CENGAGE Learning

EC-Council | Press

ETHICAL HACKING AND COUNTERMEASURES

SECURE NETWORK OPERATING SYSTEMS AND INFRASTRUCTURES

Second Edition

Book 4 of 4

C|EH™

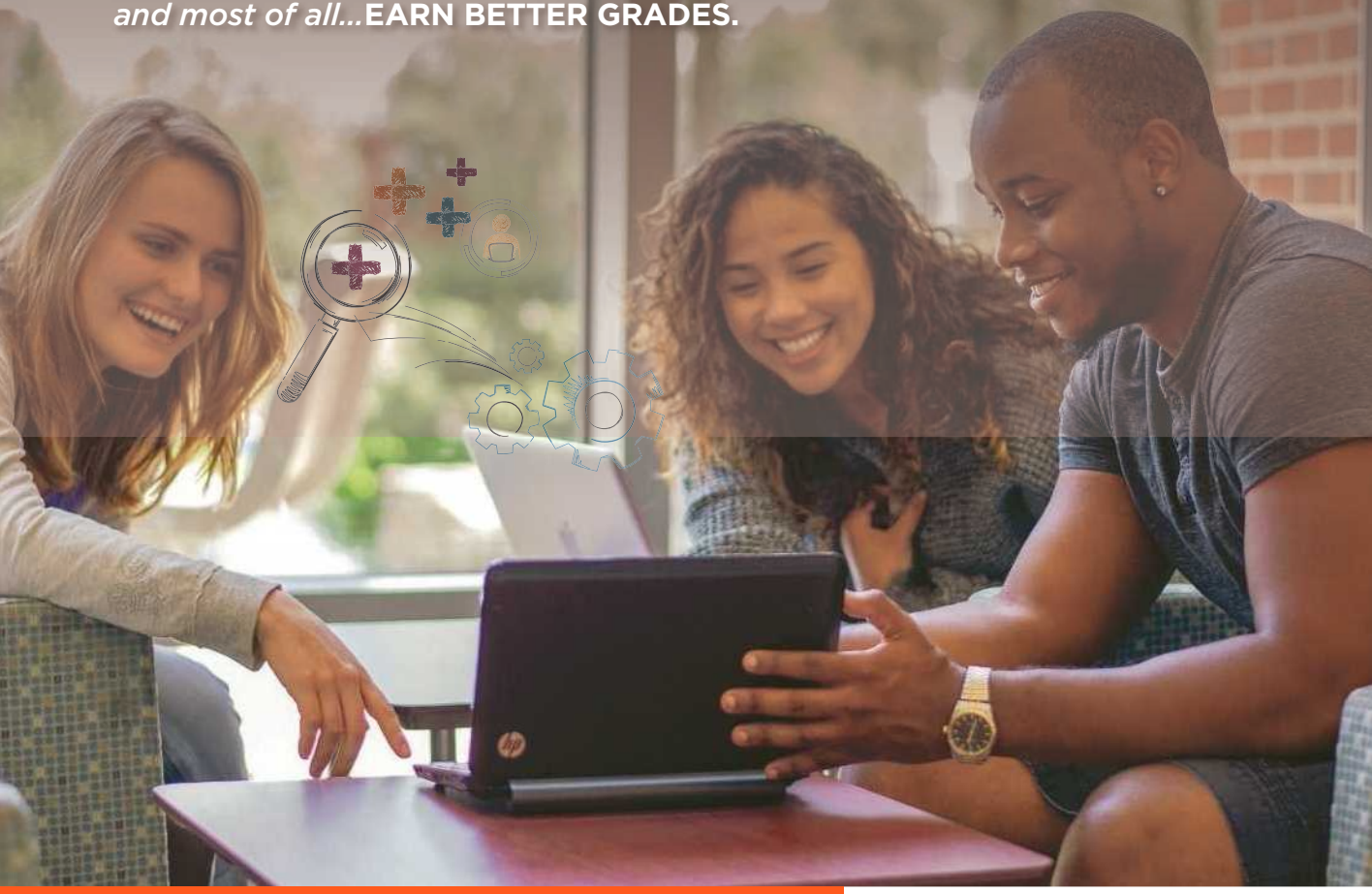
Certified Ethical Hacker

Want to turn C's into A's? Obviously, right?

But the right way to go about it isn't always so obvious. Go digital to get the grades. MindTap's customizable study tools and eTextbook give you everything you need all in one place.

Engage with your course content, enjoy the flexibility of studying anytime and anywhere, stay connected to assignment due dates and instructor notifications with the MindTap Mobile app...

*and most of all...***EARN BETTER GRADES.**



TO GET STARTED VISIT
WWW.CENGAGE.COM/STUDENTS/MINDTAP

CENGAGE Learning® | MindTap®

Secure Network Operating Systems and Infrastructures

EC-Council | Press

Book 4 of 4

C|EH™ Certified Ethical Hacker Certification

CENGAGE Learning®

Australia • Brazil • Mexico • Singapore • United Kingdom • United States

CENGAGE Learning®

Ethical Hacking and Countermeasures: Secure Network Operating Systems and Infrastructures (CEH)

EC-Council Press

SVP, GM Skills & Global Product Management: Dawn Gerrain

Product Director: Kathleen McMahon

Product Team Manager: Kristin McNary

Associate Product Manager: Amy Savino

Senior Director, Development: Marah Bellegarde

Product Development Manager: Leigh Hefferon

Managing Content Developer: Emma Newsom

Senior Content Developer: Natalie Pashoukos

Product Assistant: Abigail Pufpaff

Vice President, Marketing Services: Jennifer Ann Baker

Marketing Coordinator: Cassie Cloutier

Senior Production Director: Wendy Troeger

Production Director: Patty Stephan

Senior Content Project Manager: Brooke Greenhouse

Managing Art Director: Jack Pendleton

Software Development Manager: Pavan Ethakota

Cover Image(s): Istockphoto.com/ gong hangxu and Istockphoto.com/ Turnervisual

EC-Council:

President | EC-Council: Jay Bavisi

Vice President, North America | EC-Council: Steven Graham

Library of Congress Control Number: 2016930623

ISBN: 978-1-305-88346-8

Cengage Learning
20 Channel Center Street
Boston, MA 02210
USA

Cengage Learning is a leading provider of customized learning solutions with employees residing in nearly 40 different countries and sales in more than 125 countries around the world. Find your local representative at **www.cengage.com**.

Cengage Learning products are represented in Canada by Nelson Education, Ltd.

To learn more about Cengage Learning, visit **www.cengage.com**.

Purchase any of our products at your local college store or at our preferred online store **www.cengagebrain.com**.

Printed in the United States of America
Print Number: 01 Print Year: 2016

Brief Table of Contents

Table of Contents

Preface

Hacking and electronic crimes sophistication is consistently growing at an exponential rate. Recent reports have indicated that cybercrime already surpasses the illegal drug trade! Unethical hackers, better known as *black hat hackers*, are preying on information systems of government, corporate, public, and private networks and are constantly testing the security mechanisms of these organizations to the limit with the sole aim of exploiting them and profiting from the exercise. High-profile crimes have proven that the traditional approach to computer security is simply not sufficient, even with the strongest perimeter; properly configured defense mechanisms such as firewalls, intrusion detection, and prevention systems; strong end-to-end encryption standards; and antivirus software. Hackers have proven their dedication and ability to systematically penetrate networks all over the world. In some cases, black hat hackers may be able to execute attacks so flawlessly that they can compromise a system, steal everything of value, and completely erase their tracks in less than 20 minutes!

The EC-Council | Press is dedicated to stopping hackers in their tracks.

About EC-Council

The International Council of Electronic Commerce Consultants, better known as EC-Council, was founded in late 2001 to address the need for well-educated and certified information security and e-business practitioners. EC-Council is a global, member-based organization comprised of industry and subject matter experts all working together to set the standards and raise the bar in information security certification and education.

EC-Council first developed the *Certified Ethical Hacker* (C|EH) program. The goal of this program is to teach the methodologies, tools, and techniques used by hackers. Leveraging the collective knowledge from hundreds of subject matter experts, the C|EH program has rapidly gained popularity around the globe and is now delivered in more than 70 countries by more than 600 authorized training centers. More than 100,000 information security practitioners have been trained.

C|EH is the benchmark for many government entities and major corporations around the world. Shortly after C|EH was launched, EC-Council developed the *Certified Security Analyst* (E|CSA). The goal of the E|CSA program is to teach groundbreaking analysis methods that must be applied while conducting advanced penetration testing. The E|CSA program leads to the *Licensed Penetration Tester* (L|PT) status. The *Computer Hacking Forensic Investigator* (C|HFI) was formed with the same design methodologies and has become a global standard in certification for computer forensics. EC-Council, through its impervious network of professionals and huge industry following, has developed various other programs in information security and e-business. EC-Council certifications are viewed as the essential certifications needed when standard configuration and security policy courses fall short. Being provided with a true hands-on, tactical approach to security, individuals armed with the knowledge disseminated by EC-Council programs are securing networks around the world and beating the hackers at their own game.

About the EC-Council | Press

The EC-Council | Press was formed in late 2008 as a result of a cutting-edge partnership between global information security certification leader EC-Council and leading educational content, technology, and services company Cengage Learning. This partnership marks a revolution in academic textbooks and courses of study in information security, computer forensics, disaster recovery, and end-user security. By identifying the essential topics and content of EC-Council professional certification programs, and repurposing this world-class content to fit academic programs, the EC-Council | Press was formed. The academic community is now able to incorporate this powerful cutting-edge content into new and existing information security programs. By closing the gap between academic study and professional certification, students and instructors are able to leverage the power of rigorous academic focus and high-demand industry certification. The EC-Council | Press is set to revolutionize global information security programs and ultimately create a new breed of practitioners capable of combating the growing epidemic of cybercrime and the rising threat of cyber-war.

Ethical Hacking and Countermeasures Series

The EC-Council | Press *Ethical Hacking and Countermeasures* series is intended for those studying to become security officers, auditors, security professionals, site administrators, and anyone who is concerned about or responsible for the integrity of the network infrastructure. The series includes a broad base of topics in offensive network security, ethical hacking, as well as network defense and countermeasures. The content of this series is designed to immerse learners into an interactive environment where they will be shown how to scan, test, hack, and secure information systems. A wide variety of tools, viruses, and malware is presented in these books, providing a complete understanding of the tactics and tools used by hackers. By gaining a thorough understanding of how hackers operate, ethical hackers are able to set up strong countermeasures and defensive systems to protect their organization's critical infrastructure and information. The series, when used in its entirety, helps prepare readers to take and pass the C|EH certification exam from EC-Council.

Books in Series

- *Ethical Hacking and Countermeasures: Attack Phases*/9781305883437
- *Ethical Hacking and Countermeasures: Threats and Defense Mechanisms*/9781305883444
- *Ethical Hacking and Countermeasures: Web Applications and Data Servers*/9781305883451
- *Ethical Hacking and Countermeasures: Secure Network Operating Systems and Infrastructures*/9781305883468

Secure Network Operating Systems and Infrastructures

Secure Network Operating Systems and Infrastructures discusses hacking wireless networks; physical security; how to evade IDS and Firewalls; how to detect honey pots; and an introduction to cryptography. In addition, it covers techniques used in hacking Linux, Macintosh, routers, cable modems, firewalls, mobile devices, Bluetooth devices, RFID and USB devices and how to determine security policies for these devices.

Chapter Contents

Chapter 1, *Hacking Wireless Networks*, discusses wireless networking and the different wireless standards and provides information on SSID, wireless access points, how to crack WEP and much more. Chapter 2, *Physical Security*, focuses on the need to be aware of physical security; challenges in ensuring physical security; and ways to physically secure networks. Chapter 3, *Evading IDS, Firewalls and Detecting Honeypots*, discusses various security features that administrators deploy to protect their networks. Chapter 4, *Hacking Routers and Cable Modems*, discusses how particularly vulnerable these devices are to hackers and how these vulnerabilities are essential factors in determining security policies for both businesses and households. Chapter 5, *Linux Hacking*, looks into various aspects of security related to Linux including rootkits and intrusion detection systems. Chapter 6, *Mac OS X Hacking*, introduces some of the features of Mac OS X and then discusses vulnerabilities that affect the operating system. Chapter 7, *Hacking Mobile Phones*, PDAs and Handheld Devices, includes a discussion on the different types of handheld devices investigators have to be aware of and the vulnerabilities present in the different devices. Chapter 8, *Hacking Portable Devices*, focuses on three types of mobile devices: USB, Bluetooth and RFID. Section 1 discusses USB devices, how they are attacked, and some countermeasures to protect them. Section 2 focuses on Bluetooth and the security issues involved with it. It covers the different types of attacks hackers make against Bluetooth-enabled devices, as well as tools that make Bluetooth more secure. Section 3 focuses on RFID devices, associated security and privacy threats, and specific vulnerabilities with RFID-enabled credit cards. Additionally, the countermeasures used to avoid RFID attacks, RFID malware, and RFID exploits are discussed and it concludes with a discussion of RFID security controls. Chapter 9, *Cryptography*, explains what cryptography is and discusses the various cryptography attacks and introduces various cracking tools.

Chapter Features

Many features are included in each chapter, and all are designed to enhance the reader's learning experience. Features include:

- *Objectives* begin each chapter and focus the learner on the most important concepts in the chapter.
- *Key Terms* are designed to familiarize the learner with terms that will be used within the chapter.
- *What If?*, found in each chapter, presents short scenarios followed by questions that challenge the learner to arrive at an answer or solution to the problem presented.
- *Chapter Summary*, at the end of each chapter, serves as a review of the key concepts covered in the chapter.
- *Review Questions* allow learners to test their comprehension of the chapter content.
- *Hands-On Projects* encourage learners to apply the knowledge they have gained after finishing the chapter. Files for the Hands-On Projects can be found in the MindTap or on the Student Resource Center. Visit *www.cengagebrain.com* for a link to the Student Resource Center.

MindTap

MindTap for Ethical Hacking and Countermeasures Series is an online learning solution designed to help students master the skills they need in today's workforce. Research shows employers need critical thinkers, troubleshooters, and creative problem-solvers to stay relevant in our fast-paced, technology-driven world. MindTap helps users achieve this with assignments and activities that provide hands-on practice, real-life relevance, and mastery of difficult concepts. Students are guided through assignments that progress from basic knowledge and understanding to more challenging problems.

All MindTap activities and assignments are tied to learning objectives. The hands-on exercises provide real-life application and practice. Readings and "Whiteboard Shorts" support the lecture, while "In the News" assignments encourage students to stay current. Pre- and post-course assessments allow you to measure how much students have learned using analytics and reporting that makes it easy to see where the class stands in terms of progress, engagement, and completion rates. Use the content and learning path as-is, or pick and choose how the material will wrap around your own. You control what the students see and when they see it. Learn more at *www.cengage.com/mindtap/*.

Student Resource Center

The Student Resource Center contains all the files you need to complete the Hands-On Projects found at the end of the chapters. Visit *www.cengagebrain.com* to access the Student Resource Center.

Additional Instructor Resources

Free to all instructors who adopt *Secure Network Operating Systems and Infrastructures* for their courses is a complete package of instructor resources. These resources are available from the Cengage Learning Web site, *www.cengagebrain.com*, by going to the product page for this book in the online catalog and choosing "Instructor Downloads."

Resources include:

- *Instructor's Manual*: This manual includes course objectives and additional information to help your instruction.
- *Cengage Learning Testing Powered by Cognero:* A flexible, online system that allows you to import, edit, and manipulate content from the text's test bank or elsewhere, including your own favorite test questions; create multiple test versions in an instant; and deliver tests from your LMS, your classroom, or wherever you want.

- *PowerPoint Presentations*: A set of Microsoft PowerPoint slides is included for each chapter. These slides are meant to be used as a teaching aid for classroom presentations, to be made available to students for chapter review, or to be printed for classroom distribution. Instructors are also at liberty to add their own slides.
- *Labs*: These are additional hands-on activities to provide more practice for your students.
- *Assessment Activities*: These are additional assessment opportunities including discussion questions, writing assignments, Internet research activities, and homework assignments along with a final cumulative project.
- *Final Exam*: This exam provides a comprehensive assessment of *Secure Network Operating Systems and Infrastructures* content.

Cengage Learning Tech Connection: Information Security Community

This site was created for learners and instructors to find out about the latest in information security news and technology.

Visit *http://community.cengage.com/InfoSec2/* to:

- Learn what's new in information security through live news feeds, videos, and podcasts;
- Connect with your peers and security experts through blogs and forums;
- Browse our online catalog.

How to Become C|EH Certified

The C|EH certification focuses on hacking techniques and technology from an offensive perspective. The certification is primarily targeted at security professionals who want to acquire a well-rounded body of knowledge to have better opportunities in this field. Acquiring a C|EH certification means the candidate has a minimum baseline knowledge of security threats, risks, and countermeasures. An organization can rest assured that they have a candidate who is more than a systems administrator, a security auditor, a hacking tool analyst, or a vulnerability tester. The candidate is assured of having both business and technical knowledge.

C|EH certification exams are available through Pearson Vue testing centers. To finalize your certification after your training by taking the certification exam through a Pearson Vue testing center, you must:

1. Apply for and purchase an exam voucher by visiting the EC-Council Academic Center of Excellence at *http://ace.eccouncil.org*, if one was not purchased with your book.
2. If you have a Pearson Vue voucher, please contact a local Pearson Vue testing center accordingly to schedule your exam, or visit *www.pearsonvue.com/eccouncil/*.
3. Take and pass the C|EH certification examination with a score of 70 percent or better.

Additional EC-Council | Press Products

Computer Forensics Series

The EC-Council | Press *Computer Forensics* series, preparing learners for C|HFI certification, is intended for those studying to become police investigators and other law enforcement personnel;

defense and military personnel; e-business security professionals; systems administrators; legal professionals; banking, insurance and other professionals; government agencies; and IT managers. The content of this program is designed to expose the learner to the process of detecting attacks and collecting evidence in a forensically sound manner with the intent to report crime and prevent future attacks. Advanced techniques in computer investigation and analysis with interest in generating potential legal evidence are included. In full, this series prepares the learner to identify evidence in computer-related crime and abuse cases as well as track the intrusive hacker's path through client system. The series when used in its entirety helps prepare readers to take and pass the C|HFI Certified Forensic Investigator certification exam from EC-Council.

Books in Series

- *Computer Forensics: Investigation Procedures and Response*/9781305883475
- *Computer Forensics: Investigating File and Operating Systems, Wireless Networks and Storages*/*9781305883482*
- *Computer Forensics: Investigating Data and Image Files*/9781305883499
- *Computer Forensics: Investigating Network Intrusions and Cybercrime*/9781305883505

EC-Council's Supporting Events

TakeDownCon

TakeDownCon is a highly technical forum that focuses on the latest vulnerabilities, the most potent exploits, and current security threats. The best and the brightest come to share their knowledge, giving delegates the opportunity to learn about the industry's most important issue. With two days and two dynamic tracks, delegates will spend Day 1 on the Attack, learning how even the most protected systems can be breached. Day 2 is dedicated to Defense, and delegates will learn if their defense mechanisms are on par to thwart nefarious and persistent attacks.

For more information, visit the Web site: *www.takedowncon.com*.

Hacker Halted

Hacker Halted builds on the educational foundation of EC-Council's courses in ethical hacking, computer forensics, penetration testing, and many others. Hacker Halted brings the industry's leading researchers, practitioners, ethical hackers, and other top IT security professionals together to discuss current issues facing our industry. Hacker Halted has been delivered globally in countries such as Egypt, Mexico, Malaysia, Hong Kong, Iceland, and in the United States, in cities such as Myrtle Beach, Miami, and most recently in Atlanta.

For more information, visit the Web site: *www.hackerhalted.com*.

Global CyberLympics

Global CyberLympics is an online ethical hacking computer network defense competition. The goal is to raise awareness of increased education and ethics in information security through a series of cyber competitions that encompass forensics, ethical hacking, and defense. Teams are made up of four to six players, and each round serves as an elimination round until the top teams remain. The top teams from each region get invited to play live in-person at the world finals.

For more information, visit the Web site: *www.cyberlympics.org*.

Acknowledgments

Michael H. Goldner is the Dean of EC-Council University. He has been involved in the information security arena for over 20 years and has dedicated the last 15 years to developing hands-on academic curricula to help train the world's future cyber leaders. He received his Juris Doctorate from Stetson University College of Law and his undergraduate degree from Miami University. He is an active member of the American Bar Association and a member of the Cyber Law subcommittee. He is a member of IEEE, ISSA ISC2, ISACA and PMI, and holds a number of industrially recognized certifications, including C|CISO, CISSP, CISM, CEI, CEH, CHFI, MCT, MCSE/Security, MCSA, Security +, Network +, and A+.

He has worked closely with EC-Council and Cengage Learning in the creation of this EC-Council Press series on information security and computer forensics, and is passionate about creating a viable international leadership corps to guide our electronically connected society into a safe and prosperous future.

chapter 1

Hacking Wireless Networks

After completing this chapter, you should be able to:

- Understand wireless networking
- Understand the different types of wireless networks
- Understand the different wireless standards
- Understand SSID
- Understand wireless access points
- Understand Wired Equivalent Privacy
- Understand Wi-Fi Protected Access (WPA)
- Hack wireless networks
- Crack WEP
- Utilize tools for scanning and sniffing
- Secure wireless networks

What If?

George just moved into his new apartment and wanted to install a wireless router. He bought one at his local tech store, brought it home, removed it from the box, and plugged it in. Everything worked fine and George was quite happy until the federal police came to his door and informed him that someone with his IP address was hosting a bomb-making Web site that was getting great interest from foreign terrorist groups.

After some quite long interviews/interrogations and losing his computer, laptop, and tablet for several months, George was finally cleared of any wrongdoing, but nevertheless remains on the FBI watch list.

- What precautions should George have taken to prevent this breach and misuse of his network?
- What are the possible side effects of his naiveté in using a home wireless network?

Introduction to Hacking Wireless Networks

More and more networks are moving away from hard-wiring systems together and are instead communicating wirelessly. This leads to a host of new security concerns that will be addressed in this chapter.

Wireless Networking

A wireless LAN (WLAN) is a local area network that exchanges data without the use of cables. A wireless LAN offers data connectivity in an existing building where wiring may not be practical due to construction design, location, or expense involved. WLANs are gaining popularity due to their ease of use and potential for mobility.

WLANs do raise the issue of security due to radio waves being easier to intercept than physical wires. However, the user authentication and data encryption system known as Wired Equivalent Privacy, or WEP, helps increase the security of the network. All users accessing the wireless network share the bandwidth available via access points.

The major advantage of wireless networks is mobility, although users should not expect flawless reception between access points.

Wired Network Versus Wireless Network

Both types of communication have their pros and cons. Wireless networks offer fully mobile, untethered access to the network, allowing users to more easily connect using notebooks or other mobile devices. However, this mobility comes with the following tradeoffs:

- Higher cost
- Lower reliability
- Slower performance
- Lessened security

Effects of Wireless Attacks on Businesses

As more and more firms adopt wireless networks, security becomes more important. Businesses are at high risk from wireless hackers, sometimes called **whackers**. Whackers do not need physical entry into the business network to hack, but can easily compromise a network with the help of freely available tools. Warchalking, wardriving, and warflying are some of the ways in which a whacker can assess the vulnerability of a wireless network. Many organizations are deploying wireless networks to allow employees to roam the corporate campus without leaving the network. Some airports offer wireless connectivity so travelers can continue working while waiting for flight departures, and many hotels also provide these facilities to their customers. Unfortunately, this ease of use also comes with increased risk, as an attacker who is sitting miles away can sniff the network without being noticed.

Large companies generally make the most use of wireless networks and devices. These networks are generally expensive and troublesome to deploy and manage. They require networking expertise. However, from the whacker's point of view, wireless networks and access points (sometimes called **APEs**, WAPs, or APs) are some of the easiest, most inexpensive targets while being some of the hardest to defend.

Types of Wireless Networks

There are four basic types of wireless networks.

Peer-To-Peer Networks In this type of network, every computer can communicate directly with the other computers on the same network without going through an access point. They can share files and printers in this manner. However, they may not be able to access wired LAN resources unless one of the computers acts as a bridge to the wired LAN using special software.

Extension to a Wired Network An extension to a wired network can be obtained by placing access points between the wired network and the wireless devices. With this type of network, the access point acts like a hub, providing connectivity for the wireless computers on its system. It can connect a wireless LAN to a wired LAN, allowing wireless computer access to LAN resources such as file servers or existing Internet connections.

There are both software and hardware access points. Software access points (SAPs) can be connected to the wired network and run on a computer equipped with a wireless network interface card. Hardware access points (HAPs) provide comprehensive support to most wireless features.

Multiple Access Points This type of network consists of computers connected wirelessly by using multiple access points. If a single large area cannot be covered by a single access point, multiple access points or extension points can be established. Although extension point capability has been developed by some manufacturers, it is not defined in the wireless standard.

When using multiple access points, each access point's coverage area needs to overlap another point's coverage area. This provides users the ability to move around seamlessly using a feature called **roaming**. Some manufacturers develop extension points that act as wireless relays, extending the range of a single access point. Multiple extension points can be strung together to provide wireless access to locations far from the central access point.

LAN-To-LAN Wireless Network Access points provide wireless connectivity to local computers, and local computers on different networks can be interconnected. All hardware access points have the capability of being interconnected with other hardware access points. However, interconnecting LANs over wireless connections can be a complex task.

Advantages and Disadvantages of a Wireless Network

Using a wireless network has several key advantages:

- It provides mobility to users accessing the networks.
- Connecting to the network is easier.
- The initial cost to set up the WLAN is low compared to adding Ethernet cables to a large building.
- Data can be transmitted in different ways through cellular networks such as Mobitex, DataTAC, Cellular Digital Packet Data (CDPD), and others.
- Sharing of data is easy among wireless devices.

However, a wireless network also comes with some disadvantages:

- There is no physical protection for wireless networks.
- The risk of data sharing is high. Packets are sent through the airwaves, and an attacker can easily use various wireless sniffing tools.
- Most wireless devices use a broad spectrum, so it is easy to identify the signal, making it more vulnerable to attackers.

Wireless Standards

IEEE (Institute of Electrical and Electronics Engineers) standard 802.11 has grown from a standard of infrared communication to cover most wireless communications used today. It has several issues, such as security, roaming among multiple access points, and quality of service. Therefore, there are many extensions of this standard for different uses. The following are some of the extensions:

- *802.11a*: More channels, high speed, less interference
- *802.11b*: Protocol in use when Wi-Fi became popular
- *802.11g*: Similar to 802.11b, only faster
- *802.11i*: Improves WLAN security
- *802.11n*: Next-generation Wi-Fi standard ("Wireless N") with greatly improved throughput
- *802.11ac*: Utilizes dual-band wireless technology, supporting simultaneous connections on both the 2.4 GHz and 5 GHz Wi-Fi bands

There are also other IEEE standards covering wireless communications, including the following:

- *802.15.1*: Bluetooth, a high-speed, short-distance cable replacement option
- *802.16*: WiMAX, a long-distance wireless infrastructure

Wireless Standard: 802.11a

IEEE 802.11a has the following features:

- Works at 40 MHz in the 5-GHz range
- Theoretical transfer rates up to 54 Mbps
- Actual transfer rates of approximately 26.4 Mbps
- Limited in use because it is almost a line-of-sight transmittal that requires multiple WAPs (wireless access points)
- Uses a modulation technique called coded orthogonal frequency-division multiplexing (COFDM)
- Cannot operate in same range as 802.11b/g
- Absorbed more easily than other wireless implementations
- Overcomes the challenge of indoor radio frequencies
- Uses a single-carrier, delay-spread system

Wireless Standard: 802.11b

IEEE 802.11b was used in most home and office networks before 802.11g. It has the following features:

- Operates at 20 MHz in the 2.4-GHz range
- Theoretical transfer rates up to 11 Mbps
- Actual transfer rates of 5.9 Mbps over TCP, 7.1 Mbps over UDP
- Transmits up to 8 km in a city environment
- Not as easily absorbed as 802.11a
- Can cause or receive interference from the following:
  - Microwave ovens
  - Wireless telephones
  - Other wireless appliances operating in the same frequency

Wireless Standard: 802.11g

IEEE 802.11g is replacing 802.11b in most applications. Its features include the following:

- Operates at the same frequency range as 802.11b
- Theoretical transfer rates up to 54 Mbps
- Actual transfer rates of approximately 24.7 Mbps
- Backward compatible with 802.11b
- Same limitations as 802.11b
- May suffer significant decrease in network speeds if entire network is not upgraded from 802.11b

Wireless Standard: 802.11i

IEEE 802.11i uses improved encryption for networks that use the 802.11a, 802.11b, and 802.11g standards. Its security features include the following:

- 802.1*x* for authentication (EAP and authentication server)
- Robust Security Network (RSN) to keep track of associations
- Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) to provide confidentiality, integrity, and origin authentication

Wireless Standard: 802.11n

IEEE 802.11n is the next-generation Wi-Fi standard developed by Task Group N of the IEEE. This standard merges the use of multiple antennas, more advanced encoding, and optional spectrum doubling to attain data rates of up to 600 Mbps.

802.11n has the following basic features:

- Based on multiple-in/multiple-out (MIMO) technology
- Expected increase of throughput to potentially well over 100 Mbps
- Specifies improvement to the physical layer and medium access control layer
- Improved radio technology to increase physical data transfer
- New methods to implement effective management of improved physical-layer performance modes
- Improved data transfer efficiency to reduce performance impact of physical-layer headers and radio turnaround delays that adversely affect the physical transfer rate

Wireless Standard: 802.15.1 (Bluetooth)

IEEE 802.15.1, commonly called Bluetooth, is used for wireless personal area networks, or WPANs. It is used in short-range, low-power, low-cost small networks such as the connection between a cellular phone and headset, or computer and mouse. Bluetooth specifies standards on the physical layer and data-link layer of the OSI model with the following four sublayers:

1. RF layer
2. Baseband layer
3. Link manager
4. Logical Link Control and Adaptation Protocol (L2CAP)

Wireless Standard: 802.16 (WiMAX)

WiMAX (Worldwide Interoperability for Microwave Access) is a communication system designed to support point-to-multipoint wireless broadband access. It provides high-speed mobile Internet access with ranges of up to 30 miles and speeds of up to 75 Mbps.

There are two types of WiMAX: fixed and mobile. Fixed WiMAX is similar to a cable or DSL modem service and delivers wireless last-mile access (the connection between a communications provider and a customer) for fixed broadband services. Mobile WiMAX supports both fixed and mobile applications.

Wireless Concepts

Related Technologies and Carrier Networks

The following are some technologies and carrier networks related to wireless networks:

- *CDPD (Cellular Digital Packet Data)*: CDPD works over the popular time division multiple access (TDMA) mobile network, which is the most widely deployed mobile network in the United States. CDPD modems use serial port connections or PCMCIA slots and offer speeds of up to 19.2 Kbps. Currently, TDMA operators are moving toward GSM technology.
- *1xRTT on CDMA*: CDMA (Code Division Multiple Access) is the second most popular mobile technology in the United States. The original CDMA data services offered speeds of 9,600 bps to 14.4 kbps. An upgrade called 1xRTT is supposed to achieve a speed of up to 144 kbps, but the actual speed is somewhere between 60 and 80 kbps. 1xRTT is the first phase of the CDMA2000 plan. A technology called EVDO can theoretically achieve 2 Mbps from fixed locations over CDMA.
- *GPRS/GSM*: It is a challenge for network planning engineers to manage the integration of GPRS (General Packet Radio Service) services into GSM (Global System for Mobile communications) networks. One critical challenge comes from the requirement of providing a certain quality of service (QoS) for GPRS traffic without significantly degrading the performance of existing GSM services. In a GSM/GPRS network, it is important to keep exclusive channels for GPRS in order to offer a baseline QoS for GPRS users. On the other hand, the exclusive reservation obviously reduces the capacity of GSM traffic. This causes a significant impact on the performance of GSM traffic, especially GSM handover traffic (traffic that occurs in the process of a mobile device moving from one cell carrier to another as the device crosses cell boundaries).
- *FRS and GMRS*: FRS (Family Radio Service) operates around 462 and 467 MHz and is sometimes referred to as UHF citizens' band. FRS radios share some channels with GMRS (General Mobile Radio Service) radios but are restricted to 500 mW maximum power. FRS radios come with fixed antennas and cannot be legally modified to accommodate other antennas or amplifiers. GMRS gear can include removable antennas, making it easy to use a handheld with a car mount or stationary antenna. With the use of repeaters, GMRS can be used to communicate over large distances.
- *HPNA and Powerline Ethernet*: HPNA (Home Phone Networking Alliance) provides networking capabilities over existing CAT3 cable and can share the same wire as a standard telephone line. Powerline Ethernet uses AC power lines as a physical medium for network traffic. The data speed is comparable to 802.11b.
- *802.1*x: The 802.1*x* protocol is not a wireless protocol, but rather, a method for port authentication that can be applied to nearly any network connection, whether wired or wireless. 802.1*x* is an IEEE standard that attaches EAP (Extendable Authentication Protocol) over wired or wireless Ethernet, and provides several authentication techniques including token cards, Kerberos, certificates, and public key authentication.
- *BSS and IBSS*: BSS (Basic Service Set) has one station acting as a gateway between a wireless and a wired (Ethernet) network. IBSS (Independent Basic Service Set) does not require an access point.

Service Set Identifier (SSID)

A **service set identifier (SSID)** is a unique identifier that names a particular WLAN. It is used to establish and maintain wireless connectivity. SSIDs act as a single shared password between access points and clients. Security concerns arise when the default values are not changed since these networks can then be more easily compromised. An unsecure access mode station communicates with access points by broadcasting the configured SSID, a blank SSID, or an SSID configured as "any." Because an SSID is a unique name given to a WLAN, all devices and access points present in the WLAN must use the same SSID. It is necessary for any device that wants to join the WLAN to give the unique SSID. Unfortunately, SSID does not provide security to WLAN, as it can be sniffed in plaintext from packets.

An SSID can be up to 32-characters long. The following are some common default SSIDs:

- Comcomcom
- Default SSID
- Intel
- Linksys
- Wireless
- WLAN

Is the SSID a Secret? The SSID is a key to the network, so it is necessary for every user to choose an SSID that is difficult to guess. The following shows how devices connect to a WLAN using an SSID:

- Stations searching for an access point send the SSID in a probe request.
- Access points reply with a probe reply frame that includes the SSID and BSSID (basic service set identifier) pair.
- Stations that want to be a part of the BSS (basic service set) send an association request frame, which also includes the SSID/BSSID pair in cleartext.

The SSID is secret only on closed networks with no activity. Closed networks are mainly inconvenient to legitimate users.

Authentication and Association

To become part of a BSS, a station should first authenticate itself on the network. Then it will request association to a specific access point. The access point is responsible for authentication and accepts the association of the stations unless an add-on authentication system such as RADIUS is used. The MAC address is responsible for giving the exact identity of the station or access point. Figure 1-1 is a flowchart showing how this four-way handshake operates.

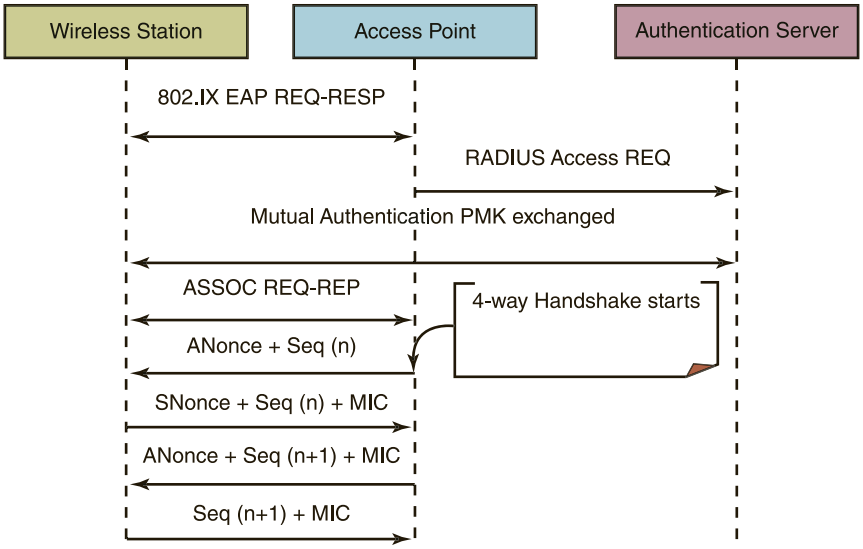


Figure 1-1 This shows the four-way handshake by which a station authenticates itself.

Authentication Modes Authentication can either be performed by a station that gives the correct SSID or through shared key authentication. In shared key authentication, the following occurs:

- The access point and all base stations in a network share a secret encryption key that has the following features:
  - Hard to deploy
  - Hard to change
  - Hard to keep secret
  - Provides no accountability
- It is necessary for the station to encrypt with WEP a challenge text that should be offered by the access point.
- An eavesdropper can determine both the plaintext and the ciphertext by performing a known plaintext attack that in turn helps to crack WEP encryption.

The 802.1x Authentication Process For 802.1*x* authentication to work on a wireless network, the AP must be able to securely identify traffic from a particular wireless client. The identification is accomplished by using authentication keys that are sent to the AP and the wireless client from the Remote Authentication Dial In User Service (RADIUS) server. When a wireless client (802.1*x* supplicant) comes within range of the AP (802.1*x* authenticator), the following process occurs:

1. The AP issues a challenge to the wireless client.
2. The wireless client responds with its identity.
3. The AP forwards the identity to the RADIUS server using the uncontrolled port.