you have to add a firewall to a WLAN design rather than having it integrated? The point may not seem obvious until you think about how the basic functionality of the WLAN can change given two important factors: software integration and traffic path.

Consider a base WLAN infrastructure being fully integrated into a rich set of security policies and traffic rules. Next, consider that in enterprise WLANs you authenticate each user to an authentication server by using 802.1X or perhaps even a web-based authentication mechanism. When knowing the exact identity of the *user* operating a WLAN client, you now know the context of that user.

Network traffic in WLANs is also an important consideration when firewall designs are implemented. In a split-MAC architecture, all network traffic traverses through the WLAN controller, usually located at the network core. In hybrid or split-MAC architectures using more advanced features, the data plane is split out at the AP, which is located at the network edge. Integrated firewalls need to inspect and block the traffic where the data plane splits off into the network.

Roles and firewall policy restrictions are pre-created on a WLAN controller. Different roles have different policies linked to the roles. Once a user has been assigned to a role, we can immediately assume certain policy restrictions for this user. For example, only employees who are in the Accounting department should have access to the accounting applications. Nonaccounting department employees should not have access to sensitive financial information such as payroll, time clock, and expense accounting systems. If nonaccounting employees need access to these systems, typically it may be only to a web-based interface to enter hours or expenses. Therefore, the opportunity exists to limit their access to these applications based on IP and TCP/UDP ports. The same goes for doctors in a health-care setting. Accounting users should not be able to access applications and servers on the network that contains sensitive patient health-care information (PHI) data.

When we design a wired network and implement firewall rules, we typically never have the opportunity to place these levels of restrictions at the network level because we don't know the user identity. The traditional model is to rely on the applications themselves to control user access.

For WLANs, we have already learned that, in order to gain much in the way of security, we must implement 802.1X/EAP. Therefore, in an enterprise WLAN, we should potentially know a great deal about each and every user who accesses the WLAN.

An integrated firewall means that when user david.coleman logs into the network, he should have uniquely identifiable and different rights than user shawn.jackman. David, for example, might work in the Atlanta office while Shawn works in the Silicon Valley office. Perhaps Shawn and David work for two different company divisions or departments. When Shawn visits Atlanta, enterprise security policy might require limiting the hours Shawn can use the network as well as potentially the network file share, printers, and other network resources at the Atlanta office. The main point here is that relying on the network itself to restrict that access is nearly impossible unless an integrated firewall is present.

WLAN vendors who have integrated firewalls can literally restrict each user down to incredibly granular levels. This may even include bandwidth restrictions. For example, perhaps the 802.1X/EAP authentication is for a VoWiFi phone for which we are aware of the traffic profile. We know that the device talks to specific gateways, devices on specific subnets, and even speaks very specific TCP and UDP protocols. Unless a firmware update is in process or something outside of normal telephony operations is occurring, we can easily place these user accounts into a VoWiFi device group that limits traffic to 500 kbps or so. Therefore, not only can anyone compromising these credentials be limited to areas that this user account can go to on the network and what protocols it is allowed to use, but the amount of traffic allowed the account is also limited, which can further limit the types of attacks a malicious hacker can perform.

Another example is the case of Hospital K, where they have a series of medical instruments that have old very old operating systems and limited ability to host antivirus software. These types of devices can be huge security risks and need to be put into a class of devices that have strict network control in place. For example, these medical devices may communicate with a single server over a specific TCP port. If each device used a unique user identity that was part of a role called BIOMEDICAL, the WLAN infrastructure would place these restrictions on each login that is a member of this role.

ACLs

An *access control list (ACL)* is a more traditional traffic control mechanism typically applied at a router interface between VLANs and more recently at a WLAN level. ACLs may still be useful for guest users where the only traffic already allowed for guests is routed to a default gateway to the Internet. In fact, many enterprises implementing guest access use a completely different Internet circuit whereby these users, from a network perspective, are just like they are outside the facility.

More advanced ACLs may also be helpful in the use of devices that may not be capable of 802.1X. For example, all VoWiFi phones might come from one MAC Organizationally Unique Identifier (OUI) such as 00:11:22:xx:xx:xx. The ACL could be applied even without 802.1X for any Wi-Fi device with a MAC OUI of 00:11:22.

Network Access Control (NAC)

Network Access Control (NAC) is a computer network security methodology that integrates endpoint security technology (such as antivirus and software patch versions) with user authentication. Access decisions are also based on a client's antivirus state and OS pack version. NAC is an upcoming security enhancement gaining a lot of industry attention, and is typically designed to work with RADIUS servers. NAC servers are often being tied into an 802.1X framework design. The goal of a NAC solution is to enforce network security compliance. NAC is designed to identify authorized and compliant network devices based on a variety of criteria and attempt to limit network access for noncompliant devices. If the device is identified as a network printer (perhaps based on its MAC OUI or the first few frames it attempted to send), a NAC system may place it on a specific VLAN that has the necessary security profile for it to perform its job but not anything more than is necessary.

NACs, depending on the vendor, can perform a client interrogation to look for a properly installed and up-to-date antivirus software package, OS server pack levels, or just about anything else that an IT department might require in order to ensure the overall network security for all users. Potential damage from emerging and active security threats may therefore be prevented.

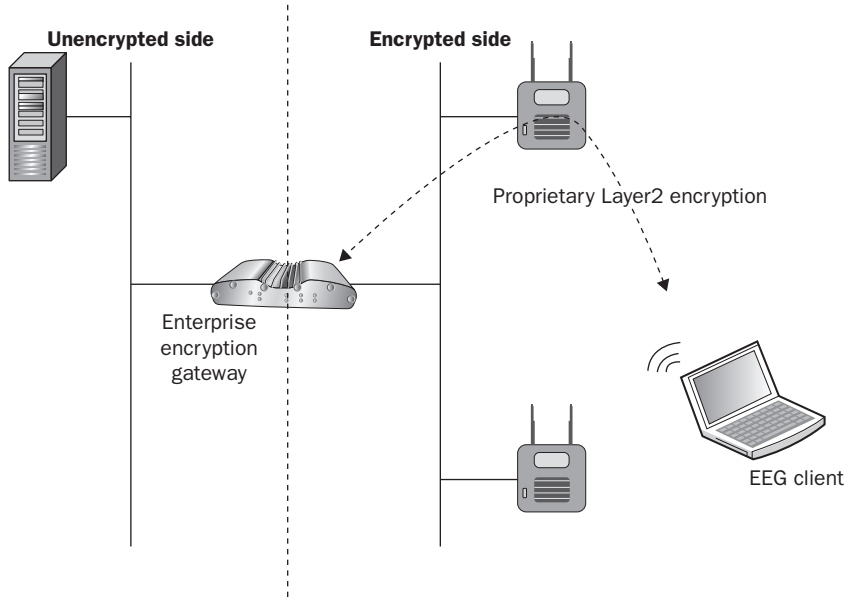
From a WLAN perspective, NACs typically work in concert with an 802.1X authentication framework and learn about the user identity and network privileges while at the same time ensuring that users have the right installed software or patches before network access is allowed. A noncompliant wireless station requesting access to a NAC-enabled WLAN might be placed on a quarantine network and users could be redirected to a web page in order to download and install the necessary components. The only network access the user would have would be to download and install the necessary components.

Enterprise Encryption Gateways

An *enterprise encryption gateway (EEG)* is an 802.11 middleware device that allows for segmentation and encryption. The main purpose of an EEG is to provide an overlay encryption solution for a pre-existing WLAN infrastructure.

An EEG solution could be characterized as a proprietary Layer 2 VPN solution, as shown in Figure 12.17. The EEG typically sits behind several autonomous access points and segments the wireless network from the protected wired network infrastructure. Proprietary encryption technology using the AES algorithm at Layer 2 is provided by the enterprise encryption gateway. Standard WPA2-compliant WLAN devices use Advanced Encryption Standard (AES) 128-bit dynamic encryption keys. EEG solutions can also provide 192-bit and 256-bit AES encryption.

FIGURE 12.17 Enterprise encryption gateway



EEGs have been around for quite some time. The military has used EEGs to encrypt traffic securely using standards-based IEEE 802.11 WLANs prior to the introduction of WPA/WPA2.

EEGs operate on a concept very similar to VPNs. On a client device, a piece of software is installed that communicates with a server (encryption gateway) typically located at the edge of a network to which users needs to gain access. Once a network connection by a client device is established, the software agent then automatically contacts the encryption gateway before any data traffic is sent. The software agent can then form a highly encrypted and perhaps even highly proprietary encrypted tunnel to the encryption gateway. An EEG is basically an overlay encryption solution that sits on top of the existing WLAN infrastructure. Companies like AirFortress and Cranite have specialized in these types of software and gateway products. Harris Corporation has even developed a WLAN radio replacement or Wi-Fi-to-Ethernet Bridge with an embedded hardware encryption module offloading all of the CPU encryption activity to the WLAN radio device itself.

Summary

WLAN security plays an integral part of client device performance. With wired LANs, firewalls are placed between networks where network activity needs to be policed. The security a wired-side firewall provides does not affect the installation or configuration of a wired client device.

IEEE 802.11 WLANs operate very differently. Security choices greatly affect the design, architecture, and type of clients that can run over the WLAN. In fact, the opposite is true as well. The devices themselves and their criticality to the business might dictate changes or exceptions to security policy. Because a WLAN is a network-based technology, we typically relate WLAN security and methodologies to the model of how wired LANs work. As you have gathered from your reading of this book, that couldn't be further from the truth. WLAN performance is tightly interwoven with WLAN security, RF propagation and design, as well as infrastructure features and capabilities. Hardly any technology architecture we commonly use today has this level of integration and co-dependency.

By reading this chapter, you have learned about the important components involved in enterprise security solutions from the infrastructure perspective and also understand the basic security design issues involved.

Exam Essentials

Understand types of WLAN architectures. Know the different types of architectures, including autonomous, split-MAC, mesh, remote site, and hybrid.

Understand Common Infrastructure Device Features and Features that Pertain to Security. Know design details and security components of infrastructure and device features.

Be Familiar with Device Management Features. Know the various device management methods, features, and protocols available in WLAN devices.

Understand RADIUS Servers and Features. Explain proxy, AVPs, VSAs, dynamic VLAN assignment, integration, and scaling.

Explain Role-Based Access Control. Understand the relationship between user roles and access policies.

Key Terms

access control list (ACL)

access controller (AC)

attribute-value pairs (AVPs)

autonomous AP

Certificate Authority (CA)

community string

Control and Provisioning of Wireless Access Points (CAPWAP)

controller-based AP

Datagram Transport Layer Security (DTLS), domain

dynamic frequency selection (DFS)

enterprise encryption gateway (EEG)

local-MAC AP

location based access control (LBAC)

management information base (MIB)

mesh point portal (MPP)

network access control (NAC)

non-root bridge

permissions

public key infrastructure (PKI)

realm

realm-based authentication

Role-based access control (RBAC)

roles

root bridge

sign

Simple Network Management Protocol (SNMP)

split MAC architecture

tromboning

vendor-specific attributes (VSAs)

WIDS/WIPS

wireless network management system (WNMS)

wireless termination points (WTPs)

WLAN controller

WLAN profiles

Review Questions

1. Which terms best describe components of a centralized WLAN architecture in which all the intelligence resides in a centralized device and pushes the configuration settings down to the access points? (Choose all that apply.)
   - **A.** WLAN controller
   - **B.** Wireless network management system
   - **C.** Enterprise wireless gateway
   - **D.** Cooperative control AP
   - **E.** Controller-based AP

2. On which device can you create and configure VLANs? (Choose all that apply.)
   - **A.** WIPS server
   - **B.** Autonomous AP
   - **C.** Ethernet switch
   - **D.** WLAN controller
   - **E.** All of the above

3. What term best describes a WLAN architecture where the integration service (IS) and distribution system services (DSS) are normally handled by a WLAN controller while generation of certain 802.11 management and control frames are handled by a the controller-based AP?
   - **A.** Cooperative control
   - **B.** Distributed data forwarding
   - **C.** Distributed hybrid architecture
   - **D.** Distributed WLAN architecture
   - **E.** Split-MAC

4. Which protocol defines split-MAC mechanisms?
   - **A.** LWAPP
   - **B.** GRE
   - **C.** CAPWAP
   - **D.** DTLS
   - **E.** VRRP

5. Which protocol can be used to provide data privacy communications between an access point and a WLAN controller?
   - **A.** LWAPP
   - **B.** GRE
   - **C.** CAPWAP
   - **D.** DTLS
   - **E.** VRRP

6. A WNMS server can be used to monitor and manage what kind of devices? (Choose all that apply.)
   - **A.** Autonomous APs
   - **B.** Mesh APs
   - **C.** Controller-based APs
   - **D.** Enterprise encryption gateways
   - **E.** WLAN controllers

7. RADIUS server dynamic VLAN assignment can be performed over which of the following? (Choose all that apply.)
   - **A.** WPA-Personal
   - **B.** WPA2-Personal
   - **C.** WPA-Enterprise
   - **D.** WPA2-Enterprise

8. Which of these protocols can be used to manage WLAN infrastructure devices?
   - **A.** HTTP
   - **B.** SSH
   - **C.** SNMP
   - **D.** Telnet
   - **E.** HTTPS
   - **F.** SNMP
   - **G.** All of the above

9. Location-based access control (LBAC) is defined in which 802.11 standard?
   - **A.** 802.11e
   - **B.** 802.11i
   - **C.** 802.11w
   - **D.** 802.11n
   - **E.** None of the above

10. Public Key Infrastructure is an important requirement for which EAP method?

- **A.** EAP-FAST
- **B.** PEAP
- **C.** EAP-TLS
- **D.** EAP-MD5
- **E.** EAP-TTLS

11. The ACME Company has over 300 WLAN users communicating through 25 access points using GRE to tunnel all 802.11 user traffic back to a central WLAN controller capable of role-based access control (RBAC). What type of access restrictions can be placed on the users after authentication?

- **A.** UDP
- **B.** TCP
- **C.** Bandwidth
- **D.** Time-of-day
- **E.** All of the above

12. RBAC mechanisms can be used to restrict user access to what resources available though a WLAN? (Choose all that apply.)

- **A.** UDP applications
- **B.** TCP applications
- **C.** Bandwidth
- **D.** RF medium
- **E.** Internet gateway

13. What components make up a distribution system? (Choose all that apply.)

- **A.** HR-DSSS
- **B.** Distribution system services
- **C.** DSM
- **D.** DSSS
- **E.** Intrusion detection system

14. Which method of role assignment allows users to associate to the same SSID yet assigns users to different roles with unique access restrictions?

- **A.** Server-based role assignment
- **B.** Pre-authentication role assignment
- **C.** Post-authentication role assignment
- **D.** Intrusion-based role assignment

15. What type of network security can be tied together with 802.1X/EAP to ensure laptops and other WLAN devices have the latest anti-virus signatures and OS server pack levels?
    - **A.** Stateful firewall policies
    - **B.** Network access control
    - **C.** Access control lists
    - **D.** Role assignment

16. What are some of the major differences between SNMPv3 and SNMPv2? (Choose all that apply.)
    - **A.** SNMPv3 requires username/passwords
    - **B.** SNMPv3 requires community strings
    - **C.** SNMPv3 uses 56-bit DES encryption to encrypt packets.
    - **D.** SNMPv3 uses 128-bit AES encryption to encrypt packets.

17. What is the biggest security risk associated with Simple Network Management Protocol (SNMP)?
    - **A.** DES encryption can be cracked
    - **B.** Weak data integrity
    - **C.** Lack of vendor support
    - **D.** Default community strings

18. Which of these RADIUS design architectures may not be appropriate when deployed using an 802.1X/EAP solution with tokens and an OTP database?
    - **A.** Single site deployment
    - **B.** Distributed autonomous sites
    - **C.** Distributed sites, centralized authentication, and security
    - **D.** Distributed sites and security, centralized authentication

19. What type of database can be integrated with a RADIUS server for proxy authentication?
    - **A.** eDirectory
    - **B.** Active Directory
    - **C.** SQL
    - **D.** LDAP
    - **E.** All of the above

20. What type of WLAN security solution using 256-bit AES encryption can be deployed on top of a pre-existing WLAN infrastructure?
    - **A.** RADIUS
    - **B.** CCMP
    - **C.** RBAC
    - **D.** EWG
    - **E.** EEGReview Questions 504

Answers to Review Questions

1. A, E. In the centralized WLAN architecture, autonomous APs have been replaced with lightweight access points also known as controller-based APs. All the intelligence resides on the centralized device known as a WLAN controller.

2. C, D. All of these devices support VLANs, but VLANs must be created and configured on either a managed Ethernet switch or a WLAN controller.

3. E. The majority of WLAN controller vendors implement what is known as split-MAC architecture. With this type of WLAN architecture, some of the MAC services are handled by the WLAN controller and some are handled by the controller-based AP.

4. C. Most WLAN controller vendors implement split-MAC architectures differently. The Internet Engineering Task Force (IETF) has proposed a set of standards for WLAN controller protocols called Control and Provisioning of Wireless Access Points (CAPWAP). CAPWAP does define split MAC standards.

5. D. CAPWAP incorporates Datagram Transport Layer Security (DTLS), as defined in RFC 4347, as the security algorithm for the CAPWAP protocol. DTLS can be used to encrypt CAPWAP control traffic between a WLAN controller and the APs. DTLS can also be used to secure tunnel communications for data traffic.

6. A, B, C, E. Any network device that supports SNMP can be centrally-managed; however, a WNMS is normally used to manage APs and WLAN controllers. The original purpose of a WNMS was to provide a central point of management and monitoring for autonomous APs. Configuration settings and firmware upgrades can be pushed down to the autonomous access points from the WNMS server. However, WLAN controllers effectively have replaced the WNMS as a central point of management for access points. Currently, most WNMS servers are now also used as a central point of management for multiple WLAN controllers and APs in a large-scale WLAN enterprise.

7. C, D. WPA/WPA2-Personal use PSK authentication. PSK networks cannot use dynamic VLAN assignment because the authentication method does not involve the use of a RADIUS server. WPA/WPA2-Enterprise use 802.1X/EAP authentication that requires the use of a RADIUS server. RADIUS attribute-value pairs (AVPs) are used to assigning users into VLANs dynamically after user authentication.

8. G. All of these protocols can be used to configure WLAN devices such as access points and WLAN controllers. Written corporate policies should mandate the use of secure protocols such as SNMPv3, SSHv2, and HTTPS.

9. E. LBAC is a proprietary security solution used to prevent user access to a WLAN based on a user's location.

10. C. EAP-TLS requires client-based certificates on all supplicants, and a PKI infrastructure is a core requirement.

11. E. Role-based access control (RBAC) is an approach to restricting system access to authorized users. The majority of WLAN controller solutions have RBAC capabilities. The three main components of an RBAC approach are users, roles, and permissions. Separate roles can be created, such as the sales role or the marketing role. Individuals or groups of users are assigned to one of these roles. Permissions can be defined as Layer 2 permissions (MAC filters), Layer 3 permissions (access control lists), Layers 4–7 permissions (stateful firewall rules), and bandwidth permissions. All these permissions can also be time based. The permissions are mapped to the roles.

12. A,B,C,E. Role-based access control (RBAC) is an approach to restricting system access to authorized users. The majority of WLAN controller solutions have RBAC capabilities. The three main components of an RBAC approach are users, roles, and permissions. Separate roles can be created, such as the sales role or the marketing role. Individuals or groups of users are assigned to one of these roles. Permissions can be defined as Layer 2 permissions (MAC filters), Layer 3 permissions (access control lists), Layers 4–7 permissions (stateful firewall rules), and bandwidth permissions. All these permissions can also be time based. The permissions are mapped to the roles.

13. B, C. The distribution system consists of two main components. The distribution system medium (DSM) is a logical physical medium used to connect access points. Distribution system services (DSS) consist of services built inside an access point or WLAN controller usually in the form of software.

14. A. RADIUS attributes can be used to assign users into a specific role automatically. This is often referred to as server-based role derivation or server-based role assignment. One advantage of server-based role assignment is that all the users can associate to the same SSID but be assigned to unique roles. This method is often used to assign users from certain Active Directory groups into predefined roles created on a WLAN controller.

15. B. Network Access Control (NAC) is a computer network security methodology that integrates endpoint security technology (such as antivirus and software patch versions) with user authentication. Access decisions are also based on a client's antivirus state and OS pack version. NAC is an upcoming security enhancement gaining much industry attention, and is typically designed to work with RADIUS servers. NAC servers are often tied into an 802.1X framework design.

16. A, C. SMNPv3 is much more secure than older versions of SNMP. Authentication is performed using SHA or MD5. SNMPv3 uses 56-bit DES encryption to encrypt packets. SNNPv3 requires usernames and passwords instead of community strings.

17. D. Most vendor equipment defaults to SNMP being enabled with default *read* and *write* community strings. This is an enormous security threat to the configuration and operation of any network and should be one of the very first lock-down steps to securing network devices. SNMP should be disabled if it is not used for management.

18. B. A distributed autonomous sites architecture uses replicated authentication databases. This scenario works best with authentication databases that can be easily replicated such as LDAP and Active Directory. One-time password (OTP) databases that use token and SQL databases are not as easily replicated.

19. E. Although a RADIUS server is most commonly integrated with Active Directory, integration with Novell's eDirectory is also possible. Many enterprise RADIUS servers even allow a SQL database or flat files to be queried. A RADIUS server should be able to communicate with any LDAP-compliant database.

20. E. An enterprise encryption gateway (EEG) is an 802.11 middleware device that allows for segmentation and encryption. The main purpose of an EEG is to provide an overlay encryption solution for a pre - existing WLAN infrastructure. Proprietary encryption technology using the AES algorithm at Layer 2 is provided by the enterprise encryption gateway. EEG solutions can also provide 192-bit and 256-bit AES encryption.

Chapter 13

Wireless Security Policies

IN THIS CHAPTER, YOU WILL LEARN ABOUT THE FOLLOWING:

- ✓ **General policy**
  - Policy creation
  - Policy management
- ✓ **Functional policy**
  - Password policy
  - RBAC policy
  - Change control policy
  - Authentication and encryption policy
  - WLAN monitoring policy
  - Endpoint policy
  - Acceptable use policy
  - Physical security policy
  - Remote office policy
- ✓ **Government and industry regulations**
  - Department of Defense (DoD) Directive 8100.2
  - Federal Information Processing Standards (FIPS 140-2)
  - Sarbanes Oxley (SOX)
  - Graham-Leach-Bliley Act (GLBA)
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Payment Card Industry (PCI) Standard
  - Compliance reports
- ✓ **802.11 WLAN Policy Recommendations**

In the previous chapters of this book, you learned about four out of five of the major components that are required for strong WLAN security. Segmentation, data privacy, AAA, and monitoring can all be accomplished with the technology solutions that were discussed. A fifth component is still needed to provide the foundation for a fortified WLAN solution. The fifth, and perhaps most important component, is policy. All companies should have a written WLAN security policy just as they should have a written wired network security policy. All of the technical WLAN security solutions you have learned about in this book are worthless unless proper WLAN security policies are documented and enforced. WLAN security policies can be as diverse as the variety of 802.11 wireless deployments they cover. Each organization or person deploying wireless devices must use their own set of criteria and evaluation methods in reaching what they believe to be their level of acceptable risk. WLAN security that may be safe enough in a small office/home office (SOHO) environment may not be safe enough in an enterprise environment. Likewise, WLAN security that may be secure enough in an enterprise environment could be viewed as overkill and an undesirable expense in a SOHO environment.

In addition to an organization's budget and internal acceptable use policies, there are governmental and industry regulations that greatly influence security models in wireless networking. A corporate WLAN may be secure but could still fall out of compliance with an external government or industry regulation. WLAN policy makers must often strike a balance between productivity and security. Very often, mandated security policies hinder normal business operations. Even more common is the possibility that allowing business operations to flow without proper security can put company assets at risk. A well-crafted security policy must take into account business functions and security as well as any external regulations. Finding the proper balance is a key part of any security policy development.

After the policy is created to meet all of the business and regulatory requirements, it must be enforced to be effective. The policy must be enforceable and adaptable as requirements change. All WLAN policies must have the full backing of management if employees are to be expected to abide by policy. Management and employees alike must be properly trained so that all security policies are understood. The best written policy that is neither followed nor enforced is truly worthless. All policies must also be flexible and adaptable if the intended use of the WLAN changes and as WLAN technology progresses. This chapter discusses some of the fundamental aspects of a wireless security policy that are needed to cement the foundation of Wi-Fi security.

General Policy

When establishing a wireless security policy, you must first define a *general policy*. A general wireless security policy establishes why a wireless security policy is needed for an organization. Even if a company has no plans for deploying a wireless network, there should be, at minimum, a policy for dealing with rogue wireless devices. A general wireless security policy will define the following items:

Statement of Authority Defines who put the WLAN policy in place and the executive management that backs the policy.

Applicable Audience Defines the audience to whom the policy applies, such as employees, visitors, and contractors.

Risk Assessment and Threat Analysis Defines the potential wireless security risks and threats and what the financial impact will be on the company if a successful attack occurs.

Security Auditing Defines internal auditing procedures as well as the need for independent outside audits.

Violation Reporting Procedures Defines how the WLAN security policy will be enforced, including what actions should be taken and who is in charge of enforcement.

Increasingly, organizations of all sizes and types have started amending their network usage policies to include a wireless policy section. If you have not done so already, a WLAN section should be added to your organization's security policy. Two good resources for learning about best practices and computer security policies are the SANS Institute and the National Institute of Standards and Technology (NIST).

Security policy templates from the SANS Institute can be downloaded from `www.sans.org/resources/policies`. You can download the NIST special publication document 800-48 regarding wireless security from `http://csrc.nist.gov/publications/nistpubs`.

General security policies covering networking are not directly focused on any one area of technology. For this reason, you will find that general security policies tend to encompass vast portions of networking if not all of it. These policies are the larger framework from which other more specific policies are formed. In this section, we will explore policy creation and policy management, as well as internal and external policy influences.

Policy Creation

Policy creation involves decisions that can impact business as a whole in both positive and negative ways. The creation of network security policy should be part of the overall network design. However, security and its related policies are often afterthoughts

that develop once it is too late. WLAN security, such as WIPS monitoring solutions, are often deployed in response to a breach in WLAN security. Likewise, security policies are often applied after the WLAN has been deployed in response to an industry concern. Creating documented security policies in advance during the design phase of a WLAN is a much better strategy. If the security team is the sole developer of a security policy, management and other departments may not want to subscribe to the defined policies. If the policies are not relevant or are too restrictive, they are likely to be ignored. Therefore, the first task in policy development must be to assemble a committee that will begin the construction of a relevant and usable policy. This group should include representatives from each group of stakeholders within the organization. The *stakeholders* are part of the applicable audience that should be involved in creating the policies to which they must abide. Everyone must endorse the security policy for it to be effective. Having such an endorsement requires an executive-level champion. Often a "C"-level executive is needed to get the ball rolling. The CEO, CIO, CTO, or CSO usually champions the cause so that the policy has the energy to move forward. Here are some of the departments that should be represented in policy creation:

- Security
- Legal
- Human Resources
- Management
- Networking
- Desktop Support
- Finance
- Users
- Research and Development
- Any group using the technology covered by the policy

Once the policy creation team is assembled, the next step is to define the scope of the policy. It is important to determine and specify whether you are creating a general policy or a functional policy. While a general policy establishes a framework for enforcement, a functional policy defines technical aspects of security. WLAN functional policies will be discussed in greater detail later in this chapter.

When building a general policy, you should look for existing written policies first and attempt to see if they are applicable and determine if they are being followed and enforced. If there is a written policy, you may only need to adapt it to current business and security needs or just ensure it is being adhered to and enforced. If there is no written policy, you will need to start from scratch, which, in some instances, may be an easier task than adjusting an existing policy. The WLAN may also fall under an industry or governmental network security regulation that does not apply to the wired infrastructure. Government and industry regulations will also be discussed in greater detail later in this chapter. Defining the applicable audience that must abide by this policy is critical. Obviously, all employees will have to abide by policy, but contractors and temporary workers are often overlooked.

With the policy development team assembled and the scope of the policy defined, you are ready to start building and documenting your policy. A large part of general policy creation is risk assessment. Risk assessment involves determining what assets are at risk, as well as the value of the assets that need protection. Often the value of the asset being protected will determine the security measures that are needed. Assets such as corporate trade secrets and credit card databases require the strongest security available. Threat analysis is also a form of risk assessment. Determining in advance what potential WLAN security threats exist will help determine the risk due to a successful WLAN attack occuring. For example, how much would it cost the company if an intruder used a rogue AP to access the customer credit card database? What would the potential legal liability be to the company if employee healthcare records were illegally accessed? What would it cost the company if a denial-of-service attack prevented the sales team from accessing email for four hours? If a specific dollar value can be assigned to these types of potential threats, better decisions can be made when choosing the proper WLAN security solution, and better policies can be written. Furthermore, if threat analysis and risk assessment can be used to determine financial impact, it will be easier to convince management to budget for needed security solutions. Even more importantly, management is more likely to endorse the enforcement of policy if they understand and are aware of the potential financial impact of a breach in security.

The final phase of policy deployment is policy communication. This involves making sure that all of the users are aware of the policies, understand them, and realize they must comply with them. This goal can be reached using several methods. Documentation of the policy must exist to eliminate confusion and to provide reference should points of clarity be required. Users need to be trained to understand and abide by security policies. This is one of the reasons why user representation in policy creation is so important. If the users are not trained on policy conformity or do not buy into the policy, it will not be followed. A formal training class regarding policy is usually necessary and highly recommended. After training, users must be required to read the corporate security policy and sign a document stating that they have read and understand it.

Many organizations make the mistake of creating policy documents that are too technical, hard to read, and hard to understand. The policy document should be written in a straightforward manner that all employees can comprehend. Another mistake often made within an organization is that employees read the security policy document, sign the document, and never see it again. The policy document will often change; therefore, it should be thought of as a living and breathing document. Many companies store the security policy document on a public share on a corporate server, and then link to the document from a desktop icon on every employee's computer. A desktop icon allows the employees to read and reference the security document whenever necessary. The lengths you go to in policy communication may vary by user, department, or organization. The key aspects of building an effective policy are that the policy should be relevant, include both internal and external requirements, and be properly documented.

Policy Management

The management of security policy is a crucial part of an effective security solution. Policy management includes policy adaptation as well as compliance monitoring, security audits, and policy enforcement. Any policy that is not enforced is not effective. Policies are also not effective when they become obsolete. As mentioned earlier, the policy document needs to be a living document that is adaptable to new business requirements and advances in technology. Knowing the requirements and monitoring for compliance allows security staff members to identify devices or communications that fall outside the policy. When such situations are located, they can be corrected — hopefully before a security incidence occurs. Should new technology be incorporated into your network, the general policy may cover it. However, functional policy for the newer technology may not exist. By monitoring policy, holes such as these can be identified, documented, and included in the next revision of the policy, or may prompt a specific policy created for its use. As new threats arise, a policy can be augmented to address the threats. It is important to realize that both internal and external changes can drive the need to update the security policy.

Many organizations have a specific monetary value defined for every minute of downtime faced by the network. Downtime can be caused by hardware failure, improper configuration, firmware issues, software glitches, or security problems. Many organizations strive for 99.999 percent uptime. Unmanaged security policies, or those that are too restrictive due to failure to adapt to business requirements, can cause downtime. Those that fail to comply with external requirements, industry or governmental, could result in networks being shut down until compliance is reached. This could also result in fines or a loss of assets due to noncompliance. As external mandates change, the network security policy must also change. The loss of money or time due to noncompliance is, essentially, a loss of corporate assets, although not via an attack. Policy management involves monitoring for compliance, both internal and external.

Policy management may also include security audits and penetration testing. In Chapter 9, "Wireless LAN Security Auditing," you learned about many of the tools and procedures needed to perform a successful audit. Penetration testing and audits will assist the security staff in determining compliance with corporate policy, as well as finding oversights in the policies, or identifying areas for improvements based on newer technologies or methods. Before conducting a security audit, or identifying penetration test, consult the written policies to help ensure that your actions are covered within corporate guidelines. Internal corporate audits should be conducted on a regular basis. Consideration should be given to hiring a third-party to perform penetration tests and audits. Third-party audits often reveal security flaws that were missed by the organization.

Policy management also includes the area of enforcement. As mentioned earlier, if policies are not enforced, they become meaningless. General policy should outline procedures to be taken if there are policy violations. Actions taken after a policy violation usually depend on the value of what was lost or compromised. An employee who violates security policy at a nuclear power plant will probably get fired, while an employee who violates policy at a retail store might just be retrained. Policy enforcement as well as reporting of violations are often hampered by the following:

- Lack of corporate standards and documentation
- Ineffective or missing management support
- Nonuniform enforcement
- No client-side enforcement
- Lack of education about risks
- Regulation compliance
- Deployment management
- Cost (this is a big one)

All policy violations and subsequent actions must be accurately documented to meet compliance with many government regulations. Documentation of policy violations is also important for liability reasons and may even be needed in case law enforcement gets involved.

Functional Policy

General policies are the framework from which functional policies are derived. A *functional policy* is required to define the technical aspects of wireless security. The functional security policy establishes how to implement and secure the wireless network, defining what solutions and actions are needed. A functional wireless security policy will at a minimum define the following items:

Policy Essentials Defines basic security procedures such as password policies, training, and proper use of the wireless network.

Baseline Practices Defines minimum wireless security practices such as configuration checklists, staging and testing procedures, and so on.

Design and Implementation Defines the actual authentication, encryption, and segmentation solutions that are to be put in place.

Monitoring and Response Defines all wireless intrusion detection procedures and the appropriate responses to alarms.

Sample WLAN Policy Document

You can find an example of a WLAN security and compliance policy document on the CD that accompanies this book. The document, `WLAN_Policy_Sample_Template.pdf`, can be used as a template to create your own WLAN security policy.

Password Policy

Functional policies should include a password policy. This policy should state the length, complexity, and age limits of passwords used in authentication, in addition to simply requiring a password. Where possible, systems should be configured to enforce the password policies, and not allow users to authenticate with weak or noncompliant passwords. Users should also be forced to change their password upon first login. This prevents administrators from knowing the users' password beyond the initial account creation. The complexity and length of the password is derived from a delicate balance of difficulty to guess (or brute force the password), and ease of remembrance. If the password is too simple or too short, it is easily guessed or cracked. If it is too long or too complex, users may forget them or write them down near their work area. This could allow someone to easily find the password and use it to gain access to network resources beyond their approved access. Additional authentication measures may also be required beyond passwords to improve security, such as multifactor security measures. These measures take into account usernames and passwords (what you know), token devices or client certificates (what you have), biometrics (who you are), and RFID tags (where you are). Some of these measures include:

- Certificate usage
- Smart card usage
- Fingerprint scan
- Retina scan
- Voice recognition
- Facial recognition
- Real-time location systems (RTLS)

As basic as it seems, the policy should also include a statement prohibiting users from disclosing their passwords to others. Often an employee or contractor may need to use the station of their coworker, and request the coworker's credentials to log in. This practice should be prohibited, as should the user logging in and allowing others to use their system.

The section "Entropy" in Chapter 6, "SOHO 802.11 Security," is extremely important when considering password policy. In digital communications, *entropy* is a measure of uncertainty associated with a random variable.

A base password complexity and length that is commonly used is a password of at least eight characters in length, at least one uppercase letter, at least one lowercase letter, at least one number, and at least one special character. For example, 8H4pT@b$ would meet the criteria of an eight-character strong password. Resources within an organization may require additional complexity or length to be more secure. Some organizations require users to maintain separate credentials for each resource. As you learned in Chapter 4,

"Enterprise 802.11 Layer 2 Authentication Methods," most organizations synchronize user passwords across resources but use centralized authentication solutions, such as *Lightweight Directory Access Protocol (LDAP)* and/or *Remote Authentication Dial-In User Service (RADIUS),* in addition to complex password requirements. The length, complexity, and age of passwords should all be spelled out in a functional policy, and followed to reach the desired security level.

Numerous freeware tools exist that can be used to assist end-users with creating strong passwords. One example is Juniper Networks' Password Amplifier utility. Password Amplifier can be downloaded from `www.juniper.net/customers/support/products/aaa_802/oac_demo.jsp`.

RBAC Policy

In Chapter 12, "Wireless Security Infrastructure," you learned about the technical aspects of *role-based access control (RBAC),* which is a method of providing or restricting WLAN access based upon the identity of the user. Every user has his or her own job and should have access to the appropriate resources to do that job. To that end, users should all have their own accounts and credentials. This helps in building nonrepudiation into network activities. Granting access to resources beyond those required by users to do their job is a security hole. RBAC helps ensure that networking resources can only be accessed by users with permission to do so.

Written RBAC policies should be clearly defined, specifying what groups of users get to access which network resources. People who need to do the same tasks usually require access to the same resources. By placing users into groups related to their job functions and assigning resource permissions to their groups, administration is an easier task and security is enhanced due to RBAC. As a user moves from job to job within an organization, permissions are easily assigned by moving the user's account into and out of the appropriate groups. If written RBAC policies are clearly defined, the RBAC technical implementations will be better planned and deployed.

Change Control Policy

Periodically, vendors release firmware and software updates to improve functionality of their products or to correct errant releases of their products. A good functional policy will include *change control* procedures governing the upgrading or downgrading of firmware and software, as well as for performing hardware maintenance. Change control processes help to ensure that changes to a product or system are introduced in a controlled and coordinated manner. Additionally, they should reduce the possibility that unnecessary changes are brought

into a system, which could introduce problems or undo required changes made by other users. Change control policy usually includes procedures to minimize disruption to services, reduce back-out activities, and provide for cost-effective utilization of resources, while adhering to the security policy. Changing firmware or software may open security holes that were not there before. Things such as sockets or ports that were used by a previous version may not be used by the currently installed version and may not have been checked or secured when the security baseline was created. Just because the newer version is compatible with everything else running on the device does not mean it meets the security requirements within your policies. Even when the objective of the changes are to meet security requirements, the changes must still be covered under written policy to help protect assets.

In addition to including a mandated change control process in your policies, you must also include monitoring and inspection of devices to make certain that required firmware and software is installed. You should also include statements covering the installation of unapproved software, such as freeware or user-purchased software. In large environments, adhering to a change control process helps to ensure uniformity of deployment. However, some devices can still be missed. Within the auditing statements of your security policy, you should include a mandate that software and firmware be at the required version level. An auditing requirement may also be included within a general policy or any policy covering risk assessment. Auditing is often required by an external regulation or industry policy. Devices missing patches are often exposed to attackers. When a vendor releases a security patch, attackers know where holes may be in unpatched systems, if they did not already know about them. Your policies may require that security patches be installed within a given period of time from their release. Once new software or firmware is installed, a new security baseline should be established and documented.

Whenever WLAN infrastructure is deployed, or changes to configurations are made, all settings should be documented. The encryption, authentication, RBAC, and VLAN settings for APs and WLAN controllers should always be documented and validated with checklists.

Authentication and Encryption Policy

Throughout this book, you have learned about enterprise solutions that are used to protect the WLAN portal. Many of these solutions only authorize network resource access for users who have had their credentials properly validated. Whenever possible, a functional policy mandating the use of 802.1X/EAP authentication should be used. Consideration should also be given to mandate the use of two-factor authentication solutions before access is granted. Handheld devices like VoWiFi phones may need to use weaker authentication solutions, such as WPA2-Personal, until 802.11r (fast BSS transition) mechanisms are widely supported. Guest networks should use captive portal authentication for liability and auditing purposes.

You have also learned about the many available enterprise encryption solutions that are used to provide data privacy for the Layer 3–7 payload of 802.11 data frames. Whenever possible, dynamic CCMP/AES encryption should be used. Dynamic TKIP encryption may be acceptable in many cases, but will not be acceptable in most government institutions that mandate FIPS 140-2 compliance. Static WEP encryption should be avoided at all costs.

WLAN Monitoring Policy

The WLAN should be monitored by a WIDS/WIPS solution for any compromise or attack of the WLAN, including rogue devices, ad hoc clients, and DoS attacks. Functional policy should define what steps should be taken when a breach is detected by the WIDS/WIPS solution. For example, will the WIPS be used to perform automatic or manual rogue containment? What action will be taken if a Layer 1 DoS attack is detected? What thresholds will be set for WIPS alarms, and how will the WIPS administrator be alerted to alarms? As you learned in Chapter 10, "Wireless Security Monitoring," a WIPS can also be used to help enforce certain functional policies. For example, the WIPS may detect authorized WLAN clients with improperly configured security settings. The WIPS also may be used to contain or blacklist improperly configured client stations and effectively enforce encryption and authentication functional policies.

Endpoint Policy

It is likely that end-user client stations will leave a company's controlled environment and operate outside of the area monitored by the WIPS. Employees will use access points that do not meet the corporate encryption and authentication policies. It is almost a certainty that employees will use company laptops to access the Internet at Wi-Fi hotspots and other public-access WLANs. Therefore, organizations must also implement an *endpoint policy* that governs the security of all client stations. While some devices such as VoWiFi phones and barcode scanners may never leave the corporate facilities, employee laptops and PDAs are coming and going every day. When end-users are at off-site locations, these devices are associating to other non-company WLANs and therefore are not able to be monitored by the company WIPS.

Throughout this book, we have discussed the reasons and solutions needed for enterprise WLAN infrastructure security, with the goal of protecting corporate assets from attackers. One of the most important facts that a WLAN security professional should always remember is that the greatest WLAN security risks will always exist off-site. The only security that Wi-Fi hotspots and public-access WLANs usually have is a captive portal. There is no provided encryption solution, and any client station is exposed to the majority of the WLAN security risks that were discussed in Chapter 8, "Wireless Security Risks." Hotspots are breeding grounds for peer-to-peer attacks, Wi-Fi phishing attacks, data theft or manipulation, eavesdropping attacks, and other malicious events. Always remember that WLAN hackers lurk at Wi-Fi hotspots.

> The use of wireless LANs and mobile workforce is on the rise; so is sophistication of wireless threats and attacks. Mobile users could get duped by hackers phishing for credentials or other sensitive information at hotspots and must be protected.
>
> *GARTNER - NOVEMBER 2002*

Endpoint security measures within both general and functional policies should always be considered mandatory. At a minimum, the functional policy should mandate the use of a personal firewall and an IPsec VPN client solution. The personal firewall will protect client stations from peer-to-peer attacks. The IPsec VPN client will be used to establish an encrypted tunnel back to the corporate VPN server. The client's data will not only be protected across the Internet, but will also provide data privacy in the air at the Wi-Fi hotspot. Because there is no security at the Wi-Fi hotspot, it is imperative that the employee bring the security to the unprotected WLAN. Another key component that many organizations are starting to deploy is WLAN endpoint policy enforcement.

In Chapter 4, we recommended the use of third-party supplicants such as Juniper Networks' Odyssey Access Client (OAC). A third-party supplicant solution will cost more per-user, but should support almost any type of EAP protocol and work with just about any Wi-Fi device. The base OS supplicants such as Microsoft's Wireless Zero Configuration (WZC) have too many known security flaws. In addition to using a third-party supplicant, give heavy consideration to using endpoint policy enforcement software such as AirTight's SpectraGuard SAFE or Motorola's AirDefense Personal.

These WLAN endpoint software solutions allow the use of wireless connectivity to be controlled when the employee is not connecting to the company's network. Policies can be enforced using these tools that allow different behaviors on different WLANs. Ad hoc network connectivity can be disallowed. As shown in Figure 13.1, bridging between the WLAN network card and the Ethernet network card can be prevented by automatically disabling one of the interfaces if the other one becomes active. Essentially, these tools help enforce WLAN security policy when the station is beyond the control of the LAN administrator. WLAN policies that can be enforced with an endpoint solution include the following:

- Requiring specific WLAN encryption and authentication settings on the client side
- Preventing ad hoc connectivity
- Preventing bridging between wired and wireless network interfaces
- Enforcing VPNs
- Authorizing only certain SSIDs
- Blacklisting certain SSIDS

FIGURE 13.1 Endpoint security enforcement

As you can see in Figure 13.2, endpoint WLAN software solutions exist that force end-users to use VPN and firewall security when accessing any wireless network other than the corporate WLAN. If an employee connects to any SSID other than the corporate SSID, machine or user policy can require that a VPN tunnel be created within a given amount of time after a wireless connection is established. If the VPN tunnel is not established, the WLAN adaptor of the device will automatically disconnect. Client-side policy should also cover the use of ad hoc wireless networking. Unless devices have a legitimate requirement to connect directly to each other, ad hoc networks should be strictly forbidden by policy.

FIGURE 13.2 VPN enforcement

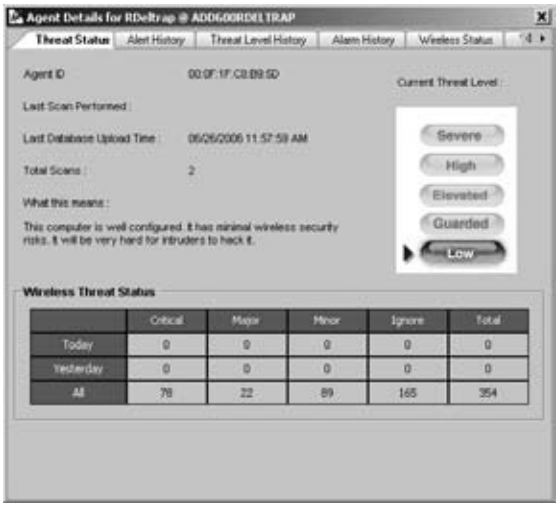
End-point security solutions also allow for centralized configuration of thousands of endpoints and provide centralized policy enforcement. There are two methods of endpoint security management:

End-User Accessible The end-user has full access and is responsible for configuring security policies and reacting to warnings or alerts.

End-User Restricted The end-user has no access to policy configuration. All security policies are defined by the WLAN security administrator.

Some endpoint software solutions can also be integrated to work with a centralized WIPS solution. As shown in Figure 13.3, data collected from the endpoints can be used by the network administrator to gain knowledge of the network usage patterns of mobile employees. The endpoint solution provides an audit trail for each WLAN client station. Endpoint client stations can also be automatically imported into a centralized WIPS as authorized devices, reducing the time it takes to classify client stations.

FIGURE 13.3 Endpoint audit trail



The use of endpoint security-focused software will increase the expense of using each WLAN device and is indeed another solution that will have to be managed by the WLAN security administrator. However, endpoint policy-enforcement software agents may be the only way to enforce device security, because end-users normally have administrative rights on their personal laptops. With administrative rights, users can connect to any unsecure WLAN, placing them at risk. A WLAN endpoint policy-enforcement software agent forces the end-user to abide by policy and prevents risky behaviors. Wireless security polices, like wireless itself, must extend beyond the walls of your organization.

Several vendors now offer endpoint WLAN policy-enforcement software agents. These agents can protect mobile users at hotspots and other public Wi-Fi networks from wireless-specific risks that could expose private data and transactions. One example of a policy enforcement solution is Motorola's AirDefense Personal. You can download a free copy of AirDefense Personal Lite at `www.airdefense.net/products/adpersonal/index.php`. Another example is AirTight Networks' SpectraGuard Security Agent For Endpoints (SAFE) solution. More information about SpectraGuard SAFE can be found at `www.airtightnetworks.com/home/products/spectraguard-safe.html`.

Acceptable Use Policy

The *acceptable use policy* defines the purpose of the WLAN and how the company employees may utilize the WLAN. The WLAN is obviously not to be used for illegal purposes and usually only for company activities. Acceptable use policies will also define what applications may be used over the WLAN. For example, the use of video streaming applications may not be allowed for employees. Certain types of downloading activities may also be banned because of the effect on throughput of the WLAN. The good news is that RBAC mechanisms, such as firewall restrictions and bandwidth throttling, can often be used to limit the activities of WLAN end-users and therefore enforce acceptable use policies.

Physical Security

The physical security policy will define how WLAN infrastructure will be protected from theft and vandalism. An attacker may also access the exposed ports of an unsecured AP to extract information about WLAN configuration settings. The location of all access points will be documented, and often the APs will be secured in indoor enclosure units that can be locked. Outdoor APs will also be secured in National Electrical Manufacturers Association (NEMA) enclosure units for protection from the weather. All WLAN controllers and servers should be secured in a data closet. Inventory and documentation of all client devices is also highly recommended.

Remote Office Policy

Given the widespread small office and home use of 802.11 wireless networks, the discussion of wireless security policy for the home and small office is worth having. To date, there are no regulations or industry standards focused on how to secure wireless home networks that are used for nonbusiness reasons. However, some laws, regulations, and standards apply to businesses no matter what the size, while others vary the requirements based on size of the business and the amount and type of information to be protected. Although the policy formation process may be less involved and the policy created less encompassing than required by an enterprise security solution, SOHO environments should also create and follow wireless security policies. Budgets and network size do not allow the same protections in SOHO environments as found in the enterprise. A small five-person office with only five laptops and one printer is not likely to install a WIPS for protection. There is no security team conducting daily audits in the SOHO environment. However, a small and medium business (SMB) office must comply with external policy influences just as a large corporation must comply. A great example would be a doctor's office having the need to be Health Insurance Portability and Accountability Act (HIPAA) compliant. HIPAA requires any needed access to patient data to be accomplished in a secure manner based on maintaining patient confidentiality. If the office uses wireless communications to transfer patient data, the office must take measures

to protect that data. A small collection agency may be required to meet Gramm-Leach-Bliley Act of 1999 (GLBA) compliance to continue to do business with their customers, putting a policy in place to protect the customers information from foreseeable security and data integrity threats. The Sarbanes-Oxley Act of 2002 (SOX) has a financial privacy rule that applies to companies receiving private financial information, whether or not they are financial institutions, requiring that anyone processing or storing such information must be SOX compliant. The business partner of a large corporation could have a small branch office that is insecure, potentially providing an attacker with an entrance into the network of the larger firm.

Securing your wireless network should be part of the design process, whether you are an office with a single remote AP or an enterprise with thousands of APs. Just as in the enterprise, SMB deployments should develop, follow, and adapt wireless security policies to protect the assets of the organization. If the business is not required to follow industry or governmental guidelines, a simple policy covering physical security, authentication, and encryption may suffice. However, if the SMB operates in business areas where regulations exist, the policy must take into account all the external policy influences as well as simple protection policies. The smaller deployment size of SOHO wireless networks in no way negates the need for security and written, followed, enforced, and adaptable wireless security policies.

Government and Industry Regulations

In most countries, mandated regulations exist, describing how to protect and secure data communications within all government agencies. In the United States, the National Institute of Technology and Standards (NIST) maintains the *Federal Information Processing Standards (FIPS)*. Of special interest to wireless security is the FIPS 140-2 standard, which defines security requirements for cryptography modules. The use of validated cryptographic modules is required by the US government for all unclassified communications. Other countries also recognize the FIPS 140-2 standard or have similar regulations. From government to healthcare, banking, or even energy sectors, more and more external regulations, laws, and standards are affecting how we use wireless networking. In this section, we will explore how some of the more widely known external mandates are directly influencing wireless use and how they should be incorporated into WLAN security policies. We will specifically examine the following as they pertain to the use of 802.11-based wireless devices:

- The US Department of Defense (DoD) Directive 8100.2
- The US Federal Information Processing Standards (FIPS 140-2)
- Sarbanes-Oxley Act (SOX)
- Graham-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry (PCI) Standard

Does the CWSP Exam Test the Specifics of Government and Industry Regulations?

The simple answer is no. The CWSP certification is recognized worldwide and the exam is available in many countries. All of the regulations discussed in the following sections are US government and industry regulations. This information is being provided strictly as reference material. It would not be practical to test a CWSP exam candidate in New Zealand about US government regulations. However, it should be noted that many countries have almost identical regulations for government and specific industries. A WLAN security professional in any country would be well advised to learn about all the applicable regulations as they apply to WLAN technology within any region.

The US Department of Defense (DoD) Directive 8100.2

On April 24, 2004, the US Department of Defense issued a directive covering the use of commercial wireless devices, services, and technologies within the Global Information Grid (GIG). This directive, titled the Department of Defense (DoD) Directive 8100.2, details the DoD policy for the secure use of wireless networks and devices. It also includes policy statements requiring the monitoring of wireless devices that are deployed, and monitoring for wireless devices in areas that do not have authorized wireless deployments. Furthermore, this directive states that there are areas in which the use of wireless networking is banned. The policy covers both authorized and banned wireless usage.

In accordance with any good wireless security policy, the DoD revisits this policy and makes needed adjustments as technology changes. In June 2006, the DoD issued a supplement to the 2004 directive. The goal of the supplement was to allow the embracing of technologies from open standards–based solutions while providing a framework from within which this can be done securely. This supplemental policy applies to 802.11-based communications and devices, but does not cover cellular, Worldwide Interoperability for Microwave Access (WiMAX), Bluetooth, or proprietary RF communication mechanisms. Directive 8100.2 applies to all DoD components, military and civilian alike. It covers any personal electronic devices, laptops, PDAs, cell phones, and so on, which are able to process, store, or transmit information wirelessly. The policy requires that heads of departments, in addition to performing other security tasks, do the following:

- Ensure that all WLAN procurements comply with the set policies starting in FY 2007.
- Submit to the DoD CIO within 180 days specific migration plans for legacy systems.
- Ensure interoperability through standards-based products.
- Prepare and execute incident response plans for wireless intrusion detection.

All components parts of the DoD must ensure that devices are certified and validated under DoD regulations for interoperability and that there is secure end-to-end communications. The June 2, 2006, supplement requires the following measures be taken:

- All cryptographic functionality must meet, at a minimum, NIST FIPS 140-2 level one validation.
- All WLAN devices deployed must be National Information Assurance Partnership (NIAP) Common Criteria Certified.
- WLAN devices must be certified by the Wi-Fi Alliance and be WPA2 certified.
- Personal electronic devices, laptops, PDAs, and so forth must use a NIAP Common Criteria Certified Personal Firewall and Antivirus.

In addition to these requirements, by fiscal year 2007, all portions of the DoD components were required to implement WLAN solutions that are IEEE 802.11i compliant and are WPA2 Enterprise certified. The policy also mandates that they implement 802.1X access control with EAP-TLS mutual authentication and a configuration that ensures exclusive use of FIPS 140-2 (minimum overall Level 1) validated AES-CCMP encrypted transmissions. The 2006 supplemental policy also requires the use of wireless intrusion detection systems (WIDS), something not included in the original 8100.2 directive. Some components of the DoD have included wireless intrusion prevention systems (WIPS) in addition to basic WIDS functionality. The 2006 addition states that:

- WIDS are required for all DoD wired and wireless networks.
- WIDS must continually scan for and detect both authorized and unauthorized devices. Continually scanning is defined as 24/7 monitoring.
- WIDS must also have location tracking capability.
- WIDS must be validated under NIAP Common Criteria Certification.

The DoD has well-defined policies at both the general and functional policy levels. Given that users within the DoD travel the globe and may have access to high-priority data, the policies for their network may be too restrictive for some environments to the point of enforcing no wireless zones. Directive 8100.2 and its supplements address security beyond configuration. They mandate monitoring for wireless devices, even where none are deployed, and cover encryption, certification, and validation. Such high standards limit the hardware and software that can be used due to the level of compliance, certification, and validation required. So who must comply with DoD 8100.2? The answer is any DoD employee, contractor, or visitor to any DoD facility as well as any others who have access to DoD information.

DoD Commercial WLAN Technologies Instruction 8420.01

While this book was being written, the U.S. Department of Defense (DOD) released the instruction document 8420.01, which defines security measures for commercial wireless local area network (WLAN) devices, systems, and technologies. The 8420.01 instruction document can be downloaded at: www.dtic.mil/whs/directives/corres/pdf/842001p.pdf.

Federal Information Processing Standards (FIPS) 140-2

The Federal Information Processing Standards (FIPS) are issued by NIST. They were created in the United States under the Information Technology Management Reform Act (Public Law 104-106). The Secretary of Commerce approves the standards and guidelines that are developed by NIST. These standards are created by NIST when there is a specific need for security and/or interoperability, and there are no industry standards that meet the requirements. We will focus on only FIPS 140-2 compliance requirements as they relate to wireless communication. FIPS Publication 140-2 was released on May 25, 2001. It supersedes FIPS 140-1, which was released on January 11, 1994. FIPS 140-2 covers the federal requirements for cryptographic modules. Specifically, it covers the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information. Many businesses and individuals conducting operations with the US government and/or selling communication devices to the government must comply with this publication. FIPS 140-2 has increasing levels of requirements from level 1 to level 4. Each higher level must meet all of the lower-level requirements in addition to their own specifications. These mandates cover areas of both secure design and secure deployment of applications and communications. The appendices of this standard summarize the requirements and describe each of the four levels of requirements. Each of the four levels spell out their functional requirements. As FIPS 140-2 relates to cryptographic modules, the four levels are as follows:

Level 1 Security requirements are specified for a cryptographic module at this level. No specific physical security mechanisms are required in a Security Level 1 cryptographic module beyond the basic requirement for production-grade components. However, at least one Approved algorithm or Approved security function shall be used.

Level 2 Level 2 requires features that show evidence of tampering, including tamper-evident coatings or seals that must be broken to attain physical access to the plaintext cryptographic keys and critical security parameters (CSPs) within the module, or pick-resistant locks on covers or doors to protect against unauthorized physical access. (Many devices use painted screws, seals, or tamper-evident tape to meet this requirement.)

Level 3 Level 3 attempts to prevent the intruder from gaining access to critical security parameters (CSPs) held within the cryptographic module. Physical security mechanisms required at Security Level 3 are intended to have a high probability of detecting and responding to attempts at compromising the cryptographic module. The practice of erasing sensitive parameters such as keys from a cryptographic module to prevent their disclosure if the equipment is captured is known as *zeroization*. Physical security mechanisms may include the use of strong enclosures and tamper detection/response circuitry that zeroizes all plaintext CSPs when the removable covers/doors of the cryptographic module are opened.

Level 4 Level 4 provides the highest level of security. Here the physical security mechanisms have the intent of detecting and responding to all unauthorized attempts at physical access. Any compromise of the cryptographic module enclosure is most likely

going to be detected, resulting in the immediate zeroization of all plaintext CSPs. Level 4 cryptographic modules are important to use in physically unprotected environments. Level 4 also requires protection for a cryptographic module against compromise due to environmental conditions, such as temperature and power variations beyond normal operation. Cryptographic modules are required to include special environmental protection features designed to detect fluctuations and zeroize CSPs, or as an alternative undergo rigorous environmental failure testing providing reasonable assurance that the module will not be compromised by fluctuations outside of the normal operating range in a manner that can reduce or negate the security of the module at Level 4 certification.

So who must comply with FIPS 140-2? Just about all US government agencies must comply. The applicable audience for FIPS 140-2 is all federal agencies that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106. Any devices sold for deployment in these areas must meet this standard. Any systems, applications, or devices approved for classified transmissions can be substituted, since they comply with standards that exceed those mandated in FIPS 140-2. In simpler words, within any federal agency that handles data of sensitive nature, the computer network solution must be FIPS 140-2 compliant.

The standard also includes an implementation schedule, export rules, and contact information for valid interpretation of its content. Realizing that there may be a need for some exceptions, there is even a waiver process outlined to allow for exemptions if needed and justified. This applies to wireless communications and the associated devices used by anyone required to follow this standard. Even outside areas where FIPS compliance and certification is mandated, following these measures improves an organization's security posture. With all of the security measures spelled out in FIPS 140-2, it is easy to see why your organization may want to follow its guidelines. However, the most compelling reason to follow FIPS 140-2 is that it is a federal mandate. This mandate will continue to be adapted as technology changes, as evidenced by the expected publication of FIPS 140-3 in late 2009.

Information about the FIPS regulations can be found at `http://csrc.nist.gov/publications/fips`. A list of FIPS-compliant vendors, devices, and software can be found at `http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm`. A draft version of FIPS 140-3 can be also found at `http://csrc.nist.gov/publications/fips`.

The Sarbanes-Oxley Act of 2002 (SOX)

The Sarbanes-Oxley Act of 2002 (SOX) defines more stringent controls on corporate accounting and auditing procedures with a goal of corporate responsibility and enhanced financial disclosure. The act is named *Sarbanes-Oxley* after Senator Paul Sarbanes and Representative Michael Oxley, the key figures who drafted it in 2002. The legislation set new or enhanced standards for all U.S. public company boards, management, and public

accounting firms. Since SOX applies to publicly traded companies, it does not apply to privately held companies or those publicly traded companies that do not operate within the United States. The act contains 11 titles and multiple sections, ranging from additional corporate board responsibilities to criminal penalties, and it requires the Securities and Exchange Commission (SEC) to implement rulings on the requirements to comply with the new law. The two most relevant sections for a wireless security discussion are 302 and 404.

Section 302: Corporate Responsibility for Financial Reporting This section may be the best known one. It requires the CEO and CFO to certify that they have reviewed the financial reports, the information is complete and accurate, and effective disclosure controls and procedures are in place to ensure material information is made known to them. Section 302 of the Act mandates a set of internal procedures that ensure accurate financial disclosure.

Section 404: Management Assessment of Internal Controls This is a newer section with the following three basic requirements:

- Establishment of effective internal controls by corporate management for accurate and complete reporting
- Annual assessment by management of the effectiveness of internal controls supported by documented evidence
- Validation of management's assessment by a registered public accounting firm

SOX Section 404 does not specifically discuss information technology (IT) and the related security requirements. However, most financial reporting systems are heavily dependent on technology. The burden falls on the CIO and IT staff members to establish effective internal controls over the network and storage infrastructure supporting the financial reporting process. Businesses are increasingly implementing wireless networks to improve productivity and reduce costs. The introduction of wireless networking also brings new security challenges and reporting and monitoring requirements for those requiring SOX compliance.

SOX also created a quasi-public agency, the Public Company Accounting Oversight Board (PCAOB). The PCAOB has the responsibility of overseeing, regulating, inspecting, and disciplining accounting firms in their roles as auditors of public companies. Furthermore, SOX covers auditor independence, corporate governance, internal control assessment, and enhanced financial disclosure. The goal of SOX was to restore faith in publicly traded companies' reporting of earnings in the wake of several large trading scandals. The applicable audience for SOX is comprised of all public companies in the United States, international companies that have registered equity or debt securities with the SEC, and the accounting firms that provide auditing services to them.

Where does *information assurance* (IA) fit into SOX compliance? IA fits within SOX compliance in the following manner:

- SOX covers everything revolving around the confidentiality, availability, and (especially) integrity of financial data.
- SOX requires a recognized internal control framework.

- The Committee of Sponsoring Organizations (COSO) framework provides structured and comprehensive guidelines for implementing internal controls for SOX.
- The COSO recommended (but did not require) a framework by PCAOB.
- Five components of effective internal control are stipulated: Control Environment, Risk Assessment, Control Activities, Information & Communication, and Monitoring.
- The Control Objectives for Information and Related Technology (COBIT) framework, which was developed by the Information Systems Audit and Control Association (ISACA), bridges the gap between IT governance and SOX, and it addresses 34 IT processes that can all be mapped to COSO.

IA and IT fit within SOX under information security policies, network security, access controls, authentication, encryption, logging, monitoring and alerting, incident response and forensics, and IT audit. The secure implementation, use, and monitoring of wireless devices and networks clearly fits into these areas and therefore into SOX compliance.

Information about SOX can be found at `http://uscode.house.gov/download/pls/15C98.txt`.

The Financial Modernization Act of 1999 which is more commonly known as the *Gramm-Leach-Bliley Act (GLBA)* requires banks and financial institutions to notify customers of policies and practices disclosing customer information. The goal is to protect personal information such as credit card numbers, Social Security numbers, names, addresses, and so forth. There are five core requirements for GLBA:

- Designate employees for information security.
- Identify and assess all risks and safeguards.
- Design, implement, test, and monitor safeguard programs.
- Respond to security events, and remediate and adjust based on monitoring.
- Select appropriate service providers.

To these ends, GLBA gives authority to states and eight federal agencies to administer and enforce two rules: the Financial Privacy Rule and the Safeguards Rule. The applicable audience for these two regulations are financial institutions. This includes banks, securities firms, insurance companies, and companies providing several other types of financial products and services. These cover a wide range of services, including lending, brokering or servicing any type of consumer loan, transferring money, safeguarding money, preparing individual tax returns, providing financial advice, credit counseling, providing residential real estate settlement services, collecting consumer debts, and several other common financial services. Let's examine the two rules as well as discuss the concept of pretexting:

The Financial Privacy Rule This rule covers the collection and disclosure of any personal financial information by financial institutions. It also applies to companies receiving such information, whether or not they are financial institutions.

The Safeguards Rule This rule requires that all financial institutions design, implement, and maintain safeguards protecting customer information. This applies to financial

institutions that collect information from their own customers and any other financial institutions that receive customer information from other financial institutions, such as reporting agencies.

Pretexting There is also coverage of fraudulently obtaining personal information. Obtaining this information under false pretenses is called *pretexting*. Social engineering is often used to obtain the private information of others. Attackers solicit the data by using what appears to be a legitimate request.

Whether or not a financial institution discloses personal information, there must be a policy in place to protect the information from foreseeable threats in security and data integrity. Institutions must take reasonable protective measures to secure client data. This is a mandatory portion of GLBA compliance and also where wireless security comes into play. Maintaining data privacy is specifically covered in Title 5 of the Act, and has the following mandates covering data privacy:

- Requires clear disclosure to clients and others by all financial institutions of their privacy policy regarding the sharing of personal information with both affiliates and third parties.
- Requires a notice to consumers and an opportunity to opt-out of sharing of personal information with nonaffiliated third parties, subject to certain limited exceptions. (Clients often must notify the institution of their desire to opt-out.)
- Addresses a potential imbalance between the treatment of large financial services conglomerates and small banks by including an exception, subject to strict controls, for joint marketing arrangements between financial institutions. (Consumers often see the exemptions as additional offerings from the institutions partners.)
- Clarifies that the disclosure of a financial institution's privacy policy is required to take place at the time of establishing a customer relationship with a consumer and not less than annually during the continuation of such relationship. (This may only be done once a year or may be done as changes to the initial agreement are implemented.)
- Provides for a separate rather than joint rulemaking to protect client privacy; the relevant agencies are directed, however, to consult and coordinate with one another for purposes of assuring, to the maximum extent possible, that the regulations that each prescribes are consistent and comparable with those prescribed by the other agencies.
- Allows the functional regulators sufficient flexibility to prescribe necessary exceptions and clarifications to the prohibitions and requirements of section 502.
- Clarifies that the remedies described in section 505 are the exclusive remedies for violations of the subtitle.
- Clarifies that nothing in this title is intended to modify, limit, or supersede the operation of the Fair Credit Reporting Act.
- Extends the time period for completion of a study on financial institutions' information-sharing practices from 6 to 18 months from the date of enactment.

- Requires that rules for the disclosure of institutions' privacy policies must be issued by regulators within six months of the date of enactment. The rules will become effective six months after they are required to be prescribed unless the regulators specify a later date.
- Assigns authority for enforcing the privacy provisions to the Federal Trade Commission and the federal banking agencies, the National Credit Union Administration, and the Securities and Exchange Commission, according to their respective jurisdictions, and it provides for enforcement of the privacy provisions by the states.

Identity theft, or using the identity of another person fraudulently, is a crime that hurts society as a whole, undermining financial institutions and the economy alike. GLBA compliance helps reduce the occurrence of this crime by regulating the protection of personal information collected by financial institutions. As financial institutions, like many other conservative organizations, begin to introduce wireless networking, additional steps must be taken to protect private data. Wireless networks introduce additional entry points into financial institutions' networks that must be monitored and secured. Mandated followers of GLBA include

- Banks, thrifts, and credit unions
- Financial advisers/investment firms
- Insurance companies
- Credit card/financial transaction processing providers
- Consumer credit reporting agencies
- Front-end/back-end (core) providers and check printers
- Tax information preparers/processors
- Other service providers receiving customer information from financial institutions as regulated by the GLBA's Safeguards Rule

GLBA emphasizes that threats to information security are ever changing and describes them in general terms. Financial institutions must evaluate and adjust their information assurance programs to keep up with changes in technology, such as the increased use of Wi-Fi, and new or emerging threats that indicate they are vulnerable to attack or compromise.

More information about GLBA and identity theft can be found at these websites:

- `http://banking.senate.gov/docs/reports/s900sum.htm`
- `http://banking.senate.gov/conf/grmleach.htm`
- `www.usdoj.gov/criminal/fraud/websites/idtheft.html`

Health Insurance Portability and Accountability Act (HIPAA)

The *Health Insurance Portability and Accountability Act (HIPAA)* establishes national standards for electronic healthcare transactions and national standards for providers,

health insurance plans, and employers. The goal is to protect patient information and maintain privacy. One major goal of the *Privacy Rule* found in HIPAA is to assure that health information is properly protected while still allowing the flow of information about an individual's health needed to provide and promote high-quality healthcare as well as protecting the public's health and well-being. The Privacy Rule seeks a balance that permits important uses of information, while protecting the individual's privacy. Healthcare is a diverse industry. The Privacy Rule is designed to be flexible and comprehensive, allowing coverage of the large variety of uses and disclosures that need to be addressed within reasonable privacy.

The use of wireless technology has proven to be a method of delivering patient care that is faster for the patients and more convenient for the caregivers. However, this more timely delivery of care may introduce situations that are outside the industry's guiding privacy standard, HIPAA. Securing WLANs within the healthcare industry is critical. Interruptions in service can lead to life-threatening situations as well as data compromise. Electronic patient records make much of the behind-the-scenes work done by doctors, nurses, and other healthcare professionals an easier task. Multidimensional bar codes on drugs and arm bands allow caregivers rapid access to life-saving information. Unlike many other enterprise environments, hospitals have many areas of physical public access that also have access to data ports such as the patient rooms. The use of wireless networking increases this risk to care and patient data privacy.

The applicable audience for the Privacy Rule, as well as all the administrative simplification rules, are health plans, healthcare clearinghouses, and any healthcare provider that transmits health information in electronic form in connection with transactions for which the Secretary of Health and Human Services (HHS) has adopted standards under HIPAA. The electronic transfer of health information includes wireless transmissions. Under section 164.530(i), HIPAA requires covered entities to develop and implement written privacy policies and procedures that are consistent with the Privacy Rule. They must also assign a person to oversee the procedure for receiving complaints about their privacy procedures and to provide individuals with information about the procedures upon request. The two largest sections that pertain to wireless as well as networking in general are as follows:

Mitigation Covered entities must reduce the effect of any loss of private data, to the extent practicable, and any harmful effect it learns was caused by use or disclosure of protected health information. This loss could have been caused by its own workforce or its business associates in violation of its privacy policies and procedures or the Privacy Rule.

Data Safeguards Covered entities must maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent compromise of protected health information in violation of the Privacy Rule. Covered entities must also limit their incidental use and disclosure pursuant to otherwise permitted or required use or disclosure.

HIPAA allows each organization to determine the appropriate measures they must take to secure private information. This is largely due to the variation in healthcare areas. Both large and small organizations determine how best to meet the requirements of HIPAA.

Therefore, there is no specified format for compliance. In general, covered entities must do the following:

- Put in place administrative safeguards to manage the selection and execution of security measures chosen.
- Ensure physical safeguards are in place protecting electronic systems, buildings, and the equipment used from environmental and unauthorized intrusions that may compromise private data.
- Make certain that technical safeguards are in place, including automated processes to control access to private data and to protect private data.
- Conduct risk assessments and document security policies and procedures.
- Covered entities must have a device, such as a firewall, to screen traffic from the Internet.

Accountability is a great area to look for a wireless fit in HIPAA when trying to ensure your organization's compliance. The Privacy Rule has the foundation for accountability within an electronic health information exchange environment. It requires all covered entities involved in the exchange of protected health information, on paper or electronically, to comply with the administrative requirements of HIPAA and to extend these obligations to all business associates. The Privacy Rule promotes this accountability with established mechanisms addressing potential noncompliance. The Privacy Rule has standards, through a covered entity's voluntary compliance, a resolution agreement, and a corrective action plan, or the imposition of civil money penalties ranging from $100 to $50,000 or higher per incident.

More information about HIPAA can be found at these websites:

- `www.hhs.gov/ocr/hipaa`
- `www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html`
- `www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm`

Payment Card Industry (PCI) Standard

As more of us continue to rely on credit cards as our primary method of payment, more of us risk losing our card numbers to attackers and identity thieves through unsecure processing and/or storing of our cardholder information. The Payment Card Industry (PCI) realizes that in order to sustain continued business growth, measures must be taken to protect customer data and card numbers. The PCI Security Standards Council (SSC) has implemented regulations for those processing and storing cardholder information. This is commonly referred to as the *Payment Card Industry (PCI) Standard*. Within this standard are components governing the use of wireless devices.

As a further explanation of PCI requirements governing wireless devices, the information supplement PCI Data Security Standard (DSS) Wireless Guideline was prepared by the PCI SSC Wireless Special Interest Group (SIG) Implementation Team and released in July 2009. The PCI standards cover many aspects of credit card use, acceptance, and processing. This

standard is designed to protect the cardholder data environment (CDE). The CDE is defined as the computer environment wherein cardholder data is transferred, processed, or stored, and any networks or devices directly connected to that environment.

Let's focus on the PCI implications of wireless networking and device use. The PCI DSS wireless requirements can be broken down into two main categories: (1) generally applicable wireless requirements and (2) requirements applicable for in-scope wireless networks. They cover protection against rogue devices and protection of networks storing or processing cardholder data.

What does PCI DSS call a rogue AP? A *rogue AP* is any device that adds an unauthorized (and therefore unmanaged and unsecured) WLAN to the organization's network. This rogue device need not be placed by an attacker. In this context, a rogue AP could be added by inserting a WLAN card into a back-office server, attaching an unknown WLAN router to the network, or by various other means. Most rogue devices are placed by internal sources, often just trying to be more productive.

There is also provision for legitimate wireless use on the same network as the CDE. If an organization decides to deploy a WLAN for any purpose and connects the WLAN to the CDE, that WLAN becomes part of the CDE and is therefore within the scope of the PCI DSS and must comply with the PCI guidelines for wireless device use. If an organization deploys a WLAN that in no way touches the network that is part of the CDE, then that WLAN is out of the scope of the PCI DSS. However, should that WLAN touch the firewall that is connected to the CDE, the firewall then falls into the scope of PCI DSS. Roughly, any network that processes or stores cardholder information or any network, wired or wireless, that touches the CDE must be PCI DSS compliant. PCI DSS requires that wireless networks that do not store, process, or transmit cardholder data must be isolated from the CDE using a firewall. Any organization required to comply with PCI standards using WLANs that do not touch the CDE must also be able to prove that there is no connectivity from the WLANs to the CDE.

Specifically the two main areas of PCI covering wireless devices state the following:

Generally Applicable Wireless Requirements All organizations that wish to comply with PCI DSS should have in place methods to protect their networks from attacks via rogue or unknown wireless access points (APs) and clients. They apply to organizations regardless of their use of wireless technology and regardless of whether the wireless technology is a part of the CDE.

Requirements Applicable for In-Scope Wireless Networks All these requirements apply in addition to the universally applicable set of requirements. All organizations that wish to comply with PCI DSS that transmit payment card information over wireless technology should have in place mechanisms to protect those systems. These requirements are specific to the usage of wireless technology that is in scope for PCI DSS compliance.

Organizations that must comply with the PCI standard must also maintain an inventory of devices. It is recommended that such organizations scan for wireless devices to keep an up-to-date listing of all known WLAN devices, making rogue detection easier. PCI standard section 11.1 states that organizations must test for the presence of wireless APs by using a wireless analyzer at least quarterly or by deploying a WIDS/WIPS to identify all wireless devices in use. This means that every location, retail outlet, warehouse, office, and so on that stores or processes cardholder information be scanned each quarter or have a WIDS/

WIPS deployed to scan for them. Since travel to thousands of locations of a large retailer, for example, is time consuming and expensive, many organizations have come to rely on the scanning and protection offered by WIPS. Section 12.9 states that there must also be an incidence response plan that is followed should a rogue device be detected. This is another compliance requirement that can be automated by an effective WIPS deployment.

The PCI Security Standards Council recommends the following with regard to rogue wireless devices and PCI compliance:

- Use a wireless analyzer or a wireless IDS/IPS at least quarterly at all locations to detect unauthorized/rogue wireless devices that could be connected to the CDE. For large organizations having several CDE locations, a centrally managed wireless IDS/IPS to detect and contain unauthorized/rogue wireless devices is recommended.
- Enable automatic alerts and containment mechanisms on the wireless IPS to eliminate rogues and unauthorized wireless connections into the CDE.
- Create an incident response plan to physically eliminate rogue devices immediately from the CDE in accordance with PCI DSS requirement 12.9.5.

Section 1.2.3 requires that organizations install perimeter firewalls between any wireless networks and the CDE. These firewalls must be configured to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment going into or leaving the CDE. These firewalls are required to be audited at least every six months. This section also states that the reliance on VLAN protection of the CDE alone is not sufficient. To reduce the risk to the CDE, any protocol or traffic that is not necessary in the processing or storing of credit card transactions or cardholder data should be blocked. To this end, the PCI Security Standards Council recommends the following practices for firewalls:

- Use a stateful packet inspection firewall to block wireless traffic from entering the CDE. Augment the firewall with a WIDS/WIPS.
- Do not use VLAN-based segmentation with MAC address filters for segmenting wireless networks.
- Monitor firewall logs daily and verify firewall rules at least once every six months.

PCI DSS compliance for networks that include WLANs as a part of the CDE require extra attention to WLAN-specific technologies and processes such as the following:

- Physical security of wireless devices
- Changing of default passwords and settings on wireless devices
- Logging of wireless access and intrusion prevention
- Strong wireless authentication and encryption
- Use of strong cryptography and security protocols
- Development and enforcement of wireless usage policies

Many older devices and WLANs touching or used by the CDE have been using WEP for security. Under PCI compliance, new wireless implementations were prohibited from implementing WEP after March 31, 2009. PCI compliance further requires that WEP not be used and stronger security be in place on any network touching the CDE by the end of

June 2010. This mandate means that many wireless devices will need to be upgraded or replaced to maintain PCI compliance for the organization. The PCI Security Standards Council recommends the following practices for WLANs and APs:

- Enable WPA or WPA2, and make sure that default PSKs are changed. Enterprise mode is recommended.
- Disable SNMP access to remote APs if possible. If not, change default SNMP passwords and use SNMPv3 with authentication and privacy enabled.
- Do not advertise organization names in the SSID broadcast.
- Synchronize the APs' clocks to be the same as other networking equipment used by the organization.
- Disable all unnecessary applications, ports, and protocols.
- WPA or WPA2 Enterprise mode with 802.1X authentication and AES encryption is recommended for WLAN networks.
- It is recommended that WPA2-Personal mode be used with a minimum 13-character random passphrase and AES encryption.
- Preshared Keys should be changed on a regular basis.
- Centralized management systems that can control and configure distributed wireless networks are recommended.
- The use of WEP in the CDE is prohibited for all deployments after June 30, 2010.

The PCI requirements are much more specific than other industry standards covering wireless device use. For example, section 12.3 requires organizations to develop usage policies for critical employee-facing technologies to define proper use of these technologies for all employees and contractors. This requirement covers PDAs, remote-access technologies, wireless technologies, removable electronic media (such as USB drives, laptops, and personal data/digital assistants [PDAs]), email usage, and Internet usage.

The PCI standard has many more wireless requirements than most other external influences. This is largely due to the widespread use of wireless devices in networks touching the CDE. There have been several large losses of cardholder information. One of the largest and most publicly known losses involved wireless devices. As technology continues to drive business efforts, look for even more regulation covering the use of electronic devices and communication, especially wireless networking due to its unbounded nature. Keep in mind that where there is something of value that can be stolen, such as the data in the CDE, attackers are more likely to exist. Being compliant is not always the same as being secure. However, the newer PCI guidelines are forcing those that process payment cards or store cardholder information to create safer environments for the data they use and store as part of meeting that compliance.

More information about the PCI standard can be found at these websites:

- `www.pcisecuritystandards.org/`
- `www.pcisecuritystandards.org/pdfs/PCI_DSS_Wireless_Guidelines.pdf`
- `www.networkworld.com/onlineresources.html?fid=50131915&s=Source`

Real World Scenario

Compliance in the Air?

Beyond the legal compliance requirements and regulations airlines face each day so that they can carry passengers and cargo, they must also face many of the same external policy influences that other industries face. For example, if they are publicly traded, they must comply with SOX mandates. Various components of airlines must comply with several external standards and regulations. In recent months, numerous airlines have begun to offer Wi-Fi hotspots on many flights. The hotspots are fee-based Internet connections. To collect the fees, the hotspots use captive portals, often outsourced to hotspot providers. Now in addition to being able to use your credit card in flight to buy drinks, food, phone calls, or items from the duty-free shop, you can use your credit card to pay for hotspot usage.

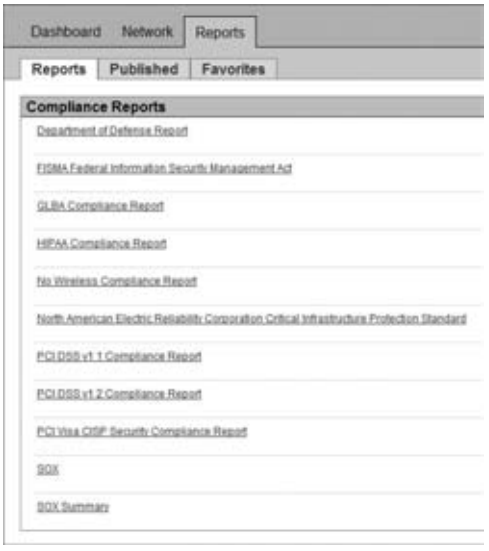
Airlines are definitely part of the applicable audience for the Payment Card Industry (PCI) standard, since they accept credit cards. The PCI standard requires several things to maintain compliance; among these is scanning for rogue devices in areas that process, transmit, or store cardholder information. PCI also requires the classification of neighboring devices. Since airplanes are mobile and thousands of feet or meters above ground level, how are the airlines maintaining compliance with the PCI standard? Simply turning the APs on and off at 10,000 feet (3,048 meters) does not meet compliance. As the role of the PCI standard expands, and as the standard is truly enforced, are airlines going to be required to have flight crews conduct periodic in-flight scans using laptops or handheld scanners? Are they going to be required to install WIPSs in all aircraft offering Wi-Fi hotspots or using wireless devices such as handheld scanners and handheld wireless credit card approval devices? If they are, how are the sensors going to report to their controllers? Currently available sensors do not have enough memory to conduct, store, and forward data upon landing, especially on flights of enough length to make Internet usage attractive to travelers. Could this mean that each aircraft must have installed onboard some sort of WIPS controller as well as sensors? The sensors will need to use the same satellite connections the APs use to connect to the controller over the Internet. Sensors can phone home over the Internet now. Even if Wi-Fi is not offered on the planes, cardholder information is processed, transmitted, and stored onboard. For aircraft to be compliant, they must be scanned.

Taking our example back to earth, will *any* hotspot that accepts credit cards as payment need to scan and protect its own WLAN to remain PCI compliant? An aircraft or any other network or hotspot, in terms of touching the CDE, should be treated no differently than a kiosk at the mall, a vendor stand at a concert processing the data, or the largest of retailers. Compliance with policies, both internal and external, reaches well beyond the walls of corporate headquarters. Compliance often drives some level of security. However, remember that being in compliance and being secure are more often than not two separate things.

Compliance Reports

Many WIPS solutions and other WLAN auditing software tools have the capability of analyzing existing WLANs and generating industry-specific compliance reports, as shown in Figure 13.4. These compliance reports can be helpful when identifying areas in need of improvement. Furthermore, industry-specific compliance reports can be useful when writing WLAN policies.

FIGURE 13.4 Compliance reporting



Examples of WIPS-generated compliance reports are included on the CD that comes with this book. The reports are titled `GBLA_Report.pdf`, `HIPPA_Report.pdf`, `SOX_Report.pdf`, and `PCI_Report.pdf`.

802.11 WLAN Policy Recommendations

Although a detailed and thorough policy document should be created for every organization's deployment of wireless technology, we highly recommend these five wireless security policies:

Remote-Access WLAN Policy End-users will be taking their laptops and handheld devices off site and away from company grounds. Most users will likely use wireless networks at home and at wireless hotspots to access the Internet. By design, many of these

remote wireless networks have absolutely no security in place, and it is imperative that a remote-access WLAN policy be strictly enforced. This policy should include the required use of an IPsec VPN solution to provide device authentication, user authentication, and strong encryption of all wireless data traffic. Hotspots are prime targets for malicious eavesdropping attacks. Personal firewalls should also be installed on all remote computers. Personal firewalls will not prevent hijacking attacks or peer-to-peer attacks, but will prevent attackers from accessing most critical information. As you have learned, endpoint WLAN policy enforcement software solutions exist that force end-users to use VPN and firewall security when accessing any wireless network other than the corporate WLAN. The remote-access policy is mandatory because the most likely and vulnerable location for an attack to occur is at a public-access hotspot.

Rogue AP Policy No end-users should ever be permitted to install their own wireless devices on the corporate network. This includes access points, wireless routers, wireless USB clients, and wireless cards. Any users installing their own wireless equipment could open unsecured portals into the main infrastructure network. This policy should be strictly enforced.

Ad Hoc Policy End-users should not be permitted to set up ad hoc or peer-to-peer networks. Peer-to-peer networks rarely use encryption, are susceptible to peer attacks, and can serve as unsecured portals to the infrastructure network if the computer's Ethernet port is also in use.

Wireless LAN implementation and proper use policy A thorough policy should outline the proper use and implementation of the main corporate wireless network. This policy should include proper installation procedures, proper security implementations, and allowed application use on the wireless LAN.

IDS Policy Policies should be written defining how properly to respond to alerts generated by the wireless intrusion detection system. An example would be how to deal with the discovery of rogue access points and all the necessary actions that should take place.

These five policies are simplistic but are a good starting point in writing a well-rounded WLAN security policy document. Keep in mind that a proper WLAN policy document should be much more detailed, cover many more topics, and be strictly enforced.

Summary

All of the wonderful benefits and return on investment offered by wireless networking may cease to exist or cease to be allowed should a security and management policy not be in place and enforced. The security of the WLAN should be an integral part of the WLAN design and deployment. The wireless devices must be physically secure. The transmission of data wirelessly must also be secured. To reach the goal of effective and secure communications, written and enforced policy must be in place and communicated to all end-users from conception forward. Data confidentiality, integrity, and non-repudiation have long been goals of network security. The introduction of wireless networking does not change these goals but rather introduces new challenges in meeting them. As the use of

wireless technology continues to grow, fueled by productivity gains, convenience, and cost savings, new security challenges are continually faced by networks. WLANs allow users untethered connectivity. This new freedom can often bypass existing security measures. As technology and business requirements change, security measures must keep up in order to avoid loss of private data and/or network functionality. Written, enforced, and adaptable policies help to ensure that when business requirements and technology move forward, security measures will be in place to protect the resources of the organization.

Exam Essentials

Explain the differences between general and functional WLAN security policies. General policy establishes a framework for enforcement; functional policy defines technical aspects of security.

Describe all aspects of general policy creation and management. General policy requires a statement of authority, defines an applicable audience, and requires risk assessment and threat analysis. Security auditing and violation procedures must also be clearly defined.

Explain the importance of functional password policy and functional RBAC policy. All end-users should abide by well-defined password policies that require strong passwords and possibly two-factor authentication. Passwords should never be shared. RBAC policies ensure that certain groups of users are only allowed access to certain network resources.

Explain the importance of functional change control policy and WLAN monitoring policy. Change control procedures govern the upgrading or downgrading of firmware and software as well as hardware maintenance. Change control processes help ensure that changes to a product or system are introduced in a controlled and coordinated manner. WLAN monitoring policy defines what steps should be taken when an attack is detected by the WIDS/WIPS solution.

Explain the importance of functional authentication and encryption policies. Whenever possible, a functional policy requiring the use of 802.1X/EAP tunneled authentication should be mandated. Consideration should also be given to mandate the use of two-factor authentication solutions that require two sets of credentials before access is granted. Whenever possible, dynamic CCMP/AES encryption should be mandated for data privacy.

Define the various aspects of endpoint security policy. Minimum endpoint compliance should mandate the use of IPsec VPNs and personal firewalls. Heavy consideration should also be given to implementing an endpoint policy enforcement software solution.

Describe the functional policies of acceptable use, physical security, and remote office security. All end-users should only use applications that are intended for use on the WLAN. All WLAN infrastructure should be locked and protected from theft and vandalism. Policies should also protect WLANs at corporate headquarters as well as at remote offices.

Key Terms

Before you take the exam, be certain you are familiar with the following terms:

acceptable use policy

applicable audience

change control

endpoint policy

Federal Information Processing Standards (FIPS)

functional policy

general policy

Gramm-Leach-Bliley Act (GLBA)

Health Insurance Portability and Accountability Act (HIPAA)

information assurance

Lightweight Directory Access Protocol (LDAP)

Payment Card Industry (PCI) Standard

pretexting

Remote Authentication Dial In User Service (RADIUS)

risk assessment

role-based access control (RBAC)

Sarbanes-Oxley

security auditing

stakeholders

statement of authority

threat analysis

violation reporting procedures

Review Questions

1. Your organization is developing a wireless device usage policy. Which group(s) should be represented in the committee that actually develops this policy?
   - **A.** IT staff
   - **B.** The Security staff
   - **C.** Management
   - **D.** End-users
   - **E.** Support staff
   - **F.** All of the above

2. A large retail store chain has decided to implement wireless registers in their gardening department to allow for seasonal reconfiguration of the sales area. Knowing that they must follow the PCI standard since they process credit cards at these stations, they have hired you to ensure that their designs are PCI compliant. Which portion of their network designs should you examine to help determine if they are compliant?
   - **A.** The wireless registers
   - **B.** The APs used by the wireless registers
   - **C.** The switches to which the APs are connected
   - **D.** The portions that touch the CDE
   - **E.** The PCI standard does not allow wireless device use.

3. A merchant hires you to install a wireless network for processing credit cards in all of their new retail outlets as the stores are opened over the next six months. They have already purchased APs at an auction for you to install. Upon inspection of the APs, you find that they cannot be upgraded to support authentication and encryption beyond 64-bit WEP. You immediately inform the merchant that the APs they have purchased cannot be deployed in their new stores. What is the best reason you can give the merchant for not being able to use the APs they have already purchased?
   - **A.** They were not purchased through you, so you cannot warranty them.
   - **B.** PCI mandates that 128-bit WEP be used in all new deployments.
   - **C.** 64-bit WEP uses a 24-bit initialization vector and 128-bit WEP uses a 48-bit initialization vector.
   - **D.** PCI compliance does not allow new installation to use WEP after March 31, 2009.
   - **E.** WEP encryption will slow down card processing, resulting in angry customers.

4. To protect users and their laptops as they travel, your organization has decided to implement a wireless mobile device policy. You have explained to management that you are not able to offer the traveling users the same protection they have within your facilities as they travel, because your company does not own or manage all the hotspots to which your users may need to connect. The executives have instructed you to develop a policy that can be enforced and followed that will improve upon the security users find at hotspots. What three things can you include in the policy that will help increase wireless security for traveling users while still allowing them to use the hotspots for connectivity? (Choose all that apply.)
   - **A.** All wireless connections must use PEAP.
   - **B.** All wireless connections must use AES.
   - **C.** All wireless connections must use a VPN.
   - **D.** All wireless connections must use a personal firewall.
   - **E.** All wireless connections must use antivirus software.

5. As the head of network security for your organization, you discover an unauthorized access point plugged into your network. Upon investigation, the person that placed the rogue AP on your network is determined to be one of your own users, not an attacker. You wish to proceed with appropriate disciplinary measures but are not allowed to do so by the Human Resources department. What is the most likely reason that the HR staff would not allow disciplinary measures to be taken?
   - **A.** There is no written policy preventing users from adding their own APs to the network.
   - **B.** The user who placed the AP is a member of management.
   - **C.** The user who placed the AP is a member of the union.
   - **D.** You are not the user's direct supervisor and cannot discipline the user.
   - **E.** No data was lost or altered as a result of the rogue device placement.

6. You have been working with the network staff to expand the wireless coverage within your customer's building. Halfway through the project you are asked by a member of management to stop and leave the premises. Which step in WLAN deployment did you most likely not take prior to beginning the WLAN expansion?
   - **A.** Obtaining a Scope of Work (SOW) agreement
   - **B.** Signing a mutual nondisclosure agreement (NDA)
   - **C.** Reviewing written corporate security policies
   - **D.** Requesting that a facility escort be present

7. When deploying a corporate 802.11 WLAN, what password-related items should always be included in a security policy? (Choose all that apply.)
   - **A.** The password policy should mandate a procedure on how passphrases are created for handheld devices that use WPA2-Personal.
   - **B.** End-user WPA2-Enterprise passwords should contain numbers, special characters, and upper- and lower-case letters.
   - **C.** Client-side certificates should always be used instead of passwords when securing a WLAN.
   - **D.** Machine authentication should always be mandated.

8. When developing a security policy, it is important to include many influences such as internal requirements, governmental regulations, and industry standards. When is it allowable not to include a specific external influence in your policy development?
   - **A.** When there is little to no chance of being audited for compliance
   - **B.** When your organization is not part of the applicable audience of the external policy influence
   - **C.** When implementing wireless devices without the knowledge of the governing body that developed the external policy
   - **D.** When adherence to the external regulation or standard is cost prohibitive

9. Over the years, your company has deployed various wireless devices throughout its network. Many of these devices have been in place for quite some time and can only be configured for secure transmissions using WEP. What can you do to improve network security with the least disruption of service?
   - **A.** Create a new security policy requiring WPA2 to be used.
   - **B.** Modify the existing policy requiring WPA2 to be used.
   - **C.** Update the firmware on legacy devices to support WPA2.
   - **D.** Replace legacy hardware with new devices that support WPA2.

10. After consulting your written security policy, to meet the new demands of an industry standard with which your organization must be compliant, an administrator logs into your WLAN controller and changes the authentication and encryption configurations on all your APs. The help desk becomes overwhelmed with calls from angry users stating that they can no longer access the network. One by one, the users are reconfigured to reconnect to the network, causing significant loss of time. Which portion of a well-written security policy is most likely missing from your company's wireless security policy that caused this problem?
    - **A.** External influence compliance
    - **B.** Authentication requirements
    - **C.** Encryption compliance
    - **D.** Change control process
    - **E.** User notification process

11. Your network just passed an external compliance audit. However, the same day it passed the audit there was an intrusion that compromised your company's private data. Your staff conducted an internal audit immediately after the intrusion was detected and found that your network is still compliant. The security audit files indicate that the network was compliant during the compromise as well. What is the most likely reason that this compromise was possible on your compliant network?
    - **A.** The auditor was indeed the attacker.
    - **B.** The attacker was a network administrator.
    - **C.** Being compliant is not the same as being secure.
    - **D.** Your network is not the applicable audience for this compliance.

12. One of the first things you should do when creating a wireless security policy is to conduct an impact analysis to assist you in determining the level of acceptable risk. What should be included in your impact analysis? (Choose all that apply.)

- **A.** Direct costs of compromise
- **B.** Indirect cost of compromise
- **C.** Legal implications
- **D.** Plausible deniability
- **E.** Implementation costs

13. You have been hired to conduct a vulnerability assessment for a chipset manufacturing company. As you conduct the physical inspection of the WLAN devices, you notice that some of their APs are in locked enclosures and others are not. Before you report the unlocked APs as being vulnerable, what should you do first?

- **A.** Determine if the locked and unlocked APs are on the same network.
- **B.** Press the reset button on the unlocked APs to prove their vulnerability.
- **C.** Open the locked enclosures to make sure APs are in them.
- **D.** Verify the physical protection requirements within the written WLAN security policy.

14. While conducting a routine security analysis of your company's network, you discover an unauthorized access point installed on the network under the vice president's desk. What should you do in dealing with the rogue device since the vice president is likely to have placed the device there to provide coverage in the office for her own wireless devices?

- **A.** Remove the device and take it to the IT office for forensics.
- **B.** Unplug the device from the network but leave it in place.
- **C.** Follow the procedures for rogue device management in company policy.
- **D.** Ask the vice president what she would like done with the device.

15. Although your organization's written policy and many external policy influences may require only periodic scanning for rogue devices, you are trying to make a case for deploying a WIPS. What are some of the benefits of using a WIPS to achieve policy compliance that make them more desirable than using periodic handheld or laptop-based scanning solutions? (Choose all that apply.)

- **A.** WIPS are less expensive and easier to implement.
- **B.** WIPS can provide 24-hour scanning and protection.
- **C.** WIPS are a more scalable solution for security.
- **D.** WIPS can correlate across multiple locations.
- **E.** WIPS can provide both compliance and security.

16. Your WIPS has detected several ad hoc devices within your building. After performing location tracking in the WIPS on these devices, you and your staff physically locate them. All of the ad hoc devices detected and found have turned out to be new printers that shipped with their wireless cards enabled for ad hoc wireless networking. Ad hoc wireless networking is specifically disallowed in written security policy. Which section of your security policy should be updated to reduce the likelihood of this happening again?
    - **A.** Printing policies
    - **B.** Deployment policies
    - **C.** Purchasing policies
    - **D.** Rogue mitigation policy

17. To provide temporary access to the Internet for a group of customers visiting your corporate headquarters, an administrator has installed an access point in your boardroom. Worried about unauthorized access, the administrator has set up the AP to use WPA2 with a very long and complex key along with AES encryption. Your WIPS sees this AP as a rogue and begins to contain it using port suppression and wireless rogue containment procedures. Your visiting customers are now unable to reach the Internet as desired. What part of your security policy may need to be updated to avoid this problem in the future?
    - **A.** WIPS usage
    - **B.** Rogue containment
    - **C.** Rogue definitions
    - **D.** Secret key length
    - **E.** Guest access

18. Your WIDS detected a rogue AP and sent an email alert to an administrator in the same building in which the rogue was detected. The administrator reads the email and does not respond to the alarm, but rather waits until after lunch and then calls you for direction. This delay has allowed the device to be on the network for over an hour and placed the organization's private information at risk. What is the most likely reason the administrator took no action?
    - **A.** The WIDS detected the rogue, and no further action was required.
    - **B.** You are the only person who knows how to deal with rogue APs.
    - **C.** The security policy lacks response procedures.
    - **D.** Only a properly configured WIPS can mitigate a rogue AP.

19. A very well-written wireless security policy is in place within your organization. However, you still find rogue devices, poorly configured APs, users who are wired leaving their wireless cards enabled, and ad hoc networks throughout your building — all of which are against policy. Policy requires that such events are remediated and documented as they occur. Your WIPS has been configured to assist you in meeting this requirement and is doing so. The only people allowed in your building are your own employees. You are not under an attack but still keep finding the same problems daily. Which portion of good security policy is most likely lacking that has lead to this problem?

A. Impact analysis

B. Management approval

C. User training

D. Documentation

20. An employee has installed his own AP on your network. Each day when he leaves, he unplugs the AP and plugs it back in the morning. He has not implemented any security on the AP. After months of being on the network, this "rogue" AP finally leads to a compromise of corporate secrets. Corporate security policy prohibits the installation of APs without approval. What other requirement(s) should be added to the security policy that could have prevented this compromise? (Choose all that apply.)

A. Monitoring for rogue devices

B. Rogue device remediation

C. User training

D. Policy enforcement procedures

Answers to Review Questions

1. F. It is important to include all stakeholders, especially management, when developing a wireless usage policy. By allowing the stakeholders to assist in policy development, you are more likely to create a usable, followed, and enforceable policy.

2. D. The PCI standard specifies how to protect the cardholder data environment (CDE) both on the wired network and wirelessly. Any organization that processes or stores cardholder information must follow PCI guidelines or risk severe penalties.

3. D. PCI compliance does not allow any new deployments to include WEP after March 31, 2009. Furthermore, PCI mandates that WEP not be used within or touching the CDE after June 30, 2010.

4. C, D, E. Traveling users are obviously not going to be able to connect to your WLAN from the road. Hotspots at best only use a captive portal for security. You cannot expect a hotspot to use a WPA2-Enterprise solution that meets your needs. For traveling users, the best things you can provide for their wireless security without additional supplicant software are an up-to-date antivirus program, an up-to-date firewall, and a strong VPN solution when connecting to public networks. It is important to include security of traveling devices in your written WLAN security policies.

5. A. If there is no written policy forbidding the placement of wireless devices without authorization, it is often difficult or impossible to take appropriate disciplinary measures, because there are none specified.

6. C. In addition to all of the required documentation used in network design, SOW, NDA, floor plans, and even a liability statement, you should always ask to see and examine the written security policies if they exist. Failure to do so may lead to a breach in security and an embarrassing situation, such as being escorted off the premises.

7. A, B. Using client-side certificates for end-user credentials and using machine authentication are both excellent methods of securing a WLAN. However, a policy mandating their use is not always practical due to the expense and administrative overhead. All end-user WPA-2 Enterprise passwords should contain numbers, special characters, and upper- and lower-case letters. Because a WPA2-Personal passphrase is static and shared among many legacy devices not capable of 802.1X/EAP, a policy should dictate the method of creation. The topic of entropy is covered in Chapter 6. It is extremely important when considering password policy.

8. B. Only the applicable audience of an external policy influence is required to follow the mandates of that regulation or standard. However, following some of the guidelines from nonrequired policies is often a good practice to increase your own security levels. This is often done within organizations that do not have to meet FIPS compliance but want to have a standardization that is deemed more secure than others without developing standards internally and adopting those designed by others.

9. C. Updating the firmware of the legacy devices would be the least expensive and least disruptive way to improve the security posture of this organization. Neither creating nor changing policy improves actual security. If the policy is not followed it will be of no use. You must change the security from WEP to something more secure. Swapping out the devices for new ones with the ability to do WPA2 would improve security, but would also be more disruptive than simply updating the firmware to do so. However, it should be noted that, in many cases, upgrading hardware is the only option because the legacy hardware does not have the processing power to support WPA2. Keeping up with security patches and making sure your devices can support the latest security should be part of a well-executed security plan.

10. D. A well-crafted security policy will include a change control process that helps to reduce the impact of making changes in security configurations. Security policies must adapt as risks and technologies change. When making changes in business practices or security measures, impact on function must be taken into consideration.

11. C. Being compliant should never be confused with being secure. For example, PCI states that WEP can still be used until June 30, 2010. If your network is using WEP to protect the CDE, you may be compliant. However, given the weakness found in WEP security and the public availability of freeware that cracks WEP and videos that teach people how to crack WEP, your network is not secure. Some of the most widely known wireless attacks happened on "compliant" networks.

12. A, B, C, E. The total impact of a compromise should be weighed when conducting an impact analysis. This includes both tangible and intangible costs. You should also consider not just the costs of implementing secure solutions but also the costs of not implementing them. You should also weigh the legal implications should there be a compromise when developing a security policy. Fines and court costs due to litigation arising from a compromise are a loss to the organization as well. Avoiding fines for noncompliance is just as much a security concern as keeping intruders off your WLAN.

13. D. Some policies mandate physical security of the APs to include locked enclosures based on the network's data privacy requirements. You should always review written security policy prior to conducting a vulnerability assessment. Hacking into the network or tampering with devices in any way are not parts of an assessment but may be part of a penetration test if covered in the SOW. It is possible to have both locked and unlocked protection requirements in the same building.

14. C. When dealing with rogue device placement, or even with legitimate device placement, company security policies should always be followed. Mitigating the rogue should be covered in the policy no matter who placed the device on the network or where the device is located.

15. B, C, D, E. Compared to handheld and laptop-based scanning solutions, WIPS are more expensive but enable organizations to maintain compliance and security with less effort once deployed. WIPS and WIDS are mentioned in several policies and offer more than just compliance. Periodic scanning only captures information while you are scanning and only from one location. WIPS scan 24 hours a day and have the ability to use proactive measures to protect the WLAN.

16. B. Deployment policies should include how devices are configured prior to deployment. Many new printers ship with the wireless card enabled and set for default ad hoc use. A policy covering device deployment that is followed can reduce misconfigurations that lead to security policy violations.

17. E. If guests are going to be allowed the use of wireless devices in your buildings, then the use of such devices should be addressed in your security policies. Many organizations use guest networks on separate Internet connections in the DMZ or on separate VLAN's within the building. The fact that a trusted employee placed the device with nothing but good intentions does not change the fact that the AP is a rogue and should be contained by the WIPS.

18. C. IDS policies should define how to respond properly to alerts generated by the wireless intrusion detection system. An example would be how to deal with the discovery of rogue access points and all the necessary actions that should take place.

19. C. Users must be trained to follow security policies. Even if they are well written and enforced, the users must know what they are and how to best comply to make security policies effective.

20. A, B, C, D. Monitoring for rogue devices, rogue device remediation, user training, and policy enforcement procedures are all part of a successful security policy implementation. End-users should never be permitted to install their own wireless devices on the corporate network. This includes access points, wireless routers, wireless hardware USB clients, and wireless cards. Any users installing their own wireless equipment could open unsecured portals into the main infrastructure network. This policy should be strictly enforced.

Appendix

A

Abbreviations, Acronyms, and Regulations

Certifications

CWNA Certified Wireless Network Administrator

CWNE Certified Wireless Network Expert

CWNT Certified Wireless Network Trainer

CWSP Certified Wireless Security Professional

CWTS Certified Wireless Technology Specialist

Organizations and Regulations

ACMA Australian Communications and Media Authority

ARIB Association of Radio Industries and Businesses (Japan)

ATU African Telecommunications Union

CEPT European Conference of Postal and Telecommunications Administrations

CITEL Inter-American Telecommunication Commission

CTIA Cellular Telecommunications and Internet Association

CWNP Certified Wireless Network Professional

DoD Department of Defense

ERC European Radiocommunications Committee

EWC Enhanced Wireless Consortium

FCC Federal Communications Commission

FIPS Federal Information Processing Standards

GLBA Gramm-Leach-Bliley Act

HIPAA Health Insurance Portability and Accountability Act

IANA Internet Assigned Number Authority

IEEE Institute of Electrical and Electronics Engineers

IETF Internet Engineering Task Force

ISO International Organization for Standardization

ITU-R International Telecommunications Union Radio Communication Sector

NEMA National Electrical Manufacturers Association

NIST National Institute of Standards and Technology

PCI Payment Card Industry

RCC Regional Commonwealth in the field of Communications

SEE-Mesh Simple, Efficient, and Extensible Mesh

SOX Sarbanes-Oxley

UTMS Universal Mobile Telecommunications System

WECA Wireless Ethernet Compatibility Alliance

WIEN Wireless Interworking with External Networks

Wi-Fi Alliance Wi-Fi Alliance

WiMA Wi-Mesh Alliance

WNN Wi-Fi Net News

Measurements

dB decibel

dBd decibels referenced to a dipole antenna

dBi decibels referenced to an isotropic radiator

dBm decibels referenced to 1 milliwatt

GHz gigahertz

Hz hertz

KHz kilohertz

mA milliampere

MHz megahertz

mW milliwatt

SNR signal-to-noise ratio

V volt

VDC voltage direct current

W watt

Technical Terms

3DES Triple DES

AA authenticator address

AAA authorization, authentication, and accounting

AAD additional authentication data

AC access category

AC access controller

AC alternating current

ACK acknowledgment

ACL access control list

AD Active Directory

AES Advanced Encryption Standard

AGL above ground level

AH Authentication Header

AID association identifier

AIFS arbitration interframe space

AKM Authentication and Key Management

AM amplitude modulation

A-MPDU Aggregate MAC Protocol Data Unit

A-MSDU Aggregate MAC Service Data Unit

ANonce authenticator nonce

AP access point

APSD automatic power save delivery

ARC4 Alleged RC4

ARP Address Resolution Protocol

ARS adaptive rate selection

ARS automatic rate selection

AS authentication server

ASCII American Standard Code for Information Interchange

ASK Amplitude Shift Keying

ATF airtime fairness

ATIM announcement traffic indication message

AVP attribute value pair

BA Block Acknowledgment

BER bit error rate

BIP broadcast/multicast integrity protocol

BPSK Binary Phase Shift Keying

BSA basic service area

BSS basic service set

BSSID basic service set identifier

BT Bluetooth

BVI bridged virtual interface

CAD computer-aided design

CAM content addressable memory

CAM continuous aware mode

CAPWAP Control and Provisioning of Wireless Access Points

CBC Cipher-Block Chaining

CBC-MAC Cipher Block Chaining Message Authentication Code

CCA clear channel assessment

CC-AP cooperative control access point

CCI co-channel interference

CCK Complementary Code Keying

CCKM Cisco Centralized Key Management

CCM Counter with CBC-MAC

CCMP Counter Mode with Cipher Block Chaining Message Authentication Code Protocol

CCX Cisco Compatible Extensions

CDE cardholder data environment

CDMA2000 code division multiple access 2000

CDP Cisco Discovery Protocol

CF CompactFlash

CF contention free

CFP contention-free period

CHAP Challenge Handshake Authentication Protocol

CKIP Cisco Key Integrity Protocol

CLI command-line interface

CN common name

COW computer on wheels

CP contention period

CRC cyclic redundancy check

CSMA/CA Carrier Sense Multiple Access with Collision Avoidance

CSMA/CD Carrier Sense Multiple Access with Collision Detection

CSR certificate-signing request

CTL Certified Trust List

CTR counter mode

CTS clear to send

CW contention window

CWG-RF Converged Wireless Group-RF Profile

DA destination address

DBPSK Differential Binary Phase Shift Keying

DC direct current

DCF Distributed Coordination Function

DDF distributed data forwarding

DDoS distributed denial of service

DECT Digital Enhanced Cordless Telecommunications

DES Data Encryption Standard

DFS dynamic frequency selection

DHCP Dynamic Host Configuration Protocol

DIFS Distributed Coordination Function interframe space

DLS direct link setup

DoS denial of service

DQPSK Differential Quadrature Phase Shift Keying

DRS dynamic rate switching

DS distribution system

DSAS distributed spectrum analysis system

DSCP differentiated services code point

DSM distribution system medium

DSP digital signal processing

DSRC Dedicated Short Range Communications

DSS distribution system services

DSSS direct sequence spread spectrum

DSSS-OFDM direct sequence spread spectrum-orthogonal frequency division multiplexing

DTIM delivery traffic indication message

DTLS Datagram Transport Layer Security

EAP Extensible Authentication Protocol

EAPOL Extensible Authentication Protocol over LAN

EAP-AKA Extensible Authentication Protocol-Authentication and Key Agreement

EAP-FAST Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling

EAP-GTC Extensible Authentication Protocol-Generic Token Card

EAP-LEAP Extensible Authentication Protocol-Lightweight Extensible Authentication Protocol

EAP-MD5 Extensible Authentication Protocol-Message Digest5

EAP-MSCHAPv2 Extensible Authentication Protocol-Microsoft Challenge Handshake Authentication Protocol

EAP-PEAP Extensible Authentication Protocol-Protected Extensible Authentication Protocol

EAP-POTP Extensible Authentication Protocol-Protected One-Time Password Protocol

EAP-SIM Extensible Authentication Protocol-Subscriber Identity Module

EAP-TLS Extensible Authentication Protocol-Transport Layer Security

EAP-TTLS Extensible Authentication Protocol-Tunneled Transport Layer Security

EDCA Enhanced Distributed Channel Access

EEG enterprise encryption gateway

EIFS extended interframe space

EIRP equivalent isotropically radiated power

EM electromagnetic

EQM equal modulation

ERP Extended Rate Physical

ERP-CCK Extended Rate Physical Complementary Code Keying

ERP-DSSS Extended Rate Physical Direct Sequence Spread Spectrum

ERP-OFDM Extended Rate Physical Orthogonal Frequency Division Multiplexing

ERP-PBCC Extended Rate Physical Packet Binary Convolutional Coding

ESA extended service area

ESP Encapsulating Security Payload

ESS extended service set

ESSID extended service set identifier

EUI extended unique identifier

EWG enterprise wireless gateway

FAST Flexible Authentication via Secure Tunnel

FCS frame check sequence

FEC forward error correction

FHSS frequency hopping spread spectrum

FM frequency modulation

FMC fixed mobile convergence

FSK Frequency Shift Keying

FSPL free space path loss

FSR fast secure roaming

FT fast BSS transition

FTAA FT authentication algorithm

FTIE fast BSS transition information element

FZ Fresnel zone

GFSK Gaussian Frequency Shift Keying

GI guard interval

GMK group master key

GPS Global Positioning System

GRE Generic Routing Encapsulation

GSM Global System for Mobile Communications

GTC Generic Token Card

GTK group temporal key

GUI graphical user interface

HC hybrid coordinator

HCCA Hybrid Coordination Function Controlled Channel Access

HCF Hybrid Coordination Function

HMAC Hashed Message Authentication Codes

HR-DSSS High-Rate Direct Sequence Spread Spectrum

HSRP Hot Standby Router Protocol

HT High Throughput

HT-GF-STF high-throughput Greenfield short training field

HT-LTF high-throughput long training field

HT-SIG high-throughput SIGNAL field

HT-STF high-throughput short training field

HTTPS Hypertext Transfer Protocol Secure

HWMP Hybrid Wireless Mesh Protocol

Hz Hertz

IAPP Inter-Access Point Protocol

IBSS independent basic service set

ICMP Internet Control Message Protocol

ICV Integrity Check Value

IDS intrusion detection system

IE Information Element

IFS interframe space

IKE Internet Key Exchange

IP Internet Protocol

IPS intrusion prevention system

IPsec Internet Protocol Security

IR infrared

IR intentional radiator

IS integration service

ISAKMP Internet Security Association and Key Management Protocol

ISI intersymbol interference

ISM Industrial, Scientific, and Medical

ITS Intelligent Transportation Systems

IV Initialization Vector

JDBC Java Database Connectivity

KCK Key Confirmation Key

KEK Key Encryption Key

L2TP Layer 2 Tunneling Protocol

LAN local area network

LBAC location based access control

LCI location configuration information

LDAP Lightweight Directory Access Protocol

LEAP Lightweight Extensible Authentication Protocol

LLC Logical Link Control

L-LTF Legacy (non-HT) long training field

LOS line of sight

L-SIG Legacy (non-HT) long signal field

L-STF Legacy (non-HT) short training field

LWAPP Lightweight Access Point Protocol

MAC media access control

MAHO Mobile Assisted Hand-Over

MAN metropolitan area network

MAP mesh access point

MCA multiple channel architecture

MCS modulation and coding schemes

MD mobility domain

MD5 Message Digest *5*

MDC mobility domain controller

MDID mobility domain identifier

MDIE mobility domain information element

MDI media dependent interface

MFP management frame protection

MIB Management Information Base

MIC Message Integrity Code

MIMO multiple-input multiple-output

MMPDU Management MAC Protocol Data Unit

MPDU MAC Protocol Data Unit

MP mesh point

MPP mesh point collocated with a mesh portal

MPPE Microsoft Point-to-Point Encryption

MRC maximal ratio combining

MSDU MAC Service Data Unit

MSK master session key

MTBA multiple traffic ID block acknowledgment

MTU maximum transmission unit

mW milliwatt

NAC network access control

NAT Network Address Translation

NAV Network Allocation Vector

NFC Near Field Communication

NOC network operations center

nQSTA Non-Quality of Service Station

OAC Odyssey Access Client

ODBC Open Database Connectivity

OFDM Orthogonal Frequency Division Multiplexing

OKC opportunistic key caching

OS operating system

OSI model Open Systems Interconnection model

OTAP Over-the-air provisioning

OTP one-time password

OU organizational unit

OUI Organizationally Unique Identifier

PAC protected access credential

PAN personal area network

PAP Password Authentication Protocol

PAT Port Address Translation

PBC push-button configuration

PBCC Packet Binary Convolutional Coding

PBX private branch exchange

PC point coordinator

PCF Point Coordination Function

PCI Peripheral Component Interconnect

PCMCIA Personal Computer Memory Card International Association (PC Card)

PCO phased coexistence operation

PD powered device

PEAP Protected Extensible Authentication Protocol

PHY physical layer

PIFS Point Coordination Function interframe space

PIN personal information number

PKI public key infrastructure

PLCP Physical Layer Convergence Procedure

PMD Physical Medium Dependent

PMK pairwise master key

PMKID pairwise master key identifier

PMK-R0 pairwise master key R0

PMK-R1 pairwise master key R1

PMKSA pairwise master key security association

PN packet number

PN pseudo-random number

PoE Power over Ethernet

POP Post Office Protocol

PPDU PLCP Protocol Data Unit

PPP Point-to-Point Protocol

PPTP Point-to-Point Tunneling Protocol

PSDU PLCP Service Data Unit

PRF pseudo-random function

PSE power-sourcing equipment

PSK Phase Shift Keying

PSK preshared key

PSMP Power Save Multi Poll

PSPF Public Secure Packet Forwarding

PS-Poll power save poll

PSTN public switched telephone network

PTK pairwise transient key

PTKSA pairwise transient key security association

PTMP point-to-multipoint

PTP point-to-point

QAM quadrature amplitude modulation

QAP quality-of-service access point

QBSS quality-of-service basic service set

QoS quality of service

QSTA quality-of-service station

QPSK Quadrature Phase Shift Keying

RA receiver address

RADIUS Remote Authentication Dial-In User Service

RAP remote access point

RBAC role-based access control

RF radio frequency

RFC request for comment

RF LOS RF line of sight

RFSM radio frequency spectrum management

RIC resource information container

RIFS reduced interframe space

R0KH R0 key holder

R1KH R1 key holder

RRM radio resource measurement

RSL received signal level

RSN robust security network

RSNA robust security network association

RSNIE robust security network information element

RSSI received signal strength indicator

RTLS real-time location system

RTS request to send

RTS/CTS request to send/clear to send

RWG residential wireless gateway

RX receive or receiver

SA security associations

SA source address

S-APSD scheduled automatic power save delivery

SCA single channel architecture

SD Secure Digital

SDR software-defined radio

SHA-1 Secure Hash Algorithm

SID system identifier

SIFS short interframe space

SIM Subscriber Identity Module

SIP Session Initiation Protocol

SRP SpectraLink Radio Protocol

SVP SpectraLink Voice Priority

SISO single input single output

SM spatial multiplexing

SMB small and medium-sized business

SMK STSL master key

SMTP Simple Mail Transfer Protocol

SNMP Simple Network Management Protocol

SNR signal-to-noise ratio

SOHO small office/home office

S0KH S0 key holder

S1KH S1 key holder

SOM system operating margin

SOW statement of work

SPA supplicant address

SQ signal quality

SSH Secure Shell

SSID service set identifier

SSL Secure Sockets Layer

STA station

STC Space Time Coding

STK STSL transient key

STP Spanning Tree Protocol

STSL station-to-station link

TA transmitter address

TBTT target beacon transmission time

TCP/IP Transmission Control Protocol/Internet Protocol

TDEA Triple Data Encryption Algorithm

TDoA Time Difference of Arrival

TIM traffic indication map

TK Temporal Key

TKIP Temporal Key Integrity Protocol

TLS Transport Layer Security

TPC transmit power control

TSC TKIP sequence counter

TSN transition security network

TTAK TKIP-mixed transmit address and key

TTL time to live

TTLS Tunneled Transport Layer Security

TX transmit or transmitter

TxBF transmit beamforming

TXOP transmit opportunity

U-APSD unscheduled automatic power save delivery

UEQM unequal modulation

UNII Unlicensed National Information Infrastructure

UP user priority

USB Universal Serial Bus

USIM User Subscriber Identity Module

UTMS Universal Mobile Telecommunications System

VLAN virtual local area network

VoIP Voice over IP

VoWiFi Voice over Wi-Fi

VPN virtual private network

VRRP Virtual Router Redundancy Protocol

VSA vendor specific attribute

VSWR voltage standing wave ratio

WAN wide area network

WAVE Wireless Access in Vehicular Environments

WDS wireless distribution system

WEP Wired Equivalent Privacy

WGB workgroup bridge

WIDS wireless instruction detection system

Wi-Fi Sometimes said to be an acronym for *wireless fidelity*, a term that has no formal definition; Wi-Fi is a general marketing term used to define 802.11 technologies.

WIGLE Wireless Geographic Logging Engine

WiMAX Worldwide Interoperability for Microwave Access

WIPS wireless intrusion prevention system

WISP Wireless Internet Service Provider

WLAN wireless local area network

WLSE Wireless LAN Solution Engine

WM wireless medium

WMAN wireless metropolitan area network

WMM Wi-Fi Multimedia

WMM-PS Wi-Fi Multimedia Power Save

WMM-SA Wi-Fi Multimedia Scheduled Access

WNMS wireless network management system

WPA Wi-Fi Protected Access

WPA2 Wi-Fi Protected Access 2

WPAN wireless personal area network

WPP Wireless Performance Prediction

WPS Wi-Fi Protected Setup

WTP wireless termination point

WWAN wireless wide area network

WZC Wireless Zero Configuration

XOR exclusive or

Power Regulations

The Federal Communications Commission (FCC) regulates communications to and from the United States. The FCC and the respective controlling agencies in other countries regulate the amount of power at the intentional radiator (IR) and the amount of power radiated from the antenna (EIRP) for 802.11 radios. Power output regulations are typically created to minimize interference within the band and to minimize interference to adjacent or nearby bands.

The rules regarding the amount of power that is permitted are typically divided into two categories: point-to-multipoint communications (PtMP) and point-to-point communications (PtP). The regulations for PtMP communications are generally more restrictive than the regulations for PtP communications. The reason is fairly straightforward: PtMP signals are generated in all directions, covering a broad area, and thus are more likely to interfere with other devices; whereas PtP signals are focused using high-gain antennas, making the area of potential interference very small. The following sections review the FCC power regulations.

2.4 GHz ISM Point-to-Multipoint (PtMP) Communications

PtMP communications consist of a central communications device communicating to multiple other devices. If the central device is connected to an omnidirectional antenna, the FCC automatically classifies the communications as PtMP. The central PtMP device does not have to be connected to an omnidirectional antenna, as is the case with many access points that are connected to semi-directional patch antennas.

The FCC limits the maximum power at the intentional radiator (IR) to 1 watt (+30 dBm) and the maximum radiated power from the antenna (EIRP) to 4 watts (+36 dBm). This means that if the IR is at the maximum power of 1 watt, or 30 dBm, the maximum gain antenna that can be used is 6 dBm, which creates a total EIRP of 36 dBm, or 4 watts. Remember that IR + antenna gain = EIRP.

No matter what you want to do, the EIRP cannot be greater than 36 dBm, or 4 watts. This means that if you want to use a higher-gain antenna, you must subtract the antenna gain from the EIRP to calculate the maximum IR that you can have. As an example, if you wanted to use a 9 dBi patch antenna, the maximum IR would be 27 dBm, or 500 mW (36 dBm – 9 dBi = 27 dBm). For every dBi increase in the antenna above 6 dBi, the IR must decrease by the same amount. This is often known as the one-to-one, or 1:1, rule.

5 GHz UNII Point-to-Multipoint (PtMP) Communications

The FCC PtMP rules for the 5 GHz UNII bands follow the same basic rules of the 2.4 GHz ISM PtMP communications. A 6 dBi antenna can be connected to the PtMP device without affecting the maximum EIRP. Any additional increase in antenna gain requires an equal decrease in IR. Figures A.1 and A.2 show the maximum IR and EIRP values for the UNII bands in both the United States (FCC) and Europe (ERC).

FIGURE A.1 5 GHz PtMP—intentional radiator power regulations

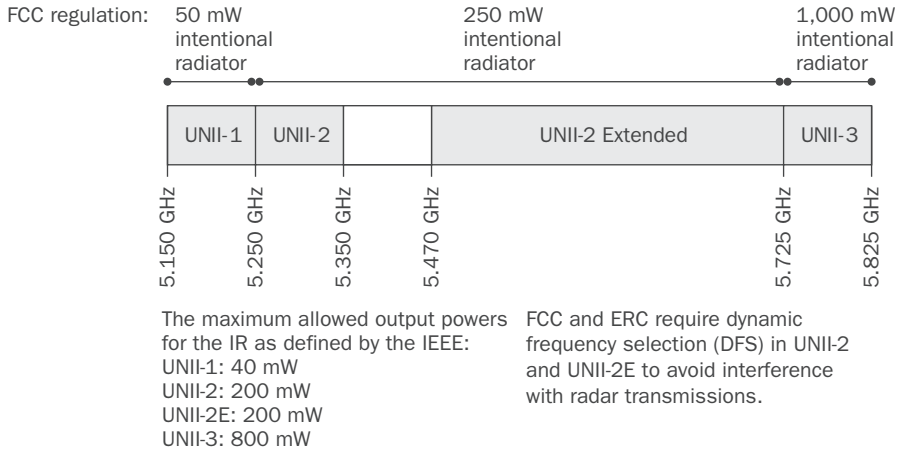
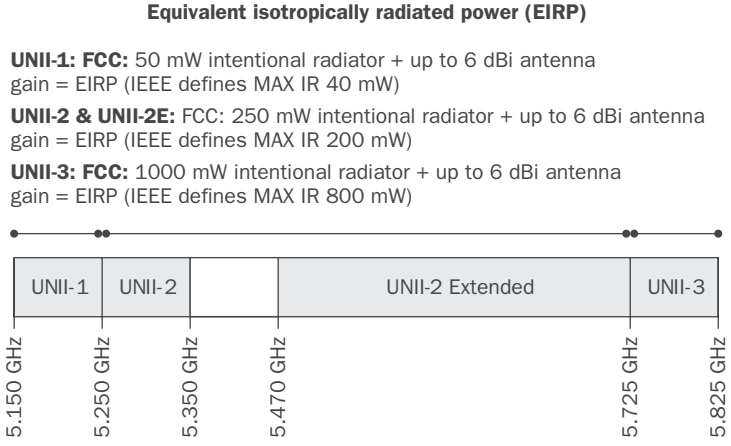


FIGURE A.2 5 GHz PtMP—equivalent isotropically radiated power (EIRP) regulations



2.4 GHz ISM Point-to-Point (PtP) Communications

Point-to-point communication consists of two devices communicating with each other by using directional antennas. The FCC PtP rules for the 2.4 GHz ISM band start with the same initial values as the PtMP rules: 1-watt IR, 6 dBi antenna, 4-watt EIRP. The maximum allowed IR is still 1 watt; however, because the antenna is directional and communicating with only one other device, the FCC allows the antenna gain and the EIRP to be increased.

For every 3 dB additional increase of the antenna (above the initial 6 dBi value), the IR must be decreased by 1 dB. This is often known as the three-to-one, or 3:1, rule.

Remember that IR + antenna gain = EIRP, so if the antenna is increased by 3 dB and the IR is decreased by 1 dB, the EIRP is increased by 2 dB. To help you understand the rule, just remember 3-2-1. A 3 dB increase in the antenna creates a 2 dB increase in the EIRP because it requires a 1 dB decrease in the IR.

IR	Antenna Gain	Maximum EIRP
+30 dBm (1 watt)	6 dBi	+36 dBm (4 watts)
+29 dBm	9 dBi	+38 dBm (6.3 watts)
+28 dBm	12 dBi	+40 dBm (10 watts)
+27 dBm	15 dBi	+42 dBm (16 watts)
+26 dBm	18 dBi	+44 dBm (25 watts)
+25 dBm	21 dBi	+46 dBm (39.8 watts)
+24 dBm	24 dBi	+48 dBm (63 watts)
+23 dBm	27 dBi	+50 dBm (100 watts)
+22 dBm	30 dBi	+52 dBm (158 watts)

5 GHz UNII Point-to-Point (PtP) Communications

The FCC PtP rules for the 5 GHz UNII-1 and UNII-2 bands are identical to the PtMP rules for these bands. For the UNII-3 band, the FCC has a separate set of rules because the UNII-3 band is often used for long-distance point-to-point communications. A fixed PtP transmitter with a maximum IR of +30 dBm (1 watt) is allowed to be connected to a directional antenna with a gain of up to 23 dBi without making any change to the IR. The maximum allowed EIRP is therefore +53 dBm (200 watts). For every dBi increase in the antenna above 23 dBi, the IR must decrease by the same amount. So if you have any gain above the 23 dBi, you must adhere to the 1:1 rule.

Windows Registry Values that Control Preauthentication and PMK Caching

The following registry entries in the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EAPOL\Parameters\General\Global subkey control the behavior of preauthentication and PMK caching for the WPA2/WPS IE Update.

PMKCacheMode
Value type: REG_DWORD - Boolean
Valid range: 0 (disabled), 1 (enabled)
Default value: 1
Present by default: No
Description: Specifies whether a Windows XP-based wireless client will perform PMK caching. By default, PMKCacheMode is enabled.

PMKCacheTTL
Value type: REG_DWORD
Valid range: 5-1440
Default value: 720
Present by default: No
Description: Specifies the number of minutes that an entry in the PMK cache can exist before being removed. The maximum value is 1440 (24 hours). The default value is 720 (12 hours).

PMKCacheSize
Value type: REG_DWORD
Valid range: 1-255
Default value: 100
Present by default: No
Description: Specifies the maximum number of entries that can be stored in the PMK cache. By default, the PMK cache has 16 entries.

PreAuthMode
Value type: REG_DWORD - Boolean
Valid range: 0 (disabled), 1 (enabled)
Default value: 0
Present by default: No
Description: Specifies whether a Windows XP-based wireless client will try preauthentication. By default, PreAuthMode is disabled.

PreAuthThrottle
Value type: REG_DWORD
Valid range: 1-16
Default value: 3
Present by default: No
Description: Specifies the number of top candidate wireless access points with which the Windows XP-based computer will try preauthentication. The value is based on the ordered list of the most favored wireless access points, as reported by the wireless network adaptor driver. By default, PreAuthThrottle has a value of 3.

Appendix

B

WLAN Vendors

There are many vendors in the 802.11 WLAN marketplace, including some of the more established companies, such as Cisco, and many startup WLAN companies, such as Meru Networks. The following is a list of some of the major WLAN vendors. Please note that each vendor is listed in only one category, even if they offer products and services that cover multiple categories. This is most notable with the infrastructure vendors, who often offer additional capabilities, such as security and troubleshooting, as features of their products.

WLAN Infrastructure

These 802.11 enterprise equipment vendors manufacture and sell WLAN controllers and access points:

- Aerohive — `www.aerohive.com`
- Aruba Networks — `www.arubanetworks.com`
- Bluesocket — `www.bluesocket.com`
- Cisco — `www.cisco.com`
- Extricom — `www.extricom.com`
- Hewlett-Packard — `www.procurve.com`
- Meru Networks — `www.merunetworks.com`
- Motorola — `www.motorola.com`
- Proxim — `www.proxim.com`
- Ruckus Wireless — `www.ruckuswireless.com`
- Siemens — `www.siemens.com`
- Trapeze Networks — `www.trapezenetworks.com`
- Xirrus — `www.xirrus.com`

WLAN Mesh Infrastructure

These WLAN vendors specialize in 802.11 mesh networking:

- BelAir Networks — `www.belairnetworks.com`
- Firetide — `www.firetide.com`
- Meraki — `www.meraki.com`

- MeshDynamics — www.meshdynamics.com
- Strix Systems — www.strixsystems.com
- Tropos Networks — www.tropos.com

WLAN Auditing, Diagnostic, and Design Solutions

These are some companies that sell 802.11 protocol analyzers, spectrum analyzers, site survey software, and other WLAN analysis solutions:

- AirMagnet — www.airmagnet.com
- Berkeley Varitronics Systems — www.bvsystems.com
- CACE Technologies — www.cacetech.com
- Ekahau — www.ekahau.com
- Fluke Networks — www.flukenetworks.com
- Immunity — www.immunityinc.com
- MetaGeek — www.metageek.net
- Nuts About Nets — www.nutsaboutnets.com
- TamoSoft — www.tamos.com
- WildPackets — www.wildpackets.com
- Wireshark — www.wireshark.org

WLAN Management

These companies provide wireless network management system (WNMS) solutions:

- AirWave — www.airwave.com
- Wavelink — www.wavelink.com

WLAN Security Solutions

These WLAN companies offer overlay encryption solutions, WIDS/WIPs solutions, or 802.1X/EAP supplicant/server solutions:

- AirDefense — www.airdefense.net
- AirTight Networks — www.airtightnetworks.com
- Fortress Technologies — www.fortresstech.com
- Harris Corporation — www.rfcomm.harris.com
- Juniper Networks — www.juniper.net

VoWiFi Solutions

Manufacturers of 802.11 VoWiFi phones and VoIP gateway solutions include:

- Ascom — www.ascom.com
- Polycom — www.polycom.com
- Vocera — www.vocera.com

WLAN Fixed Mobile Convergence

Manufacturers of 802.11 and cellular convergence solutions include:

- Agito Networks — www.agitonetworks.com
- DiVitas Networks — www.divitas.com

WLAN RTLS Solutions

Manufacturers of 802.11 real-time location system (RTLS) solutions include:

- AeroScout — www.aeroscout.com
- Newbury Networks — www.newburynetworks.com

WLAN SOHO Vendors

Some of the many WLAN vendors also sell SOHO solutions that provide Wi-Fi for the average home user:

- Apple — www.apple.com
- Buffalo Technology — www.buffalotech.com
- Belkin — www.belkin.com
- D-Link — www.dlink.com
- Hawking Technology — www.hawkingtech.com
- Linksys — www.linksys.com
- Netgear — www.netgear.com
- SMC Networks — www.smc.com

Appendix

C

About the Companion CD

IN THIS APPENDIX:

- ✓ What you'll find on the CD
- ✓ System requirements
- ✓ Using the CD
- ✓ Troubleshooting

What You'll Find on the CD

The following sections are arranged by category and summarize the software and other goodies you'll find on the companion CD. If you need help with installing the items provided on the CD, refer to the installation instructions in the "Using the CD" section of this appendix.

Some programs on the CD might fall into one of these categories:

Shareware programs are fully functional, free, trial versions of copyrighted programs. If you like particular programs, register with their authors for a nominal fee and receive licenses, enhanced versions, and technical support.

Freeware programs are free, copyrighted games, applications, and utilities. You can copy them to as many computers as you like—for free—but they offer no technical support.

GNU software is governed by its own license, which is included inside the folder of the GNU software. There are no restrictions on distribution of GNU software. See the GNU license at the root of the CD for more details.

Trial, demo, or *evaluation* versions of software are usually limited either by time or by functionality (such as not letting you save a project after you create it).

White papers to serve as additional reference material.

Sybex Test Engine

For Windows

The CD contains the Sybex test engine, which includes the entire assessment test and all the chapter review questions in electronic format, as well as two bonus exams located only on the CD.

Electronic Flashcards

For PC, Pocket PC, and Palm

These handy electronic flashcards are just what they sound like. One side contains a question or fill-in-the-blank question, and the other side shows the answer.

System Requirements

Make sure your computer meets the minimum system requirements shown in the following list. If your computer doesn't meet most of these requirements, you may have problems using the software and files on the companion CD. For the latest and greatest information, please refer to the ReadMe file located at the root of the CD.

- A PC running Microsoft Windows 98, Windows 2000, Windows NT4 (with SP4 or later), Windows Me, Windows XP, or Windows Vista.
- An Internet connection
- A CD-ROM drive

Using the CD

To install the items from the CD to your hard drive, follow these steps:

1. Insert the CD into your computer's CD-ROM drive. The license agreement appears.

Windows users: The interface won't launch if you have Autorun disabled. In that case, click Start ➢ Run (for Windows Vista, Start ➢ All Programs ➢ Accessories ➢ Run). In the dialog box that appears, type **`D:\Start.exe`**. (Replace D with the proper letter if your CD drive uses a different letter. If you don't know the letter, see how your CD drive is listed under My Computer.) Click OK.

2. Read the license agreement, and then click the Accept button if you want to use the CD.

The CD interface appears. The interface allows you to access the content with just one or two clicks.

Troubleshooting

Wiley has attempted to provide programs that work on most computers with the minimum system requirements. Alas, your computer may differ, and some programs may not work properly for some reason.

The two likeliest problems are that you don't have enough memory (RAM) for the programs you want to use or you have other programs running that are affecting installation or running of a program. If you get an error message such as "Not enough

memory" or "Setup cannot continue," try one or more of the following suggestions and then try using the software again:

Turn off any antivirus software running on your computer. Installation programs sometimes mimic virus activity and may make your computer incorrectly believe that it's being infected by a virus.

Close all running programs. The more programs you have running, the less memory is available to other programs. Installation programs typically update files and programs, so if you keep other programs running, installation may not work properly.

Have your local computer store add more RAM to your computer. This is, admittedly, a drastic and somewhat expensive step. However, adding more memory can help the speed of your computer and allow more programs to run at the same time.

Customer Care

If you have trouble with the book's companion CD, please call the Wiley Product Technical Support phone number at (800) 762-2974. Outside the United States, call +1(317) 572-3994. You can also contact Wiley Product Technical Support at `http://sybex.custhelp.com`. John Wiley & Sons will provide technical support only for installation and other general quality-control items. For technical support on the applications themselves, consult the program's vendor or author.

To place additional orders or to request information about other Wiley products, please call (877) 762-2974.

Glossary

Numbers

4-Way Handshake Under the 802.11i amendment, two stations (STAs) must establish a procedure to authenticate and associate with each other as well as create dynamic encryption keys through a process known as the 4-Way Handshake.

802.11-2007 standard On March 8, 2007, the most current iteration of the standard that was approved: IEEE Std. 802.11-2007. This new standard is an update of the IEEE Std. 802.11-1999 revision, with the inclusion of eight ratified amendments. This new standard includes the following:

IEEE Std. 802.11-1999 (R2003)

IEEE Std. 802.11a-1999

IEEE Std. 802.11b-1999

IEEE Std. 802.11d-2001

IEEE Std. 802.11g-2003

IEEE Std. 802.11h-2003

IEEE Std. 802.11i-2004

IEEE Std. 802.11j-2004

IEEE Std. 802.11e-2005

802.1X The 802.1X standard is a port-based access control standard. 802.1X provides an authorization framework that allows or disallows traffic to pass through a port and thereby access network resources. An 802.1X framework may be implemented in either a wireless or wired environment. The three main components of an 802.1X framework are the supplicant, the authenticator, and the authentication server.

A

acceptable use policy Defines the purpose of the WLAN and how the company employees may utilize the WLAN.

access control list (ACL) Specifies who or what is allowed to access the object and what operations are allowed to be performed on the object (such as an AP or port). The ACL allows or blocks access or function based on a set of policies, identifiers, protocols, and group memberships.

access layer The access layer of the network is responsible for delivery of the traffic directly to the end-user or end node. The access layer ensures the final delivery of packets to the end-user. It is connected to the distribution layer, which is connected to the core.

access point The CWNP definition is a half-duplex wireless device with switch-like intelligence. In reality, an access point is simply a hub with a radio card and an antenna. Access point radios must contend for the half-duplex medium in the same fashion as do the client station radio cards.

accounting Tracking the use of network resources by users. Accounting is an important aspect of network security, and is employed to keep a paper trail of who used what resource, when, and where.

accounting trail A record is kept of user identity, which resource was accessed, and at what time. Keeping such information is often a requirement of many industry regulations, such as the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA).

active attacks Assaults on networks that require the attacker to transmit in order to solicit the desired response from intended victims, such as an injection attack or buffer overflow attack.

Active Directory (AD) Microsoft's adaptation of the Lightweight Directory Access Protocol (LDAP).

active scanning In order for a station to be able to connect to an access point, it first needs to discover an access point. Active scanning is one of the methods that stations use to discover access points. The station and access point will exchange probe requests and probe responses to establish the capabilities of the basic service set.

ad hoc The 802.11 standard defines three topologies, known as service sets. One topology, known as an independent basic service set (IBSS), involves direct communications between 802.11 client stations without the use of an access point. An 802.11 IBSS network is also known as a peer-to-peer network, or an ad hoc network.

Ad Hoc mode A common term used to refer to a station that is configured to connect to an independent basic service set.

ad hoc policy Written policy covering the use of ad hoc networking within an organization.

Additional Authentication Data (AAD) Constructed from portions of the MPDU header, this information is used for data integrity of portions of the MAC header when using CCMP encryption. Receiving stations can then validate the integrity of these MAC header fields.

Advanced Encryption Standard (AES) The AES algorithm, originally named the Rijndael algorithm, is a block cipher that offers much stronger protection than the RC4 streaming cipher. AES is used to encrypt 802.11 wireless data by using an encryption method known as counter mode with Cipher Block Chaining Message Authentication Code (CCMP). The AES algorithm encrypts data in fixed data blocks with choices in encryption key strength of 128, 192, or 256 bits.

Aggregate MAC Protocol Data Unit (A-MPDU) A frame aggregation technique that combines multiple frames into a single frame transmission. All of the 802.11 frames (MPDUs) do not have to have the same destination address. Also, the data payload of each MPDU is encrypted separately by using the multiple dynamic encryption keys that are unique between the access point and each individual client.

Aggregate MAC Service Data Unit (A-MSDU) A frame aggregation technique that combines multiple MSDU payloads into a single frame transmission. The aggregated MSDUs will have a single destination when wrapped together in a single frame. Multiple MSDUs are encrypted by using the same dynamic encryption key.

alarm A record within a WIDS or WIPS that indicates an event has taken place and has been detected by the system. Intrusion and performance alarms can be triggered by signature analysis, spectrum analysis, behavioral analysis, or performance analysis.

all-band interference All-band interference is RF interference that occurs across the entire frequency range that is being used. The term all-band interference is typically associated with frequency hopping spread spectrum (FHSS) communications that disrupt HR-DSSS and/or ERP-OFDM channel communications.

antenna An antenna provides two functions in a communication system. When connected to the transmitter, it collects the AC signal that it receives from the transmitter and directs, or radiates, the RF waves away from the antenna in a pattern specific to the antenna type. When connected to the receiver, it takes the RF waves that it receives through the air and directs the AC signal to the receiver.

applicable audience The person or persons to whom a policy applies.

ARC4 A stream cipher that was designed by Ron Rivest of RSA Security in 1987. RSA never released the algorithm, so unofficial versions of it are often referred to as *Arcfour* or *ARC4*, which stands for "Alleged RC4."

Arcfour *See* ARC4.

association After a station has authenticated with the access point, the next step is for it to associate with the access point. When a client station associates, it becomes a member of a basic service set (BSS). Association means that the client station can send data through the access point and on to the distribution system medium.

asymmetric algorithm An encryption algorithm technique that uses a pair of keys rather than a single key; one key is used for encryption and the other for decryption.

attenuation The decrease of amplitude or signal strength. Also known as signal loss.

attribute value pairs (AVPs) A method of data representation in computing systems. AVPs are often used in RADIUS communications to dynamically assign WLAN users to roles and/or VLANs.

authentication Authentication is the verification of user identity and credentials. Users must identify themselves and present credentials, such as usernames and passwords or digital certificates. More secure authentication systems exist that require multifactor authentication where at least two sets of different credentials must be presented.

authentication attacks Specific attacks launched to crack the authentication mechanism used in a network. These may be active or passive in nature.

authentication server (AS) When an 802.1X/EAP solution is deployed, an authentication server validates the credentials of the supplicant that is requesting access, and notifies the authenticator that the supplicant has been authorized. The authentication server will maintain a user database or may proxy with an external user database to authenticate user credentials.

authenticator When an 802.1X/EAP solution is deployed, a device that blocks or allows traffic to pass through its port entity is known as the authenticator. Authentication traffic is normally allowed to pass through the authenticator while all other traffic is blocked until the identity of the supplicant has been verified.

authenticator nonce (ANonce) A random numerical value that is generated one time only and is used by the authenticator during a 4-Way Handshake frame exchange.

authorization, authentication, and accounting (AAA) AAA is a security concept. Authorization involves granting access to network resources and services. Before authorization to network resources can be granted, proper authentication must occur. Authentication is the verification of user identity and credentials. Accounting is tracking the use of network resources by users. It is an important aspect of network security, and is employed to keep a paper trail of who used what resource, when, and where.

autonomous AP A term for the traditional access point. An autonomous access point contains at least two physical interfaces, usually an RF radio card and a 10/100BaseT port. All configuration settings exist in the autonomous access point itself, and therefore, management and configuration occurs at the access layer. All encryption and decryption mechanisms and MAC layer mechanisms also operate within the autonomous AP. The distribution system service (DSS) and integration service (IS) function within an autonomous AP.

B

bandwidth Wireless communication is typically performed within a constrained set of frequencies known as a *frequency band*. This frequency band is the bandwidth. The term bandwidth is sometimes also used to refer to 802.11 data rates, which are the speed of data transfer. The proper term for the changes in speed due to modulation and coding is data rates; however, they are also often referred to as data bandwidth.

baseline practices Setting a benchmark for normal operations and security. This benchmark is used to monitor variance from the normal operation and security posture, allowing administrators to take corrective measures if required.

basic rates The set of data rates that a client station must be capable of communicating with in order to associate with an access point successfully. Basic rates are required rates with a basic service set (BSS).

basic service area (BSA) The physical area of coverage provided by an access point in a BSS is known as the basic service area (BSA). Client stations may move throughout the coverage area and maintain communications with the AP as long as the signal received between the radios remains above RSSI thresholds. Client stations may also shift between concentric zones of variable data rates that exist within the BSA.

basic service set (BSS) The 802.11 standard defines three topologies known as service sets. One topology, known as the basic service set (BSS), involves communications between a single access point and client stations that are associated with the access point.

basic service set identifier (BSSID) The BSSID address is a 48-bit (6-octet) MAC address used as a unique identifier of a basic service set. In either a BSS or ESS topology, the BSSID address is simply the MAC address of a single access point. In an IBSS topology, the BSSID address is a virtual address.

beacon management frame One of the most important 802.11 frame types, commonly referred to as the beacon. Beacons are essentially the heartbeat of the wireless network. They are sent only by the access point of a basic service set. Client stations transmit beacons only when participating in an IBSS, also known as Ad Hoc mode.

bit A bit is a basic unit of information storage and communication consisting of a single digit, either a 0 (zero) or 1 (one).

block cipher A symmetric key cipher operating on a fixed length of bits, called blocks.

blocks A fixed length of bits used in encryption.

Bluetooth A short-distance RF technology defined by the 802.15 standard. Bluetooth operates using FHSS and hops across the 2.4 GHz ISM band at 1,600 hops per second. Older Bluetooth devices were known to cause all-band interference. Newer Bluetooth devices utilize adaptive mechanisms to avoid interfering with 802.11 WLANs.

Bridged Virtual Interface (BVI) Autonomous access points contain at least two physical interfaces, usually an RF radio card and a 10/100BaseT port. The majority of the time, these physical interfaces are bridged together by a virtual interface known as a Bridged Virtual Interface (BVI). The BVI is assigned an IP address that is shared by the two physical interfaces.

broadcast key When an 802.1X/EAP solution is used with dynamic WEP encryption, a static key known as the broadcast key exists on the access point. The broadcast key is used to encrypt and decrypt all broadcast and multicast 802.11 data frames.

brute-force attacks Sequentially trying every possible key in an attempt to break a code or encryption key.

C

captive portal A technique used largely at wireless hot spots and publicly available Internet connections that forces an HTTP client on a network to be directed to a special web page (usually for authentication or payment purposes) before granting access to the Internet. Captive portal authentication is widely used for guest access WLANs.

Cardholder Data Environment (CDE) Under the PCI standard, the computer environment wherein cardholder data is transferred, processed, or stored. CDE defines the areas that must be protected to reduce cardholder information compromise, including any networks or devices directly connected to that environment.

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) Media access control method used by 802.11 networks. Four mechanisms are used together to ensure that only one station is transmitting at any given time on the half-duplex RF medium. The four mechanisms are physical carrier-sense, virtual carrier-sense, interframe spaces, and the random back-off algorithm.

casual eavesdropping Casual eavesdropping is not considered malicious and is also often referred to as wardriving. Software utilities known as WLAN discovery tools exist for the purpose of finding open WLAN networks. Wardriving is strictly the act of looking for wireless networks, usually while in a moving vehicle. The most common wardriving software tool is a freeware program called NetStumbler.

CBC *See* cipher-block chaining.

CBC-MAC *See* Cipher Block Chaining Message Authentication Code.

CCM *See* Counter with CBC-MAC.

CDMA2000 A hybrid 2.5G/3G technology used in mobile telecommunications standards that utilize CDMA (a multiple access scheme for digital radio) to send voice, data, and signaling data between mobile phones and cell sites.

Challenge Handshake Authentication Protocol (CHAP) An authentication scheme used by Point-to-Point Protocol (PPP) servers to validate the identity of remote clients, which provides protection against playback attacks through the use of an incrementally changing identifier and a variable challenge-value.

change control process A defined method of implementing changes that is intended to reduce disruption of workflow and increase uniformity and compliance.

channel bonding Combining two channels in an effort to increase throughput. Channel bonding takes two 20 MHz wide channels and combines them into 40 MHz of bandwidth. Earlier adoptions in 2.4 GHz were referred to as Super G and blamed for creating interference for other devices in 2.4 GHz. The 802.11n-2009 standard defines 40 MHz channel capabilities for HT compliant radios in both the 2.4 GHz and 5 GHz frequency bands.

cipher An algorithm used to perform encryption.

cipher-block chaining A mode of operation for a block cipher in which a sequence of bits is encrypted as a single unit or block with a cipher key applied to the entire block.

ciphertext The result of a process used to protect information (plaintext) using an encryption cipher.

clear channel assessment (CCA) A Layer 1 process that determines whether the RF medium is busy. 802.11 radios cannot transmit if the RF medium is busy.

client-side policies Policies designed to protect the endpoints of a WLAN as they function both on and off the WLAN.

client station A radio card that is not used in an access point is referred to as a client station. Client station radio cards are typically used in laptops, PDAs, scanners, phones, and many other mobile devices.

client utilities Software used to configure a wireless client card. The software interface will usually have the ability to create multiple connection profiles. Configuration settings of a client utility typically include the SSID, transmit power, security settings, 802.11e/QoS capabilities, and power management.

closed network A wireless service set within which the SSID is not broadcast in the beacon or probe response frames of the APs.

common name (CN) LDAP display name of an object.

Complementary Code Keying (CCK) A spreading/coding technique used by 802.11b cards to provide higher data rates (HR-DSSS).

compliance Functioning within the guidelines of a given standard, policy, or law.

Control and Provisioning of Wireless Access Points (CAPWAP) CAPWAP, as defined in RFC 5415, is a standards-based protocol commonly used for split-MAC architectures for controlling and provisioning of APs.

control frames Control frames help with the delivery of the data frames. Control frames must be able to be heard by all stations; therefore, they must be transmitted at one of the basic rates. Control frames are also used to clear the channel, acquire the channel, and provide unicast frame acknowledgments. They contain only Layer 2 header information.

controlled port A virtual port used during 802.1X/EAP authentication. The authenticator maintains two virtual ports: an uncontrolled port and a controlled port. The uncontrolled port allows EAP authentication traffic to pass through, while the controlled port blocks all other traffic until the supplicant has been authenticated.

core The high-speed backbone of the network. The goal of the core is to carry large amounts of information between key data centers or distribution areas. The core layer does not route traffic or manipulate packets but rather performs high-speed switching. Redundant solutions are usually designed at the core layer to ensure the fast and reliable delivery of packets.

Counter Mode with Cipher Block Chaining Message Authentication Code (CCMP) The default encryption method defined under the 802.11i amendment. This method uses the Advanced Encryption Standard (AES) cipher. CCMP/AES uses a 128-bit encryption key size and encrypts in 128-bit fixed-length blocks. An 8-byte Message Integrity Check (MIC) is used that is considered much stronger than the one used in TKIP. CCMP/AES is the default encryption method defined by WPA2.

cracking Bypassing, resolving, or removing security measures to gain access to networks and or data without permission.

credentials In computer networks, credentials are used to establish identity. Credentials can be something you know, something you have, or something you are.

cryptanalysis The science of decrypting the ciphertext without knowledge of the key or cipher.

cryptography The science of concealing the plaintext and then revealing it.

cryptology The practice or science that includes the techniques used to encrypt and decrypt information.

CTR *See* Counter mode.

cyclic redundancy check (CRC) An error-detecting code.

D

Data Encryption Standard (DES) A block cipher that is based on a symmetric-key algorithm and uses a 56-bit key.

data frames 802.11 data frames carry the Layer 3-7 MSDU payload. The MSDU is usually encrypted for data privacy purposes.

data privacy One of the key components of a wireless security solution. Data privacy is achieved by using encryption.

data rates Data rates are the transmission rates specified by the 802.11 standard and amendments, not actual throughput. Because of medium access methods, aggregate throughput is typically half or less of the available data rate bandwidth.

dBm Compares a signal to 1 milliwatt of power. dBm means decibels relative to 1 milliwatt. Because dBm is a measurement that is compared to a known value, 1 milliwatt, dBm is actually a measure of power.

deauthentication frame A notification frame used to terminate an authentication. Because authentication is a prerequisite for association, disassociation will also occur. Deauthentication cannot be refused by either party.

decryption The process of converting the ciphertext back to plaintext.

dedicated radio A radio in a device that is configured to perform only one function. For example, if an AP has two radios, one could only function as an AP while the other is functioning only as a sensor.

default configurations Options on devices set to manufacturer defaults such as passwords, usernames, channels, security, and power level.

denial of service (DoS) Any individual with ill intent can temporarily disable a Wi-Fi network by preventing legitimate wireless users from accessing network resources. Layer 1 and Layer 2 attacks exist that can deny 802.11 wireless services to legitimate authorized users. 802.11 DoS attacks cannot be prevented, but they can be detected with the proper intrusion detection tools.

dictionary attack A technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by searching likely possibilities from a large file. Often used in brute-force attacks.

Diffie-Hellman A cryptographic protocol that allows two devices to exchange a secret key across an insecure communications channel.

direct link setup (DLS) In most WLAN environments, all frame exchanges between client stations that are associated with the same access point must pass through the access point. DLS allows for client stations to bypass the access point and communicate with each other using direct frame exchanges.

directed probe request 802.11 probe request frame with a specific SSID.

disassociation frame An 802.11 notification frame used to terminate an association. Disassociation is considered a polite way of terminating the association. Disassociation cannot be refused by either party.

distributed spectrum analysis system (DSAS) A WIDS/WIPS solution that uses a centralized server with multiple spectrum analyzer sensors.

distribution layer The distribution layer of the network routes or directs traffic toward the smaller clusters of the network's nodes. The distribution layer routes traffic between VLANs and subnets.

distribution system (DS) The DS is a system used to interconnect a set of basic service sets (BSSs) and integrated local area networks (LANs) to create an extended service set (ESS). The DS consists of a medium used for transport of traffic as well as services used for transport of traffic.

distribution system medium (DSM) The DSM is a logical physical medium used to connect access points. Normally, the DSM is an 802.3 Ethernet backbone; however, the medium can also be wireless or some other type of medium.

distribution system service (DSS) A system service built inside an autonomous access point or WLAN controller usually in the form of software. The distribution system service is used to transport 802.11 traffic.

Duration/ID A field in an 802.11 frame header that is typically used to set the NAV timer in other stations. Used with virtual carrier-sense.

dynamic frequency selection (DFS) Used for spectrum management of 5 GHz channels for 802.11a radio cards. The European Radio communications Committee (ERC) originally mandated that radio cards operating in the 5 GHz band implement a mechanism to avoid interference with radar systems as well as provide equable use of the channels. The DFS service is used to meet the ERC regulatory requirements. This requirement has since become a requirement of other regulatory bodies, such as the FCC in the United States.

dynamic rate switching (DRS) Also known as dynamic rate shifting, adaptive rate selection, or automatic rate selection. A process that client stations use to shift to lower bandwidth capabilities as they move away from an access point and to higher bandwidth capabilities as they move toward an access point. The objective of DRS is upshifting and downshifting for rate optimization and improved performance.

dynamic RF An environment in which a WLAN controller is a centralized device that can dynamically change the configuration of the lightweight access points based on accumulated RF information gathered from the access points' radio cards.

E

Encapsulating Security Payload (ESP) Used for both encryption and authentication of the IP packet. ESP provides origin confidentiality, integrity, and authenticity of packets. ESP does not protect the IP packet header but protects the entire inner IP packet, including the header.

encryption The process of transforming data using a cipher to make it unreadable to anyone except those possessing special knowledge, such as a key.

endpoint policy A policy that governs the security of all client stations.

Enrollee When using Wi-Fi Protected Setup (WPS), the enrollee is the device seeking to join the WLAN.

enterprise encryption gateway (EEG) A specialty 802.11 device that provides for segmentation and encryption. The EEG typically sits behind several fat access points and segments the wireless network from the protected wired network infrastructure. Proprietary encryption technology using the AES algorithm at Layer 2 is provided by the enterprise encryption gateway. Proprietary or specialty supplicants are also often required.

entropy A measure of uncertainty associated with a random variable.

evil twin attack The evil twin attack, also known as wireless hijacking, occurs when a hacker disrupts communications between client stations and a legitimate AP. Client stations lose their connection to the legitimate AP and reconnect to the evil twin access point. The evil twin hijacks the client stations at Layer 1 and Layer 2, allowing the hacker to proceed with peer-to-peer attacks.

Exclusive-OR (XOR) A Boolean algebra function that results in a 0 (false) when two values are the same (0,0 or 1,1), and results in a 1 (true) when two values are different (0,1 or 1,0). XOR is used by many encryption processes.

Extended Rate Physical (ERP) A physical layer specification (PHY) defined for clause 19 radios. This PHY operates in the 2.4 GHz ISM band and uses ERP-OFDM to support data rates of 6–54 Mbps. ERP/DSSS/CCK technology is used to maintain backward compatibility with HR-DSSS (clause 18) radios and DSSS (clause 15) radios.

Extended Rate Physical DSSS/CCK 802.11g clause 19 radios must maintain backward compatibility with 802.11 (DSSS only) and 802.11b (HR-DSSS) radios. A Physical layer (PHY) technology called Extended Rate Physical DSSS (ERP-DSSS/CCK) is used for backward compatibility and support for the data rates of 1, 2, 5.5, and 11 Mbps. This PHY operates in the 2.4 GHz ISM band.

Extended Rate Physical OFDM (ERP-OFDM) A Physical layer (PHY) technology used by 802.11g clause 19 radios to achieve greater bandwidth. Uses OFDM as defined in the 802.11a amendment. Therefore, data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbps are possible using OFDM technology. This PHY operates in the 2.4 GHz ISM band.

Extended Rate Physical PBCC (ERP-PBCC) An optional PHY defined by the 802.11g ratified amendment for clause 19 radios.

extended service set (ESS) The 802.11 standard defines three topologies known as service sets. One topology, known as the extended service set (ESS), involves communications between multiple access points that share a network infrastructure. An ESS is one or more basic service sets that share a distribution system medium.

Extensible Authentication Protocol (EAP) Extensible Authentication Protocol (EAP) is used to provide user authentication for an 802.1X port-based access control solution. EAP is a flexible Layer 2 authentication protocol that resides under Point-to-Point Protocol (PPP).

Extensible Authentication Protocol (EAP) Authentication and Key Agreement (EAP-AKA) An EAP type primarily developed for the mobile phone industry and more specifically for third-generation (3G) mobile networks. EAP-AKA defines the use of the authentication and key agreement mechanisms already being used by the two types of 3G mobile networks. The 3G mobile networks include the Universal Mobile Telecommunications System (UMTS) and CDMA2000. EAP-SIM was primarily developed for the mobile phone industry and more specifically for second-generation (2G) mobile networks.

Extensible Authentication Protocol (EAP) Flexible Authentication via Secure Tunneling (EAP-FAST) Developed by Cisco to be a convenient, easy-to-implement replacement for LEAP, EAP-FAST provides for both mutual authentication and tunneled authentication, just like EAP-PEAP and EAP-TTLS. However, EAP-FAST does not use standards-based X.509 digital certificates to create the TLS tunnel. Instead, EAP-FAST uses PACs.

Extensible Authentication Protocol (EAP) Generic Token Card (EAP-GTC) EAP-GTC is defined in the IETF RFC 3748 and was developed to provide interoperability with existing security token device systems that use one-time passwords (OTP), such as RSA's SecurID solution. The EAP-GTC method is intended for use with security token devices, but the credentials can also be a username and password.

Extensible Authentication Protocol (EAP) Lightweight Extensible Authentication Protocol (EAP-LEAP) A proprietary EAP protocol developed by Cisco, typically referred to simply as LEAP. LEAP is susceptible to offline dictionary attacks.

Extensible Authentication Protocol (EAP) Message Digest 5 (EAP-MD5) A legacy EAP protocol that uses one-way authentication and is susceptible to offline dictionary attacks.

Extensible Authentication Protocol (EAP) over LAN (EAPOL) A method used to encapsulate EAP messages during 802.1X authentication.

Extensible Authentication Protocol (EAP) - PEAPv0 (EAP-MSCHAPv2) Microsoft's EAP-PEAPv0 (EAP-MSCHAPv2) is the most common form of PEAP. The protocol used for user authentication inside the tunnel is EAP-MSCHAPv2. The credentials used for this version of PEAP are usernames and passwords. Client-side certificates are not used and are not supported.

Extensible Authentication Protocol (EAP) PEAPv0 (EAP-TLS) A type of PEAP from Microsoft, EAP-PEAPv0 (EAP-TLS) uses the EAP-TLS protocol for the inner tunnel authentication method. EAP-TLS requires the use of a client-side certificate. The client-side certificate is validated inside the TLS tunnel. No username is used for validation because the client-side certificate serves as the user credentials.

Extensible Authentication Protocol (EAP) PEAPv1 (EAP-GTC) Cisco's implementation of PEAP authentication. EAP-PEAPv1 (EAP-GTC) uses EAP-Generic Token Card (EAP-GTC) for the inner-tunnel authentication.

Extensible Authentication Protocol (EAP) Protected One-Time Password Protocol (EAP-POTP) IETF RFC 4793 defines EAP-Protected One-Time Password Protocol (EAP-POTP), which is an EAP method suitable for use with one-time password (OTP) token devices. EAP-POTP may be used as a better alternative for an internal authentication method inside the TLS tunnel of other protocols, such as EAP-PEAP or EAP-TTLS.

Extensible Authentication Protocol (EAP) Subscriber Identity Module (EAP-SIM) Uses a *Subscriber Identity Module (SIM)* card and specifies an EAP mechanism that is based on 2G mobile network GSM authentication and key agreement primitives. For mobile phone carriers, this is a very valuable piece of information that can be utilized for authentication. EAP-SIM does not offer mutual authentication and key lengths are much shorter than the third-generation mechanisms used in 3G mobile networks.

Extensible Authentication Protocol (EAP) Transport Layer Security (EAP-TLS) Defined in RFC 5216, this is a widely used security protocol, largely considered one of the most secure EAP methods used in WLANs today. It requires the use of client-side certificates in addition to a server certificate.

Extensible Authentication Protocol (EAP) Tunneled Transport Layer Security (EAP-TTLS) Uses a TLS tunnel to protect less secure inner authentication methods and supports more inner authentication methods than PEAP such as the legacy methods of PAP, CHAP, MS-CHAP, and MS-CHAPv2. EAP-TTLS also supports the use of EAP protocols as the inner authentication method.

F

fast basic service set transition (FT) Fast secure roaming mechanisms defined by the 802.11r-2008 amendment.

fast secure roaming (FSR) Mechanisms for faster handoffs when roaming occurs between cells in a wireless LAN using the strong security defined in a robust security network (RSN). Fast and secure 802.11 roaming is needed to meet latency requirements for time-sensitive applications in a WLAN.

Federal Communications Commission (FCC) The FCC is an independent U.S. government agency, directly responsible to the U.S. Congress. It was established by the Communications Act of 1934 and is responsible for regulating interstate and international communications by radio, television, wire, satellite, and cable. The FCC's jurisdiction covers all 50 states, the District of Columbia, and U.S. possessions.

Federal Information Processing Standards (FIPS) In the United States, the National Institute of Standards and Technology (NIST) maintains the Federal Information Processing Standards (FIPS). The FIPS 140-2 standard defines security requirements for cryptography modules. The use of validated cryptographic modules is required by the U.S. government for all unclassified communications. Other countries also recognize the FIPS 140-2 standard or have similar regulations.

fixed mobile convergence (FMC) An environment in which a device with a single telephone number is capable of switching between different communications networks, always using the lowest cost network. FMC devices typically are capable of communicating via either a cellular telephone network or a VoWiFi network.

frame A unit of data at the Data-Link layer.

frequency A term describing a behavior of waves. How fast the waves travel—or more specifically, how many waves are generated over a 1-second period of time—is known as frequency.

functional policy A functional security policy defines the technical aspects of wireless security. The functional security policy establishes how to secure the wireless network in terms of what solutions and actions are needed. A functional policy defines essentials, baseline practices, design, implementation, and monitoring procedures.

G

gain Also known as amplification. Gain is the increase of amplitude or signal strength. The two types of gain are active gain and passive gain.

general policy A general wireless security policy establishes why a wireless security policy is needed for an organization. The general wireless security policy defines a statement of authority, applicable audience, violating policy procedures, risk assessment, threat analysis, and auditing.

Generic Routing Encapsulation (GRE) A process in which frames, such as 802.11 frames, are encapsulated in an IP packet, transmitted between two devices on a network, and then removed from the packet and forwarded.

Global System for Mobile communications (GSM) A second-generation mobile network standard designed to authenticate the subscriber using a preshared key and challenge response. GSM authenticates the user to the network but does not authenticate the network to the user.

Group Key Handshake Used only to issue a new group temporal key (GTK) that has already formed previous security associations. Effectively, the Group Key Handshake is identical to the last two frames of the 4-Way Handshake. The purpose of the Group Key Handshake is to deliver a new GTK to all client stations that already have an original GTK generated by an earlier 4-Way Handshake.

group master key (GMK) A part of the 4-Way Handshake that is randomly created on the access point/authenticator and is used to create the group temporal key (GTK).

group temporal key (GTK) Used to encrypt all broadcast and multicast transmissions between the access point and multiple client stations.

guest network Guest networks are usually created by businesses as a courtesy, providing access to visitors. Most guest networks use captive portal authentication.

H

hacking A term once used to describe making changes to something in order to have it function differently than what it was designed for. When relating to security, this term is used to commonly define breaking into a system, network, or database.

Hashed Message Authentication Codes (HMAC) A type of message authentication code that is calculated using a specific algorithm involving a cryptographic hash function in combination with a secret key.

hertz (Hz) A standard measurement of frequency, which was named after the German physicist Heinrich Rudolf Hertz. An event that occurs once in 1 second is equal to 1 Hz. An event that occurs 325 times in 1 second is measured as 325 Hz.

High Throughput (HT) High Throughput (HT) provides PHY and MAC enhancements to support wireless throughput of 100 Mbps and greater. HT is defined by the 802.11n amendment for clause 20 radios.

High-Rate DSSS (HR-DSSS) The 802.11b 5.5 and 11 Mbps speeds are known as High-Rate DSSS, or HR-DSSS.

hijacking Within an IT context, this term refers to taking over by force a device, network, connection, program, web page, and so on.

honeypot This is a trap set for potential hackers to detect and possibly counteract unauthorized access of a computer network.

hotspot A free or pay-for-use wireless network that is normally used to provide guest access to the Internet.

I

independent basic service set (IBSS) The 802.11 standard defines three topologies known as service sets. One topology, known as an independent basic service set (IBSS), involves direct communications between 802.11 client stations without the use of an access point. An 802.11 IBSS network is also known as a peer-to-peer network or an ad hoc network.

information assurance (IA) The practice of managing information-related risks. By using confidentiality, integrity, authentication, availability, and nonrepudiation, those practicing IA strive to protect assets and related networks and devices.

information elements Variable-length fields that are optional in the body of a management frame.

information fields Fixed-length mandatory fields in the body of a management frame.

infrastructure mode A common term used to refer to a client station that is configured to connect to a basic service set or an extended service set.

Initialization Vector (IV) The IV is utilized by the RC4 streaming cipher that WEP encryption uses. The IV is a block of 24 bits that is combined with a static key. It is sent in cleartext and is different for every frame. The effective key strength of combining the IV with the 40-bit static key is 64-bit encryption. TKIP uses an extended IV.

injection attack This attack uses an arbitrary injection of data to disrupt service, cause buffer overflows, and or gain information or access. Injection attacks are used in EAPOL start floods and WEP cracks.

Institute of Electrical and Electronics Engineers (IEEE) The IEEE is a global professional society with more than 375,000 members. The IEEE's mission is to "promote the engineering process of creating, developing, integrating, sharing, and applying knowledge about electro and information technologies and sciences for the benefit of humanity and the profession."

integration service (IS) Enables delivery of MSDUs between the distribution system (DS) and a non-IEEE-802.11 local area network (LAN), via a portal.

Integrity Check Value (ICV) A data integrity checksum that is computed on data before encryption. The ICV is used to identify if data has been modified.

Inter-Access Point Protocol (IAPP) A protocol used for announcement and handover processes that result in how autonomous APs inform other autonomous APs about roamed clients and that define a method of delivery for buffered packets.

International Organization for Standardization (ISO) The ISO is a global, nongovernmental organization that identifies business, government, and societal needs and develops standards in partnership with the sectors that will put them to use. The ISO is responsible for the creation of the Open Systems Interconnection (OSI) model, which has been a standard reference for data communications between computers since the late 1970s. The OSI model is the cornerstone to data communications, and understanding it is one of the most important and fundamental tasks a person in the networking industry can undertake. The layers of the OSI model are as follows:

Layer 1—Physical

Layer 2—Data-Link

Layer 3—Network

Layer 4—Transport

Layer 5—Session

Layer 6—Presentation

Layer 7—Application

Internet Protocol Security (IPsec) IPsec is a Layer 3 VPN technology. IPsec can use RC4, DES, 3DES, and AES ciphers for encryption. It provides for encryption, encapsulation, data integrity, and device authentication.

Internet Security Association and Key Management Protocol (ISAKMP) A protocol that is used to establish security associations (SA) and cryptographic keys. ISAKMP typically uses Internet Key Exchange (IKE and IKEv2) protocols to set up security associations (SA).

J

jamming The transmission of nonmodulated signals into the air with the intent of disrupting legitimate modulated signals.

K

key A process or algorithm used to transform plaintext into encrypted text; also referred to as cipher.

Key Confirmation Key (KCK) Used to provide data integrity during the 4-Way Handshake and Group Key Handshake.

Key Encryption Key (KEK) Used by the EAPOL-key frames to provide data privacy during the 4-Way Handshake and Group Key Handshake.

keying material Information derived from the mutual authentication exchange of credentials which is used as seeding material to generate a matching dynamic encryption key for both the supplicant and the authentication server.

keying method When data is sent, a signal is transmitted from the transceiver. In order for the data to be transmitted, the signal must be manipulated so that the receiving station has a way of distinguishing 0s and 1s. This method of manipulating a signal so that it can represent multiple pieces of data is known as a keying method. A keying method is what changes a signal into a carrier signal. It provides the signal with the ability to encode data so that it can be communicated or transported.

keystream A stream of random or pseudorandom characters that are combined with a plaintext message to produce an encrypted message.

L

Layer 2 Tunneling Protocol (L2TP) A tunneling protocol used to support virtual private networks (VPNs). L2TP does not provide any encryption or confidentiality by itself but rather relies on an encryption protocol that passes within the tunnel to provide privacy.

Layer 3 roaming Any roaming technology that allows mobile-device users to move from one Layer 3 network to another while maintaining their original IP address.

lightweight access point Lightweight access points are used in a centralized WLAN architecture together with WLAN controllers. A lightweight AP has minimal intelligence and is functionally just a radio card and an antenna. All the intelligence resides in the centralized WLAN controller, and all the AP configuration settings, such as channel and power, are distributed to the lightweight APs from the WLAN controller and stored in the RAM of the lightweight AP. The encryption and decryption capabilities might reside in the centralized WLAN controller or may still be handled by the lightweight APs, depending on the vendor. Lightweight access points tunnel 802.11 wireless traffic to the WLAN controller that is typically deployed at either the distribution or core layer. Lightweight APs are also called controller-based APs or wireless termination points (WTPs).

Lightweight Directory Access Protocol (LDAP) An application protocol for querying and modifying directory services running over TCP/IP. LDAP-compliant databases are often used with RADIUS solutions during proxy authentication.

Logical Link Control (LLC) The upper portion of the Data-Link layer is the IEEE 802.2 Logical Link Control (LLC) sublayer, which is identical for all 802-based networks, although not used by all IEEE 802 networks.

M

MAC filtering Allowing or disallowing connectivity based on the MAC address of cards trying to associate.

MAC Protocol Data Unit (MPDU) An 802.11 frame. The components include a MAC header, an MSDU (data payload), and a trailer.

MAC Service Data Unit (MSDU) The MSDU contains data from the LLC and Layers 3–7. A simple definition of the MSDU is the data payload that contains the IP packet plus some LLC data.

malicious eavesdropping The unauthorized use of protocol analyzers to capture wireless communications is known as malicious eavesdropping and is typically considered illegal. Most countries have laws making it unlawful to listen in on any type of electromagnetic communications such as phone conversations. Unauthorized monitoring of 802.11 wireless transmissions is considered malicious and normally illegal. The most common target of malicious eavesdropping attacks is public access hotspots.

management frame protection (MFP) Techniques used to deliver management frames in a secure manner with the hope of preventing many Layer 2 denial-of-service attacks.

management frames A majority of the frame types in an 802.11 network. Management frames are used by wireless stations to join and leave the network. Another name for an

802.11 management frame is a Management MAC Protocol Data Unit (MMPDU). Management frames do not carry any upper-layer information. There is no MSDU encapsulated in the MMPDU frame body, which carries only Layer 2 information fields and information elements.

man-in-the-middle attack After successfully completing wireless hijacking, an attacker may use a second wireless card with their laptop to execute what is known as a man-in-the-middle attack. The second wireless card is associated with the original legitimate AP. The hacker bridges the second wireless card to the evil twin access point radio and routes all hijacked traffic right back to the gateway of the original network. The attacker can therefore sit in the middle and execute peer-to-peer attacks indefinitely while remaining completely unnoticed.

master session key (MSK) Used to derive the pairwise master key (PMK); also sometimes referred to as the AAA key.

Media Access Control (MAC) The bottom portion of the Data-Link layer is the Media Access Control (MAC) sublayer, which is identical for all 802.11-based networks.

mesh networking A network environment in which wireless mesh access points communicate with each other using proprietary Layer 2 routing protocols, creating a self-forming and self-healing wireless infrastructure (a mesh) over which edge devices can communicate.

mesh point (MP) Any 802.11 device capable of using a mandatory mesh routing protocol called Hybrid Wireless Mesh Protocol (HWMP).

mesh point portal (MPP) Any 802.11 device that provides both mesh functionality and acts as a gateway to one or more external networks such as an 802.3 wired backbone.

Message Digest 5 (MD5) A widely used cryptographic hash function with a 128-bit hash value that has been shown not to be collision resistant and, as such, is not suitable for applications like SSL certificates or digital signatures that rely on this property. This hash is typically expressed as a 32-digit hexadecimal number.

Message Integrity Check Code (MIC) TKIP uses a data integrity check known as the Message Integrity Code (MIC) to mitigate known bit-flipping attacks against WEP. The MIC is sometimes referred to by the nickname Michael. It is also sometimes referred to as a Message Integrity Check.

Microsoft Point-to-Point Encryption (MPPE) MPPE is a 128-bit encryption method that uses the RC4 algorithm. MPPE is used with Point-to-Point Tunneling Protocol (PPTP) VPN technology.

Mobile IP An Internet Engineering Task Force (IETF) standard protocol that allows mobile-device users to move from one Layer 3 network to another while maintaining their original IP address. Mobile IP is defined in IETF Request for Comments (RFC) 3344.

mobility domain A set of basic service sets (BSSs), within the same extended service set (ESS), that support fast BSS transitions between themselves.

modulation The manipulation of a signal so that the receiving station has a way of distinguishing 0s and 1s.

modulation coding schemes (MCS) As mandated by the 802.11n-2009 amendment, data rates for clause 20 HT radios are defined by multiple variables known as modulation coding schemes (MCS). Non-HT radios that used OFDM technology (802.11a/g) defined data rates of 6 Mbps–54 Mbps based on the modulation that was used. HT radios, however, define data rates based on numerous factors, including modulation, the number of spatial streams, channel size, and guard interval.

multifactor authentication The use of more than one set of credentials to be presented for user validation.

multipath A propagation phenomenon that results in two or more paths of a signal arriving at a receiving antenna at the same time or within nanoseconds of each other.

multiple channel architecture (MCA) A WLAN channel reuse pattern with overlapping coverage cells that utilizes three channels at 2.4 GHz or numerous channels at 5 GHz.

multiple-input multiple-output (MIMO) Any RF communications system that uses multiple antennas at both the transmitter and receiver to improve communication performance. MIMO communications are used by 802.11n radios.

N

National Institute of Standards and Technologies (NIST) A federal technology agency that develops and promotes measurement, standards, and technology in the United States.

Near Field Communication (NFC) A short-range wireless communication technology that operates at 13.56 MHz.

Network Access Control (NAC) A computer network security methodology that integrates endpoint security technology (such as antivirus host patch versions) with user authentication.

Network Allocation Vector (NAV) A timer mechanism that maintains a prediction of future traffic on the medium based on duration value information seen in a previous frame transmission. When an 802.11 radio is not transmitting, it is listening. When the listening radio hears a frame transmission from another station, it looks at the header of the frame and determines whether the Duration/ID field contains a Duration value or an ID value. If the field contains a Duration value, the listening station will set its NAV timer to this value. The listening station will then use the NAV as a countdown timer, knowing that the RF medium should be busy until the countdown reaches 0.

noise floor A measurable level of background noise. This is often compared to received signal amplitudes. *See* signal-to-noise ratio (SNR).

nonce A random or pseudo-random value issued in an authentication protocol to ensure that previous communications cannot be reused in replay attacks.

nonroot bridge Wireless bridges support two major configuration settings: root and nonroot. Bridges work in a parent/child type of relationship, so think of the root bridge as the parent and the nonroot bridge as the child.

notification An alert message sent from a monitoring system, such as a WIPS, when a detected behavior or device meets configured criteria within the monitoring system. The message is sent to an administrator, monitoring system, or database. This could be done via email, SMS, SNMP, FTP, or any means supported by the WIDS/WIPS and the intended recipient.

null probe request A probe request management frame with no SSID information.

O

octet A series of 8 bits used to form a single byte.

one-time password (OTP) A password that is valid only for a single login session or transaction.

Open System authentication Open System authentication is the simpler of the two 802.11 authentication methods. It provides authentication without performing any type of client verification. It is essentially an exchange of hellos between the client and the access point.

opportunistic PMK caching A commonly used FSR method not defined by the 802.11-2007 standard. OKC allows for PMK caching between multiple APs that are under some sort of administrative control.

organizational unit (OU) A container object used in LDAP.

Organizationally Unique Identifier (OUI) This is a 24-bit number that is purchased from and registered with the Institute of Electrical and Electronics Engineers (IEEE). It is intended to be an identifier uniquely given to a vendor, manufacturer, or other organization that reserves a block of each possible type of derivative identifier (such as MAC addresses) for the exclusive use of the assignee.

Orthogonal Frequency Division Multiplexing (OFDM) Orthogonal Frequency Division Multiplexing is one of the most popular communications technologies used in both wired and wireless communications. As part of 802.11 technologies, OFDM is specified in the 802.11a and 802.11g amendments and can transmit at speeds of up to 54 Mbps. OFDM technology is also used by 802.11n HT radios. OFDM transmits across separate, closely and precisely spaced frequencies, often referred to as subcarriers.

P

packet A unit of data at the Network layer.

packet analysis Decoding frames to determine content, frame type, origin, and destination.

packet spoofing Creating and transmitting fake traffic with the intent of masquerading as a different device, disrupting service, or compromising a device or network.

pairwise master key (PMK) A cryptographic key that is used to derive lower-level keys.

pairwise transient key (PTK) Used to encrypt all unicast transmissions between a client station and an access point. Each PTK is unique between each individual client station and the access point. Every client station possesses a unique PTK for unicast transmissions between the client STA and the AP. PTKs are used between a single supplicant and a single authenticator.

passive scanning In order for a station to be able to connect to an access point, it needs first to discover an access point. Passive scanning involves the client station listening for the beacon frames that are continuously being sent by the access points.

passphrase A simple ASCII character string.

passphrase-PSK mapping A formula used to create a PSK from a static passphrase used with PSK authentication.

Password Authentication Protocol (PAP) Defined in RFC 1334, PAP provides no protection to the peer identity. It was originally designed for use with Point-to-Point Protocol (PPP). Although rarely used, PAP would only be logical to use inside an encrypted TLS tunnel because of its insecure nature.

Peer Key Handshake Occurs as part of the TDLS Direct Link setup procedure and is executed between the two non-AP STAs that intend to establish an RSNA for direct link communication.

peer-to-peer See independent basic service set (IBSS).

peer-to-peer attack A wireless client station can attack the resources of any peer 802.11 client station in the same 802.11 service set. Peer-to-peer attacks can occur in any ad hoc network or through any access point or Wi-Fi switch where client stations share an association. Wireless peer-to-peer attacks can be mitigated with a personal firewall on the client side or through the use of PSPF on the access point or Wi-Fi switch.

penetration testing This is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source. Some refer to this as authorized hacking, not just looking for vulnerabilities but exploiting them to simulate what an actual attacker could find or do.

per session, per user After an EAP frame exchange where mutual authentication is required, both the AS and the supplicant know information about each other because of the exchanging of credentials. This newfound information is used as seeding material or keying material to generate a matching dynamic encryption key for both the supplicant and the authentication server. These dynamic keys are generated per session per user, meaning that every time a client station authenticates, a new key is generated and every user has a unique and separate key.

periodic scans The occasional or scheduled use of laptop-based or handheld devices to conduct scanning for devices and communications within or outside a given policy or standard.

personal information number (PIN) Password used to access resources.

phishing The criminally fraudulent process of attempting to acquire sensitive information, such as usernames, passwords, and credit card details, by masquerading as a trustworthy entity in an electronic communication. These attacks can range from email scams to devices placed to lure victims onto what appears to be a real network.

physical carrier-sense Performed constantly by all stations that are not transmitting or receiving data. Determines whether a frame transmission is inbound for a station to receive or whether the medium is busy before transmitting. This is known as the clear channel assessment (CCA).

Physical Layer Convergence Procedure (PLCP) The upper portion of the Physical layer. PLCP prepares the frame for transmission by taking the frame from the MAC sublayer and creating the PLCP Protocol Data Unit (PPDU).

Physical Medium Dependent (PMD) The lower portion of the Physical layer. The PMD sublayer modulates and transmits the data as bits.

plaintext Unencrypted information or data.

PLCP Protocol Data Unit (PPDU) When the PLCP receives the PSDU, it prepares the PSDU to be transmitted and creates the PLCP Protocol Data Unit (PPDU). The PLCP adds a preamble and PHY header to the PSDU.

PLCP Service Data Unit (PSDU) Equivalent to the MPDU. The MAC layer refers to the frame as the MPDU, whereas the Physical layer refers to this same exact frame as the PSDU.

PMK caching A fast secure roaming method used by APs and client stations to maintain PMKSAs for a period of time while a client station roams to a target AP and establishes a new PMKSA. An authenticator and a client station can cache multiple PMKs.

point-to-multipoint (PtMP) A wireless network configuration that has a central communications device, such as a bridge or an access point, providing connectivity to multiple devices, such as other bridges or clients.

point-to-point (PtP) A wireless network configuration that connects only two devices together. This is typically a wireless bridge link.

Point-to-Point Tunneling Protocol (PPTP) PPTP is a Layer 3 VPN technology. It uses 128-bit Microsoft Point-to-Point Encryption (MPPE), which uses the RC4 algorithm. MPPE encryption is considered adequate but not strong. PPTP also uses MS-CHAP version 2 for user authentication, which is susceptible to offline dictionary attacks.

port-based access control The 802.1X standard defines port-based access control. 802.1X provides an authorization framework that allows or disallows traffic to pass through a port and thereby access network resources. 802.1X defines two virtual ports: an uncontrolled port and a controlled port. The uncontrolled port allows EAP authentication traffic to pass through, while the controlled port blocks all other traffic until the supplicant has been authenticated.

port lookup A query sent to a managed switch, usually via SNMP, to determine the switch port to which a device is detected as being connected.

port suppression Sending an SNMP set statement to a managed switch telling the switch to disable a specific port. This is a method of rogue mitigation used in both wired and wireless IDS deployments.

Power over Ethernet (PoE) A solution that can be used to power remote network devices over the same Ethernet cabling that carries data to the remote device. Using PoE to provide power to 802.11 access points is often a simpler and more cost-effective solution than hiring an electrician to install new electrical drops and outlets for every AP.

preauthentication A fast secure roaming method used by clients to establish a new PMKSA with an AP prior to roaming to the AP. Preauthentication allows a client station to initiate a new 802.1X/EAP exchange with a RADIUS server while associated with the original AP.

preshared keys (PSKs) A method of distributing encryption passphrases or keys by manually typing the matching passphrases or keys on both the access point and all client stations that will need to be able to associate to the wireless network. This information is shared ahead of time (preshared) by using a manual distribution method such as telephone, email, or face-to-face conversation.

pretexting Fraudulently obtaining personal information under false pretenses.

Privacy Rule A portion of HIPAA compliance that is designed to assure that health information is properly protected while still allowing the flow of information about an individual's health that is needed to provide and promote high-quality health care as well as protecting the public's health and well-being.

private branch exchange (PBX) A telephone exchange that serves a particular business or office.

private key A decryption key that is typically kept secret. Also called a secret key.

probe request An 802.11 management frame that is transmitted during active scanning. A client station that is looking for an SSID sends a probe request. Access points that hear the probe request will send a probe response, notifying the client of the access points' presence. If a client station receives probe responses from multiple access points, signal strength and quality characteristics are typically used by the client station to determine which access point has the best signal and thus to which access point it should connect.

probe response An 802.11 management frame that is transmitted during active scanning. After a client station sends a probe request, access points that hear the probe request will send a probe response, notifying the client of the access points' presence. The information that is contained inside the body of a probe response frame is the exact same information that can be found in a beacon frame, with the exception of the traffic indication map (TIM).

probe response flood This is a mass transmission of fake probe response frames to a station that may result in the attacker being able to phish the station away from the legitimate AP and onto their own device because the target believes it tried to connect to the AP listed in the response.

proprietary PSK A vendor-specific preshared key method mitigates social engineering and employee sharing of the passphrase.

Protected Access Credential (PAC) A credential used with EAP-FAST.

protocol analysis The employing of proper software and/or hardware tools to capture, decode, and interpret the contents of data packets as they travel in a given media.

proxy authentication A proxy query to a preestablished LDAP-compliant database.

pseudo-random function (PRF) Hashes various inputs to derive a pseudo-random value and expands a key and a seed to a pseudo-random output, usually of a variable length.

public key An encryption key that is part of a key pair. The public key is shared, allowing others to encrypt data to be sent to the person who shared the key. This data can only be decrypted with the private key that is typically known only to the creator of the key pair.

public key infrastructure (PKI) An arrangement that binds public keys with respective user identities by means of a certificate authority.

Public Secure Packet Forwarding (PSPF) PSPF is a feature that can be enabled on WLAN access points or switches to block wireless clients from communicating with other wireless clients on the same wireless segment. With PSPF enabled, client devices cannot communicate with other client devices on the wireless network. PSPF is a term most commonly used by Cisco; other vendors have similar capabilities under different names. PSPF is useful in preventing peer-to-peer attacks through an access point.

public switched telephone network (PSTN) The public network of telephone systems and providers.

push-button configuration (PBC) Previously called Wi-Fi Simple Config. In some Wi-Fi Protected Setup networks, the user may connect multiple devices to the network and enable data encryption by pushing a button. The access point/wireless router will have a physical button, and other devices may have a physical or software-based button.

Q

Quality of service (QoS) The attempt to prioritize and provide certain levels of predictable throughput along a shared access medium.

quality-of-service basic service set (QBSS) An 802.11 basic service set that provides quality of service (QoS). An infrastructure QBSS contains an 802.11e-compliant access point.

Queensland Attack A DoS attack that exploits the CCA functionality in a WLAN, making devices believe the medium is busy and not allowing the devices to transmit since they are forced to back off.

R

radio chain A single radio and all of its supporting architecture including mixers, amplifiers, and analog/digital converters.

radio resource measurement (RRM) A mechanism in which client station resource data is gathered and processed by an access point or WLAN controller.

rainbow table A lookup table offering a time-memory trade-off used in recovering plaintext passwords; a variant of a dictionary used in brute-force attacks.

range The area or distance that an RF signal can provide effective usable coverage.

RC4 The RC4 algorithm is a streaming cipher used in technologies that are often used to protect Internet traffic, such as Secure Sockets Layer (SSL). The RC4 algorithm is used to protect 802.11 wireless data and is incorporated into two encryption methods known as WEP and TKIP.

RC5 A symmetric block cipher that was designed by Ron Rivest in 1994, and a U.S. patent was granted in May 1997. RC5 allows for a variable block size, a variable key size, and a variable number or rounds. The block size can be set to 32, 64, or 128 bits; the key size can range from 0 bits to 2,040 bits; and the number of rounds can range from 0 to 255. A key table is created, with the size of the table varying depending on the number of rounds that will be performed. When the user-provided secret key is entered, a key-expansion routine will expand the user-provided key to fill the key table. This key table is used for both encryption and decryption.

real-time location system (RTLS) Software and hardware solutions that can track the location of any 802.11 radio device as well as active Wi-Fi RFID tags.

reassociation When a client station decides to roam to a new access point, it will send a reassociation request frame to the new access point. It is called a reassociation, not because it is reassociating to the access point, but because it is reassociating to the SSID of the wireless network.

receive sensitivity The amount of signal a wireless station must receive in order to distinguish between data and noise.

received amplitude The received signal strength is most often referred to as received amplitude. RF signal strength measurements taken during a site survey is an example of received amplitude.

received signal strength A measurement of the amount of signal received.

received signal strength indicator (RSSI) An optional 802.11 parameter with a value from 0 to 255. It is designed to be used by the hardware manufacturer as a relative measurement of the RF power that is received. The RSSI is one of the indicators that is used by a wireless device to determine whether another device is transmitting, also known as a clear channel assessment (CCA).

receiver The receiver is the final component in the wireless medium. The receiver takes the carrier signal that is received from the antenna and translates the modulated signals into 1s and 0s. It then takes this data and passes it to the computer to be processed.

Registrar The Registrar issues credentials to Enrollees. The role of the Registrar may be integrated into an AP or as a separate device residing behind several APs. Because WPS is intended for use in a SOHO environment, the Registrar will usually be integrated within the AP and an External Registrar will not be needed.

regulatory domain authority Local regulatory domain authorities of individual countries or regions define the spectrum policies and transmit power rules.

remote-access WLAN policy A policy covering the use of wireless stations gaining access to the organization's network through an external wireless connection (not part of the organization's WLAN).

remote AP Enables any access point to be securely and easily connected from a remote location to a WLAN controller across the Internet.

Remote Authentication Dial-In User Service (RADIUS) A networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management.

RF fingerprinting Determining and labeling devices and their actions based on a known set of behaviors. This is also a term used in location tracking when comparing signal values of the device being tracked with a set of known signal values and locations.

Rijndael algorithm A cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen.

risk assessment A process used in determining the level of acceptable risk within a process or organization; a weighing of the exposure against the benefit of use.

risk mitigation Reducing the exposure to and impact of risks by the identification, assessment, and prioritization of risks paired with the allocation of resources to minimize, monitor, and control the probability and or impact of events.

roaming The ability for the client stations to transition from one access point and basic service set (BSS) to another while maintaining network connectivity for the upper-layer applications.

robust security network (RSN) A robust security network (RSN) is a network that only allows for the creation of robust security network associations (RSNAs). An RSN utilizes CCMP/AES encryption as well as 802.1X/EAP authentication.

robust security network associations (RSNAs) As defined by the 802.11i security amendment, two stations (STAs) must establish a procedure to authenticate and associate with each other as well as create dynamic encryption keys through a process known as the 4-Way Handshake. This association between two stations is referred to as a robust security network association (RSNA).

robust security network information element (RSNIE) Often referred to simply as the RSN information element. An information element is an optional field of variable length that can be found in 802.11 management frames. The RSN information element can identify the encryption capabilities of each station. The RSN information element will also indicate whether 802.1X/EAP authentication or preshared key (PSK) authentication is being used.

rogue access point A rogue access point is any wireless device that is connected to the wired infrastructure but is not under the management of the proper network administrators. The rogue device acts as a portal into the wired network infrastructure. Because the rogue device has no authorization or authentication security in place, any intruder can use the open portal to gain access to network resources.

rogue station An unauthorized station that is associated with an authorized access point.

role-based access control (RBAC) Role-based access control (RBAC) is an approach to restricting system access to authorized users. The three main components of an RBAC approach are users, roles, and permissions. Separate roles can be created such as the sales role or the marketing role. Individuals or groups of users are assigned to one of these roles. Permissions can be defined as firewall permissions, Layer 2 permissions, Layer 3 permissions, or bandwidth permissions, and they can be time based. The permissions are then mapped to the roles. When wireless users authenticate via the WLAN, they inherit the permissions of whatever roles to which they have been assigned.

root bridge Wireless bridges support two major configuration settings: root and nonroot. Bridges work in a parent/child type of relationship, so think of the root bridge as the parent and the nonroot bridge as the child.

round function An iterative process or function used in block cipher creation.

S

Sarbanes-Oxley Defines more stringent controls on corporate accounting and auditing procedures with a goal of corporate responsibility and enhanced financial disclosure. The act is named *Sarbanes-Oxley* after Senator Paul Sarbanes and Representative Michael Oxley, the key figures who drafted it in 2002.The legislation set new or enhanced standards for all U.S. public company boards, management, and public accounting firms.

scope of work agreement (SOW) A division or description of work to be performed under a contract or subcontract in the completion of a project.

secret key A decryption key typically kept secret. Also called a private key.

Secure Hash Algorithm 1 (SHA-1) A cryptographic hash function that is employed in several widely used security applications and protocols.

Secure Socket Layer (SSL) A cryptographic protocol normally used to provide secure communications over the Internet. SSL uses end-to-end encryption at the Transport layer of the OSI model.

security associations (SA) The establishment of shared security information between two network devices to support secure communication.

security auditing Defines internal auditing procedures as well as the need for independent outside audits.

security token Any physical device that an authorized user of computer services is given to ease authentication.

segmentation The splitting of a computer network into subnetworks. Traffic from the split networks is placed on separate VLANS or cable segments.

service set identifier (SSID) The SSID is a logical name used to identify an 802.11 wireless network. The SSID wireless network name is the logical name of the WLAN. The SSID can be made up of as many as 32 characters and is case sensitive.

service sets Three separate 802.11 topologies that describe how radio cards may be used to communicate with each other. The three 802.11 topologies are known as a basic service set (BSS), an extended service set (ESS), and an independent basic service set (IBSS).

Shared Key authentication The more complex of the two 802.11 authentication methods. Shared Key authentication uses WEP to authenticate client stations and requires

that a static WEP key be configured on both the station and the access point. In addition to WEP being mandatory, authentication will not work if the static WEP keys do not match. The authentication process is similar to Open System authentication, but includes a challenge and response between the AP and client station.

shared secret A preshared key between the client and the authentication server.

signal strength The magnitude of the electric field at a reference point that is a significant distance from the transmitting antenna.

signal-to-noise ratio (SNR) The SNR is the difference in decibels between a received signal and the background noise. The SNR is an important value because, if the background noise is too close to the received signal, data can get corrupted and retransmissions will increase.

single channel architecture (SCA) A WLAN architecture in which all access points in the network can be deployed on one channel in either the 2.4 GHz or 5 GHz frequency bands. Uplink and downlink transmissions are coordinated by a WLAN controller on a single 802.11 channel in such a manner that the effects of co-channel and adjacent-channel interference are minimized.

single-input single-output (SISO) A system that makes use of a single radio chain.

site survey A process performed to determine RF coverage, potential sources of interference, and the proper placement, installation, and configuration of 802.11 hardware.

small and medium-sized businesses (SMBs) Businesses with 100 or fewer employees are referred to as small businesses; those having 101 to 999 employees are referred to as medium sized.

small office/home office (SOHO) A common reference to the office environment of self-employed people, satellite employees, or an environment in which someone is likely to bring work home with them.

smart card Any pocket-sized card with embedded integrated circuits that can process data. A smart card is also often referred to as an *integrated circuit card (ICC)*.

social engineering A technique used to manipulate people into divulging confidential information such as computer passwords.

software-defined radio (SDR) A future technology that will be able to dynamically switch across a wide range of frequency bands, transmission techniques, and modulation schemes so that a single radio could replace multiple products.

spectrum analysis Locating sources of interference in the 2.4 GHz ISM and 5 GHz UNII bands is considered mandatory when performing an 802.11 wireless site survey. Using a spectrum analyzer to determine the state of the RF environment within a certain frequency range is known as spectrum analysis.

spectrum analyzer Spectrum analyzers are frequency domain measurement devices that can measure the amplitude and frequency space of electromagnetic signals. A spectrum analyzer is a tool that should always be used to locate sources of interference during an 802.11 wireless site survey. Spectrum analyzers are also used for security purposes to locate Layer 1 DoS attacks. Most spectrum analyzers are stand-alone devices, but distributed solutions exist that can be used as Layer 1 intrusion detection systems.

split MAC architecture With this type of WLAN architecture, some of the MAC services are handled by the WLAN controller and some are handled by the lightweight access point. For example, the integration service (IS) and the distribution system service (DSS) are handled by the controller. WMM QoS methods are usually handled by the controller. Depending on the vendor, encryption, and decryption of 802.11 data, frames might be handled by the controller or by the AP. Some 802.11 management frames, such as beacons and ACKs, might originate at the AP instead of the WLAN controller.

spoof To clone or create fraudulent traffic or configurations.

stakeholder Any person, group, or organization that has a direct or indirect stake in a process or entity because they can affect, or be affected by, the process or entity's actions, objectives, and or policies.

state A block size of 128 bits, which is actually a 4×4 array of bytes used in AES.

statement of authority Defines who put the WLAN policy in place and the executive management that backs the policy.

station (STA) The main component of an 802.11 wireless network is the radio card, which is referred to by the 802.11 standard as a station (STA). The radio card can reside inside an access point or be used as a client station.

station-to-station link (STSL) A direct link established between two stations.

steganography Derived from the Greek language, meaning "concealed writing." Unlike cryptography, where the goal is to make the message unreadable to someone without access to the key or cipher, steganography strives to hide the fact that there is a message.

stream cipher A symmetric key cipher where plaintext bits are combined with a pseudorandom cipher bit stream called the keystream.

STSL master key (SMK) Used to derive the STSL transient key (STK); the SMK is a random value generated by an AP.

STSL transient key (STK) Used during a peer-key handshake and derived from the STK.

Subscriber Identity Module (SIM) An embedded identification and storage device very similar to a smart card.

supplicant When an 802.1X/EAP solution is deployed, a host with software that is requesting authentication and access to network resources is known as the supplicant.

supported rates The set of data rates that the access point will use when communicating with an associated station.

symmetric algorithm A class of algorithms that use trivially related, often identical, cryptographic keys for both decryption and encryption functions.

T

task group Various 802.11 task groups are in charge of revising and amending the original standard that was developed by the MAC Task Group (MAC) and the PHY Task Group (PHY). Each group is assigned a letter from the alphabet, and it is common to hear the term 802.11 alphabet soup when referring to all the amendments created by the multiple 802.11 task groups. Quite a few of the 802.11 task group projects have been completed, and amendments to the original standard have been ratified. Other 802.11 task group projects still remain active and exist as draft amendments.

Temporal Key (TK) The temporal encryption key used to encrypt/decrypt the MSDU payload of 802.11 data frames between the supplicant and the authenticator.

Temporal Key Integrity Protocol (TKIP) TKIP is an enhancement of WEP encryption that addresses many of the known weaknesses of WEP. TKIP starts with a 128-bit temporal key that is combined with a 48-bit Initialization Vector (IV) and source and destination MAC addresses in a complicated process known as per-packet key mixing. TKIP also uses sequencing and uses a stronger data integrity check known as the Message Integrity Check (MIC). TKIP is the mandatory encryption method under WPA and is optional under WPA2.

Temporal Key Integrity Protocol (TKIP) countermeasures Countermeasures used to protect against active attacks against the TKIP MIC.

Temporal Key Integrity Protocol (TKIP) mixed transmit address and key (TTAK) After the 128-bit temporal key is created, the two-phase key mixing process begins. A 48-bit TKIP sequence counter (TSC) is generated and broken into 6 octets labeled TSC0 (least significant octet) through TSC5 (most significant octet). Phase 1 key mixing combines the appropriate temporal key (pairwise or group) with the TSC2 through TSC5 octets of the TKIP sequence counter as well as the *transmit address (TA)*. The TA is the MAC address of the transmitting 802.11 radio. The output of the Phase 1 key mixing is the creation of the TKIP-mixed transmit address and key (TTAK).

Temporal Key Integrity Protocol (TKIP) sequence counter (TSC) A process used by TKIP to sequence the MPDUs a device sends. An 802.11 station drops all MPDUs that are received out of order. Sequencing is designed to defeat replay and reinjection attacks that are used against WEP.

threat analysis Also called risk assessment, threat analysis defines the potential wireless security risks and threats and what the financial impact will be on the company if a successful attack occurs.

throughput A measurement of the amount of user data that successfully traverses the network over a period of time.

Time Difference of Arrival (TDoA) This method uses the variation of arrival times of the same transmitted signal at three or more receivers to help determine the location of the transmitting device. Time Difference of Arrival (TDoA) can also be called multilateration or hyperbolic positioning.

topology The physical and/or logical layout of nodes in a computer network.

transceiver A radio that is capable of both transmitting and receiving.

transform set A combination of the security protocols and algorithms that will be used to protect data.

transition security network (TSN) An 802.11 wireless network that allows for the creation of pre-robust security network associations (pre-RSNAs) as well as RSNAs is known as a transition security network. A TSN supports 802.11i-defined security as well as legacy security, such as WEP, within the same BSS.

transmit address (TA) The MAC address of the transmitting 802.11 radio.

transmit amplitude The amount of initial amplitude that leaves the radio transmitter.

transmit opportunity (TXOP) A limited-duration controlled access phase, providing contention-free transfer of QoS data.

transmit power control (TPC) Part of the 802.11h amendment. TPC is used to regulate the power levels used by 802.11a radio cards. The ERC and the FCC mandate that radio cards operating in the 5 GHz band use TPC to abide by a maximum regulatory transmit power and are able to alleviate transmission power to avoid interference. The TPC service is used to meet the ERC and FCC regulatory requirements.

transmitter The initial component in the creation of the wireless medium. The computer hands the data off to the transmitter, and it is the transmitter's job to begin the RF communication.

Transport Layer Security (TLS) A cryptographic protocol normally used to provide secure communications. Just like SSL, the TLS protocol uses end-to-end encryption at the Transport layer of the OSI model.

triangulation A process of determining the location of a point by measuring angles to it from known points. Triangulation, as it relates to WIDS/WIPS, is a way of using signals detected by sensors that are in known locations to find devices that are in unknown locations.

trilateration Deriving a location based on known distances from other locations using circular patterns.

Triple Data Encryption Algorithm (TDEA) *See* Triple DES (3DES).

Triple DES (3DES) The Triple Data Encryption Algorithm (TDEA) block cipher that applies the Data Encryption Standard (DES) cipher algorithm three times to each data block without requiring a completely new block cipher algorithm.

tunneled authentication Used to protect the exchange of client credentials between the supplicant and the AS within an encrypted TLS tunnel.

two-factor authentication *See* multifactor authentication.

U

uncontrolled port A virtual port used during 802.1X/EAP authentication. The authenticator maintains two virtual ports: an uncontrolled port and a controlled port. The uncontrolled port allows EAP authentication traffic to pass through, while the controlled port blocks all other traffic until the supplicant has been authenticated.

unicast key A dynamically generated encryption key that is generated per session per user is often referred to as the unicast key. Unicast keys are used to encrypt and decrypt all unicast 802.11 data frames.

Universal Mobile Telecommunications System (UMTS) The European standard for 3G mobile communications systems providing an enhanced range of multimedia services.

Unlicensed National Information Infrastructure (UNII) The IEEE 802.11a amendment designated OFDM data transmissions within the frequency space of the 5 GHz UNII bands. The 802.11a amendment defined three groupings, or bands, of UNII frequencies, known as UNII-1 (lower), UNII-2 (middle), and UNII-3 (upper). All three of these bands are 100 MHz wide and each has four channels. The IEEE 802.11h amendment introduced the capability for 802.11 radios to transmit in a new frequency band called UNII-2 Extended with 11 more channels. The 802.11h amendment effectively is an extension of the 802.11a amendment.

The UNII bands are as follows:

UNII-1 (lower) is 5.15–5.25 GHz.

UNII-2 (middle) is 5.25–5.35 GHz.

UNII-2 Extended is 5.47-5.725 GHz.

UNII-3 (upper) is 5.725–5.825 GHz.

V

vendor-specific attributes (VSAs) Provides functionality that is not supported in standard attributes.

violation reporting Documenting variance from compliance mandates or from stated written policy.

virtual AP Multiple SSIDs configured on a single physical AP, where each SSID is mapped to a unique BSSID.

virtual branch offices Off-site offices and home offices which connect to the main office.

virtual BSSID The BSSID is typically the MAC address of the access point's radio card and the Layer 2 identifier of a basic service set (BSS). Because access points are capable of advertising multiple SSIDs, and because each SSID requires a separate BSSID, the access point will generate virtual BSSID addresses.

virtual carrier-sense A CSMA/CA mechanism used by listening 802.11 stations. When the listening radio hears a frame transmission from another station, it looks at the header of the frame and determines whether the Duration/ID field contains a Duration value or an ID value. If the field contains a Duration value, the listening station will set its NAV timer to this value. The listening station will then use the NAV as a countdown timer, knowing that the RF medium should be busy until the countdown reaches 0.

virtual local area network (VLAN) Virtual local area networks (VLANs) are used to create separate broadcast domains in a Layer 2 network and are often used to restrict access to network resources without regard to the physical topology of the network. In a WLAN environment, individual SSIDs can be mapped to individual VLANs and users can be segmented by the SSID/VLAN pair, all while communicating through a single access point.

virtual private network (VPN) A private network that is created by the use of encryption, tunneling protocols, and security procedures. VPNs are typically used to provide secure communications when physically connected to an insecure network.

Voice over IP (VoIP) Voice over Internet Protocol. The transmission of voice conversations over a data network using TCP/IP protocols.

Voice over Wi-Fi (VoWiFi) Any software or hardware that uses Voice over IP communications over an 802.11 wireless network is known as VoWiFi. Because of latency concerns, VoWiFi requires QoS mechanisms to function properly in an 802.11 BSS.

VPN client A station that initiates the connection by trying to communicate with the VPN server.

VPN tunnel Encapsulated traffic on a public network.

VPN wireless routers VPN wireless routers have all the same features that can be found in a SOHO wireless router, along with providing secure tunneling functionality in addition to 802.11 Layer 2–defined security capabilities. Supported VPN protocols may include PPTP, L2TP, IPsec, and SSH2.

W

wardriving Wardriving is the act of looking for wireless networks, usually while in a moving vehicle. Software utilities, known as WLAN discovery tools, exist for the purpose of finding open WLAN networks. The most common wardriving software tool is a freeware program called NetStumbler.

weak keys Encryption keys of short length or insufficient complexity.

Wi-Fi A brand marketing name that is used by the Wi-Fi Alliance to promote 802.11 WLAN technology.

Wi-Fi Alliance The Wi-Fi Alliance is a global, nonprofit industry trade association with more than 300 member companies. The Wi-Fi Alliance is devoted to promoting the growth of wireless LANs (WLANs). One of the Wi-Fi Alliance's primary tasks is to ensure the interoperability of WLAN products by providing certification testing. During the early days of the 802.11 standard, the Wi-Fi Alliance further defined the 802.11 standard and provided a set of guidelines to ensure compatibility among vendors. Products that pass the Wi-Fi certification process receive a "Wi-Fi CERTIFIED" certificate.

Wi-Fi Multimedia (WMM) The Wi-Fi Alliance maintains the Wi-Fi Multimedia (WMM) certification as a partial mirror of the 802.11e QoS amendment. WMM currently provides for traffic prioritization via four access categories.

Wi-Fi phishing attack After completing a wireless hijacking attack at a hotspot, a hacker may also use web server and captive portal software to perform a Wi-Fi phishing attack. After client stations have been hijacked to an evil twin access point, they are redirected to a login web page that looks exactly like a hotspot's login page. The hacker's fake login page will request a credit card number from the hijacked user. Phishing attacks are common on the Internet and are now appearing at Wi-Fi hotspots.

Wi-Fi Protected Access (WPA) Prior to the ratification of the 802.11i amendment, the Wi-Fi Alliance introduced Wi-Fi Protected Access (WPA) certification as a snapshot of the not-yet-released 802.11i amendment, supporting only the TKIP/RC4 dynamic encryption key management. 802.1X/EAP authentication was required in the enterprise, and passphrase authentication was required in a SOHO environment.

Wi-Fi Protected Access 2 (WPA2) WPA2 is based on the security mechanisms that were originally defined in the IEEE 802.11i amendment defining a robust security network

(RSN). Two versions of WPA2 exist: WPA2-Personal defines security for a small office, home office (SOHO) environment, and WPA2-Enterprise defines stronger security for enterprise corporate networks. Each certified product is required to support WPA2-Personal or WPA2-Enterprise.

Wi-Fi Protected Setup (WPS) Wi-Fi Protected Setup defines simplified and automatic WPA and WPA2 security configurations for home and small-business users.

Wired Equivalent Privacy (WEP) WEP is a Layer 2 encryption method that uses the RC4 streaming cipher. The original 802.11 standard defined 64-bit and 128-bit WEP. WEP encryption has been cracked and is not considered a strong encryption method.

wired leakage Traffic from a wired device or wired devices that is broadcast into the air by one or more APs.

wireless distribution system (WDS) Although the distribution system (DS) typically uses a wired Ethernet backbone, it is possible to use a wireless connection instead. A wireless distribution system (WDS) can connect access points together, using what is referred to as a wireless backhaul. WLAN bridges, repeaters, and mesh access points all use WDS connectivity.

wireless hijacking Wireless hijacking, also known as the evil twin attack, occurs when a hacker disrupts communications between client stations and a legitimate AP. Client stations lose their connection to the legitimate AP and reconnect to the hacker's access point. The hacker AP hijacks the client stations at Layer 1 and Layer 2, allowing the hacker to proceed with peer-to-peer attacks.

wireless intrusion detection system (WIDS) A WIDS is a client/server solution that is used to constantly monitor for 802.11 wireless attacks such as rogue APs, MAC spoofing, Layer 2 DoS, and so on. A WIDS usually consists of three components: a server, sensors, and monitoring software. Wireless intrusion detection uses policies and alarms to classify attacks properly and to alert administrators to potential attacks.

wireless intrusion prevention system (WIPS) A WIPS is a wireless intrusion detection system (WIDS) that is capable of mitigating attacks from rogue access points. WIPS use spoofed deauthentication frames, SMNP, and proprietary methods effectively to render a rogue access device useless and to protect the network backbone.

wireless LAN bridge A common nonstandard deployment of 802.11 technology. The purpose of bridging is to provide wireless connectivity between two or more wired networks. A bridge generally supports all the same features that a fat access point possesses; however, the purpose is to connect wired networks and not to provide wireless connectivity to client stations. Although bridge links are sometimes used indoors, generally they are used outdoors to connect the wired networks inside two buildings.

Wireless LAN security auditing Analysis of wireless security configurations and comparison to mandated policy or standards compliance used in vulnerability assessments to determine areas of or devices vulnerable to compromise.

wireless local area network (WLAN) The 802.11 standard is defined as a wireless local area network technology. Local area networks provide networking for a building or campus environment. The 802.11 wireless medium is a perfect fit for local area networking simply because of the range and speeds that are defined by the 802.11 standard and its amendments. The majority of 802.11 wireless network deployments are indeed local area networks (LANs) that provide access at businesses and homes.

wireless network management system (WNMS) A central management device originally used to configure and maintain as many as 5,000 autonomous access points. A WNMS can be either a hardware appliance or a software solution. The current WNMS servers are used to manage multiple WLAN controllers from a single vendor and may also be used to manage other vendors' WLAN infrastructure, including autonomous APs.

wireless rogue containment The process by which a WIPS is able to disconnect rogue APs and stations from the protected network. This process involves the WIPS sensors' cloning devices and transmitting a series of deauthentication and disassociation frames to the rogue and the legitimate devices that end the respective associations.

Wireless Zero Configuration (WZC) service The most widely used client utility is an integrated operating system client utility, more specifically known as the WZC service utility that is enabled by default in Windows XP.

WLAN controller WLAN controllers are used in a centralized WLAN architecture together with lightweight access points, also known as thin APs. All the intelligence resides in the centralized WLAN controller, and all the AP configuration settings, such as channel and power, are distributed to the lightweight APs from the WLAN controller and stored in the RAM of the lightweight AP. The encryption and decryption capabilities might reside in the centralized WLAN controller or may still be handled by the lightweight APs, depending on the vendor. The distribution system service (DSS) and integration service (IS) function within the WLAN controller. Also known as a wireless switch, WLAN controllers provide AP management, user management, RF spectrum planning and management, Layer 2 security, Layer 3 security, captive portal, VRRP redundancy, WIDS, and VLAN segmentation.

WLAN profile A set of configuration parameters that are configured on the WLAN controller. The profile parameters can include the WLAN logical name (SSID), WLAN security settings, VLAN assignment, and QoS parameters.

WLAN switch See WLAN controller.

X

xSec A proprietary Layer 2 encryption protocol developed by Juniper Networks and Aruba Networks.

Y

Yagi antenna A type of semidirectional antenna designed to direct a signal in a specific direction. Used for short- to medium-distance communications.

Index

Note to the Reader: Throughout this index **boldfaced** page numbers indicate primary discussions of a topic. *Italicized* page numbers indicate illustrations.

Numbers

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z

Wiley Publishing, Inc.
End-User License Agreement

READ THIS. You should carefully read these terms and conditions before opening the software packet(s) included with this book "Book". This is a license agreement "Agreement" between you and Wiley Publishing, Inc. "WPI". By opening the accompanying software packet(s), you acknowledge that you have read and accept the following terms and conditions. If you do not agree and do not want to be bound by such terms and conditions, promptly return the Book and the unopened software packet(s) to the place you obtained them for a full refund.

1. License Grant. WPI grants to you (either an individual or entity) a nonexclusive license to use one copy of the enclosed software program(s) (collectively, the "Software," solely for your own personal or business purposes on a single computer (whether a standard computer or a workstation component of a multi-user network). The Software is in use on a computer when it is loaded into temporary memory (RAM) or installed into permanent memory (hard disk, CD-ROM, or other storage device). WPI reserves all rights not expressly granted herein.

2. Ownership. WPI is the owner of all right, title, and interest, including copyright, in and to the compilation of the Software recorded on the physical packet included with this Book "Software Media". Copyright to the individual programs recorded on the Software Media is owned by the author or other authorized copyright owner of each program. Ownership of the Software and all proprietary rights relating thereto remain with WPI and its licensers.

3. Restrictions On Use and Transfer.

(**a**) You may only (i) make one copy of the Software for backup or archival purposes, or (ii) transfer the Software to a single hard disk, provided that you keep the original for backup or archival purposes. You may not (i) rent or lease the Software, (ii) copy or reproduce the Software through a LAN or other network system or through any computer subscriber system or bulletin-board system, or (iii) modify, adapt, or create derivative works based on the Software.

(b) You may not reverse engineer, decompile, or disassemble the Software. You may transfer the Software and user documentation on a permanent basis, provided that the transferee agrees to accept the terms and conditions of this Agreement and you retain no copies. If the Software is an update or has been updated, any transfer must include the most recent update and all prior versions.

4. Restrictions on Use of Individual Programs. You must follow the individual requirements and restrictions detailed for each individual program in the About the CD-ROM appendix of this Book or on the Software Media. These limitations are also contained in the individual license agreements recorded on the Software Media. These limitations may include a requirement that after using the program for a specified period of time, the user must pay a registration fee or discontinue use. By opening the Software packet(s), you will be agreeing to abide by the licenses and restrictions for these individual programs that are detailed in the About the CD-ROM appendix and/or on the Software Media. None of the material on this Software Media or listed in this Book may ever be redistributed, in original or modified form, for commercial purposes.

5. Limited Warranty.

(**a**) WPI warrants that the Software and Software Media are free from defects in materials and workmanship under normal use for a period of sixty (60) days from the date of purchase of this Book. If WPI receives notification within the warranty period of defects in materials or workmanship, WPI will replace the defective Software Media.

(**b**) WPI AND THE AUTHOR(S) OF THE BOOK DISCLAIM ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THE SOFTWARE, THE PROGRAMS, THE SOURCE CODE CONTAINED THEREIN, AND/OR THE TECHNIQUES DESCRIBED IN THIS BOOK. WPI DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE WILL BE ERROR FREE.

(**c**) This limited warranty gives you specific legal rights, and you may have other rights that vary from jurisdiction to jurisdiction.

6. Remedies.

(**a**) WPI's entire liability and your exclusive remedy for defects in materials and workmanship shall be limited to replacement of the Software Media, which may be returned to WPI with a copy of your receipt at the following address: Software Media Fulfillment Department, Attn.: *CWSP: Certified Wireless Security Professional Official Study Guide*, Wiley Publishing, Inc., 10475 Crosspoint Blvd., Indianapolis, IN 46256, or call 1-800-762-2974. Please allow four to six weeks for delivery. This Limited Warranty is void if failure of the Software Media has resulted from accident, abuse, or misapplication. Any replacement Software Media will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer.

(**b**) In no event shall WPI or the author be liable for any damages whatsoever (including without limitation damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising from the use of or inability to use the Book or the Software, even if WPI has been advised of the possibility of such damages.

(**c**) Because some jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation or exclusion may not apply to you.

7. U.S. Government Restricted Rights. Use, duplication, or disclosure of the Software for or on behalf of the United States of America, its agencies and/or instrumentalities "U.S. Government" is subject to restrictions as stated in paragraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, or subparagraphs (c) (1) and (2) of the Commercial Computer Software - Restricted Rights clause at FAR 52.227-19, and in similar clauses in the NASA FAR supplement, as applicable.

8. General. This Agreement constitutes the entire understanding of the parties and revokes and supersedes all prior agreements, oral or written, between them and may not be modified or amended except in a writing signed by both parties hereto that specifically refers to this Agreement. This Agreement shall take precedence over any other documents that may be in conflict herewith. If any one or more provisions contained in this Agreement are held by any court or tribunal to be invalid, illegal, or otherwise unenforceable, each and every other provision shall remain in full force and effect.

The Best CWSP Book/CD Package on the Market!

Get ready for your Certified Wireless Security Professional (CWSP) certification with the most comprehensive and challenging sample tests anywhere!

The Sybex Test Engine features:

- All the review questions, as covered in each chapter of the book.
- Challenging questions representative of those you'll find on the real exam.
- Two full-length bonus exams available only on the CD.
- An Assessment Test to narrow your focus to certain objective groups.

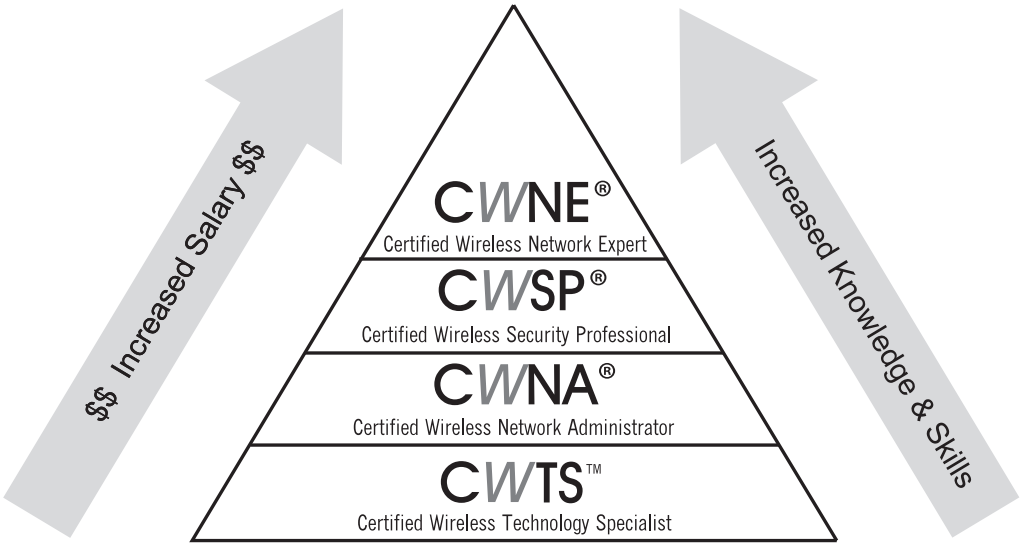
Use the Electronic Flashcards for PCs or Palm devices to jog your memory and prep last-minute for the exam!

- Reinforce your understanding of key concepts with these hardcore flashcard-style questions.
- Download the Flashcards to your Palm device and go on the road. Now you can study for the CWSP (PW0-204) exam anytime, anywhere.

cwnp®

Certified *Wireless* Network Professional

Pyramid of Wireless Certification Success



CWTS™

Audience:
- Enterprise Wi-Fi Sales
- First Tier Tech Support

Core Curriculum:
- Wi-Fi Fundamentals
- Wi-Fi Terminology

CWNA®

Audience:
- Network Administrators
- Network Installers
- Site Surveyors

Core Curriculum:
- RF Foundations
- Wi-Fi technologies

CWSP®

Audience:
- Network Engineers
- IT Security Experts

Core Curriculum:
- Wi-Fi Intrusion Tactics
- Wi-Fi Security Solutions

CWNE®

Audience:
- Network Engineers
- Troubleshooting Experts

Core Curriculum:
- Wi-Fi Analysis
- Optimization
- Troubleshooting

Learn more at **www.cwnp.com/certifications**

CWSP: Certified Wireless Security Professional Official Study Guide

Exam PW0-204

OBJECTIVE	CHAPTER
WIRELESS NETWORK ATTACKS AND THREAT ASSESSMENT	
1.1 Demonstrate how to recognize, perform, and prevent the following types of attacks, and discuss their impact on the organization: Information theft and placement; Physical device damage or theft; PHY and MAC Denial of Service (DoS); Client hijacking, phishing, and other peer-to-peer attacks; Protocol analysis (eavesdropping); MAC layer protocol attacks; Social engineering; Man-in-the-middle; Authentication and encryption cracking; Infrastructure hardware theft; Management interface exploits; Rogue infrastructure hardware placement	8
1.2 Understand the probability of, demonstrate the methodology of, and execute the preventative measures against the following attacks on wireless infrastructure devices: Weak/default passwords on wireless infrastructure equipment; Misconfiguration of wireless infrastructure devices by administrative staff	8
1.3 Explain and demonstrate the use of protocol analyzers to capture the following sensitive information: Usernames / Passwords / SNMP Community Strings / X.509 certificates; Encryption keys / Passphrases; MAC addresses / IP addresses; Unencrypted data	8
1.4 Explain and/or demonstrate security protocol circumvention against the following types of authentication and/or encryption: WEP (Any key length); Shared Key Authentication; WPA-Personal / WPA2-Personal; LEAP; PPTP	2, 6, 8
1.5 Perform a risk assessment for a WLAN, including: Asset risk; Legal implications; Regulatory compliance	13
1.6 Explain and demonstrate the following security vulnerabilities associated with public access or other unsecured wireless networks: Spamming through the WLAN; Malware (viruses / spyware / adware / remote control); Direct Internet attacks through the WLAN; Placement of illegal content; Information theft; Peer-to-peer attack	8
MONITORING, MANAGEMENT, AND TRACKING	
2.1 Understand how to use laptop-based protocol and spectrum analyzers to effectively troubleshoot and secure wireless networks.	9
2.2 Describe the use, configuration, and components of an 802.11 Wireless Intrusion Prevention Systems (WIPS): WIPS server software or appliance; Dedicated sensor hardware/software; Access points as part-time sensors; Access points with dedicated sensor radios; Integration between WLAN controller and WIPS server; Deployment strategies: overlay and integrated; Performance and security analysis; Protocol and spectrum analysis	10

Sybex®
An Imprint of
WILEY

OBJECTIVE	CHAPTER
2.3 Explain 802.11 WIPS baselining and demonstrate the following tasks: Measuring performance parameters under normal network conditions; Understand common reasons for false positives and false negatives; Configuring the WIPS to recognize all APs and client stations in the area as authorized, external, or rogue	10
2.4 Describe and understand common security features of 802.11 WIPS: Device detection, classification, and behavior analysis; Rogue Triangulation, RF Fingerprinting, and Time Difference of Arrival (TDoA) techniques for real-time device and interference tracking; Event alerting, notification, and categorization; Policy enforcement and violation reporting; Wired/Wireless intrusion mitigation; Protocol analysis with filtering; Rogue containment and remediation; Data forensics	10
2.5 Describe and demonstrate the different types of WLAN management systems and their features: Network discovery; Configuration and firmware management; Audit management and policy enforcement; Network and user monitoring; Rogue detection; Event alarms and notification	12
2.6 Describe and implement compliance monitoring, enforcement, and reporting Industry requirements (PCI); Government regulations	13
SECURITY DESIGN AND ARCHITECTURE	
3.1 Describe wireless network security models	1, 11
Hotspot / Public Access / Guest Access; Small Office / Home Office; Small and Medium Enterprise; Large Enterprise; Remote Access: Mobile User and Branch Office	1, 11
3.2 Recognize and understand the following security concepts: 802.11 Authentication and Key Management (AKM) components and processes; Robust Security Networks (RSN) and RSN Associations (RSNA); Pre-RSNA Security; Transition Security Networks (TSN); RSN Information Elements; How WPA and WPA2 certifications relate to 802.11 standard terminology and technology; Functional parts of TKIP and its differences from WEP; The role of TKIP/RC4 in WPA implementations; The role of CCMP/AES in WPA2 implementations; TKIP compatibility between WPA and WPA2 implementations; Appropriate use and configuration of WPA-Personal and WPA-Enterprise; Appropriate use and configuration of WPA2-Personal and WPA2-Enterprise; Appropriate use and configuration of Per-user Pre-shared Key (PPSK); Feasibility of WPA-Personal and WPA2-Personal exploitation	3, 4, 6
3.3 Identify the purpose and characteristics of 802.1X and EAP: Supplicant, authenticator, and authentication server roles; Functions of the authentication framework and controlled/uncontrolled ports; How EAP is used with 802.1X port-based access control for authentication; Strong EAP types used with 802.11 WLANs: PEAPv0/EAP-TLS, PEAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-TLS, EAP-TTLS/MS-CHAPv2, EAP-FAST	4
3.4 Recognize and understand the common uses of VPNs in wireless networks, including: Remote AP; VPN client software; WLAN Controllers	11
3.5 Describe, demonstrate, and configure centrally managed client-side security applications: VPN policies; Personal firewall software; Wireless client utility software	11

OBJECTIVE	CHAPTER
3.6 Describe and demonstrate the use of secure infrastructure management protocols: HTTPS; SNMPv3; SFTP (FTP/SSL or FTP/SSH); SCP; SSH2	12
3.7 Explain the role, importance, and limiting factors of VLANs and network segmentation in an 802.11 WLAN infrastructure.	12
3.8 Describe, configure, and deploy a AAA server and explain the following concepts related to AAA servers: RADIUS server; Integrated RADIUS services within WLAN infrastructure devices; RADIUS deployment strategies; RADIUS proxy services; LDAP Directory Services integration deployment strategies; EAP support for 802.11 networks; Applying user and AAA server credential types (Username/Password, Certificate, Protected Access Credentials (PACs), & Biometrics); The role of AAA services in wireless client VLAN assignments; Benefits of mutual authentication between supplicant and authentication server	4, 12
3.9 Explain frame exchange processes and the purpose of each encryption key within 802.11 Authentication and Key Management, including: Master Session Key (MSK) generation; PMK generation and distribution; GMK generation; PTK / GTK generation & distribution; 4-Way Handshake; Group Handshake; Passphrase-to-PSK mapping	5
3.10 Describe and configure major security features in WLAN infrastructure devices: Role Based Access Control (RBAC) (per-user or per-group); Location Based Access Control (LBAC); fast BSS transition in an RSN; 802.1Q VLANs and trunking on Ethernet switches and WLAN infrastructure devices; Hot standby/failover and clustering support; WPA/WPA2 Personal and Enterprise; Secure management interfaces (HTTPS, SNMPv3, SSH2); Intrusion detection and prevention; Remote access (branch office and mobile users)	12
3.11 Explain the benefits of and configure management frame protection (802.11w) in access points and WLAN controllers.	10
3.12 Explain the purpose, methodology, features, and configuration of guest access networks, including: RADIUS Dynamic Change of Authorization (CoA) messages; Segmentation; Captive Portal (Web) Authentication: User-based authentication methods, Secure authentication protocols	12
SECURITY POLICY	
4.1 Explain the purpose and goals of the following WLAN security policies: Password policy; End-user and administrator training on security solution use and social engineering mitigation; Internal marketing campaigns to heighten security awareness; Periodic network security audits; Acceptable network use & abuse policy; Use of Role Based Access Control (RBAC) and traffic filtering; Obtaining the latest security feature sets through firmware and software upgrades; Consistent implementation procedure; Centralized implementation and management guidelines and procedures; Inclusion in asset and change management programs	13

OBJECTIVE	CHAPTER
4.2 Describe appropriate installation locations for and remote connectivity to WLAN devices in order to avoid physical theft, tampering, and data theft. Considering the following: Physical security implications of infrastructure device placement; Secure remote connections to WLAN infrastructure devices	11, 13
4.3 Explain the importance and implementation of client-side security applications: VPN client software and policies; Personal firewall software; 802.1X/EAP supplicant software	11, 13
4.4 Explain the importance of ongoing WLAN monitoring and documentation: Explain the necessary hardware and software for ongoing WLAN security monitoring; Describe and implement WLAN security audits and compliance reports	9, 13
4.5 Summarize the security policy criteria related to wireless public access network use. User risks related to unsecured access; Provider liability, disclaimers, and acceptable use notifications	13
4.6 Explain the importance and implementation of a scalable and secure WLAN solution that includes the following security parameters: Intrusion detection and prevention; Role Based Access Control (RBAC) and traffic filtering; Strong authentication and encryption; fast BSS transition	12
FAST BSS TRANSITION (FAST/SECURE ROAMING)	
5.1 Describe and implement 802.11 Authentication and Key Management (AKM) including the following: Preauthentication; PMK Caching	7
5.2 Describe and implement Opportunistic Key Caching (OKC) and explain its enhancements beyond 802.11 AKM.	7
5.3 Describe and implement 802.11r Authentication and Key Management (AKM) and compare and contrast 802.11r enhancements with 802.11 AKM and Opportunistic Key Caching. Fast BSS Transition (FT) Key Architecture; Key Nomenclature; Initial Mobility Domain Association; Over-the-Air Transition; Over-the-DS Transition	7
5.4 Describe applications of fast BSS transition.	7
5.5 Describe and implement non-traditional roaming mechanisms. Single Channel Architecture (SCA) WLAN controllers with controller-based APs; Infrastructure-controlled handoff	7
5.6 Describe how 802.11k Radio Resource Measurement factors into fast BSS transition: Neighbor Reports; Contrasting SCA and MCA Architectures	7, 10
5.7 Describe the importance, application, and functionality of Wi-Fi Voice-Personal product certification.	1

Exam objectives are subject to change at any time without prior notice and at CWNP's sole discretion. Please visit CWNP's website (`www.cwnp.com`) for the most current listing of exam objectives.

Sybex®
An Imprint of
WILEY

The Official Study Guide for Exam PW0-204 from CWNP®

Prepare for the Certified Wireless Security Professional exam (PW0-204) with this new *Official Study Guide* from CWNP. This comprehensive resource covers everything you need for the exam, including wireless security basics, risks, and policies; legacy 802.11 security and robust network security (RSN); encryption ciphers and methods; enterprise 802.11 layer 2 authentication methods; fast secure roaming, wireless intrusion prevention; and many other essential WLAN security topics and concepts. Inside you'll find:

- Full coverage of all exam objectives in a systematic approach, so you can be confident you're getting the instruction you need for the exam
- Practical hands-on exercises to reinforce critical skills
- Real-world scenarios that put what you've learned in the context of actual job roles
- Challenging review questions in each chapter to prepare you for exam day
- Exam Essentials, a key feature in each chapter that identifies critical areas you must become proficient in before taking the exam
- White papers, demo software, practice exams, and over 150 flashcards on the CD to further facilitate your learning
- A handy tear card that maps every official exam objective to the corresponding chapter in the book, so you can track your exam prep objective by objective

Look inside for complete coverage of all exam objectives.

ABOUT THE AUTHORS

David D. Coleman, CWNE #4, CWNA, CWSP, CWNT, is a WLAN security consultant and technical trainer with over twenty years of IT experience. The company he founded, AirSpy Networks (www.airspy.com), specializes in corporate WLAN training. **David A. Westcott,** CWNE #7, CWNA, CWSP, CWNT, is an independent consultant and WLAN technical trainer with over twenty years of experience. He has been a certified trainer for over fifteen years. **Bryan E. Harkins,** CWNE #44, CWSP, CWNA, CWNT, is the Training and Development Manager for Motorola AirDefense Solutions, a market leader in wireless intrusion prevention systems. **Shawn M. Jackman,** CWNE #54, CWNA, CWSP, CWAP is a principal WLAN engineer with Kaiser Permanente. He has over fifteen years' experience working with wireless manufacturers and integrators.

ISBN 978-0-470-43891-6

Sybex®
An Imprint of
WILEY

$69.99 US
$83.99 CN

~StormRG~

FEATURED ON THE CD

SYBEX TEST ENGINE:
Test your knowledge with advanced testing software. Includes all chapter review questions and practice exams.

ELECTRONIC FLASHCARDS:
Reinforce your understanding with electronic flashcards.

The CD also includes white papers and demo software.

Study anywhere, any time, and approach the exam with confidence.

ABOUT THE CWNP PROGRAM
CWNP is the industry standard for vendor-neutral, enterprise WLAN certifications. The focus is to educate IT professionals in the technology behind all enterprise WLAN products and to enable these professionals to manage wireless LAN enterprise infrastructures, regardless of the vendor solution utilized. CWNP is a privately held corporation based in Atlanta, Georgia. For more information, visit www.cwnp.com.

www.sybex.com

CATEGORY:
COMPUTERS/Certification Guides