

Gilbert Held

WILEY

Securing Wireless LANs

A Practical Guide for
Network Managers,
LAN Administrators
and the Home Office User



securing wireless LANs

**A Practical Guide for Network
Managers, LAN Administrators
and the Home Office User**

GILBERT HELD

4-Degree Consulting, Macon, Georgia, USA



WILEY

securing wireless LANs

Books by Gilbert Held, published by Wiley

Ethernet Networks, 4th, Edition

0 470 84476 0 (September 2002)

Quality of Service in a Cisco® Networking Environment

0 470 84425 6 (April 2002)

Bulletproofing TCP/IP-Based Windows NT/2000 Networks

0 471 49507 7 (April 2001)

Understanding Data Communications: From Fundamentals to Networking,

3rd Edition

0 471 62745 3 (October 2000)

High Speed Digital Transmission Networking: Covering T/E-Carrier

Multiplexing, SONET and SDH, 2nd Edition

0 471 98358 6 (April 1999)

Data Communications Networking Devices: Operation, Utilization and LAN

and WAN Internetworking, 4th Edition

0 471 97515 X (November 1998)

Dictionary of Communications Technology: Terms, Definitions and

Abbreviations, 3rd Edition

0 471 97517 6 (May 1998)

Internetworking LANs and WANs: Concepts, Techniques and Methods,

2nd Edition

0 471 97514 1 (May 1998)

LAN Management with SNMP and RMON

0 471 14736 2 (September 1996)

securing wireless LANs

**A Practical Guide for Network
Managers, LAN Administrators
and the Home Office User**

GILBERT HELD

4-Degree Consulting, Macon, Georgia, USA



WILEY

Copyright © 2003

John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester,
West Sussex PO19 8SQ, England

Telephone (+44) 1243 779777

Email (for orders and customer service enquiries): cs-books@wiley.co.uk
Visit our Home Page on www.wileyeurope.com or www.wiley.com

All Rights Reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except under the terms of the Copyright, Designs and Patents Act 1988 or under the terms of a licence issued by the Copyright Licensing Agency Ltd, 90 Tottenham Court Road, London W1T 4LP, UK, without the permission in writing of the Publisher. Requests to the Publisher should be addressed to the Permissions Department, John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England, or emailed to permreq@wiley.co.uk, or faxed to (+44) 1243 770620.

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold on the understanding that the Publisher is not engaged in rendering professional services. If professional advice or other expert assistance is required, the services of a competent professional should be sought.

Other Wiley Editorial Offices

John Wiley & Sons Inc., 111 River Street, Hoboken, NJ 07030, USA

Jossey-Bass, 989 Market Street, San Francisco, CA 94103-1741, USA

Wiley-VCH Verlag GmbH, Boschstr. 12, D-69469 Weinheim, Germany

John Wiley & Sons Australia Ltd, 33 Park Road, Milton, Queensland 4064, Australia

John Wiley & Sons (Asia) Pte Ltd, 2 Clementi Loop #02-01, Jin Xing Distripark, Singapore 129809

John Wiley & Sons Canada Ltd, 22 Worcester Road, Etobicoke, Ontario, Canada M9W 1L1

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

British Library Cataloguing in Publication Data

A catalogue record for this book is available from the British Library

ISBN 0-470-85127-9

Typeset in 10.5/13pt Melior by Laserwords Private Limited, Chennai, India

Printed and bound in Great Britain by Antony Rowe Ltd, Chippenham, Wiltshire

This book is printed on acid-free paper responsibly manufactured from sustainable forestry in which at least two trees are planted for each one used for paper production.

*To the students of Georgia College and State University
whose inquisitive minds makes teaching most interesting and rewarding.*

contents

Preface xv

Acknowledgements xvii

Chapter 1 Introduction to Wireless LANs 1

1.1	SECURING THE INSECURE	2
1.1.1	AAE AND A FUNCTIONS	2
1.1.2	AUTHENTICATION	2
1.1.3	AUTHORIZATION	3
1.1.4	ENCRYPTION	3
1.1.5	ACCOUNTING	4
1.1.6	PRACTICAL NETWORK PROTECTION METHODS	4
1.2	NETWORK ARCHITECTURE	7
1.2.1	BASIC NETWORKING DEVICES	7
1.2.2	THE WIRELESS LAN STATION	8
1.2.3	THE ACCESS POINT	10
1.2.4	THE WIRELESS BRIDGE	13
1.2.5	THE WIRELESS ROUTER	13
1.2.6	THE BASIC SERVICE SET	18
1.2.7	THE EXTENDED SERVICE SET (ESS)	20
1.2.8	STATION SERVICES	21
1.3	IEEE WIRELESS LAN STANDARDS	27
1.3.1	THE BASIC IEEE 802.11 STANDARD	28
1.3.2	802.11B	30
1.3.3	802.11A	30
1.3.4	802.11C	30
1.3.5	802.11D	31
1.3.6	802.11E	31
1.3.7	802.11F	31

1.3.8	802.11G	31
1.3.9	802.11H	31
1.3.10	802.11I	32
1.4	BOOK PREVIEW	32
1.4.1	FRAME FORMATS AND BASIC SECURITY OPERATIONS	32
1.4.2	UNDERSTANDING WIRELESS SIGNALS	33
1.4.3	UNDERSTANDING WEP	33
1.4.4	SECURITY RISKS	33
1.4.5	PROPRIETARY SECURITY ENHANCEMENT TECHNIQUES	33
1.4.6	STANDARDS BASED SECURITY	34

Chapter 2 Frame Formats and Basic Security Operation 35

2.1	FRAME FORMATS	35
2.1.1	BASIC FRAME FORMAT	36
2.1.2	FRAME CONTROL FIELD	36
2.1.3	CONTROL FRAMES	43
2.1.4	MANAGEMENT FRAMES	46
2.1.5	THE AUTHENTICATION PROCESS	53
2.2	WEP AND PRIVACY	53
2.2.1	MISCONCEPTIONS	53
2.2.2	DEVELOPMENT CONSTRAINTS	54
2.2.3	DEFICIENCIES	58

Chapter 3 Understanding Wireless Signals 61

3.1	THE WIRELESS RF SPECTRUM AND BASIC MEASUREMENTS	62
3.1.1	FREQUENCY	62
3.1.2	PERIOD AND WAVELENGTH	63
3.1.3	BANDWIDTH	64
3.1.4	THE FREQUENCY SPECTRUM	64
3.1.5	POWER MEASUREMENTS	66
3.1.6	POWER LEVEL	69
3.1.7	SIGNAL-TO-NOISE RATIO	69
3.2	ANTENNA BASICS	71
3.2.1	BASIC OPERATION	72
3.2.2	CATEGORIES	73
3.2.3	ANTENNA GAIN	73

3.2.4	DIRECTIONALITY AND EIRP	74
3.2.5	POWER LEVELS	74
3.2.6	PROPAGATION LOSS	75
3.2.7	INCREASING ANTENNA GAIN	76
3.2.8	POWER LIMITS	77
3.2.9	RECEIVER SENSITIVITY	78
3.2.10	REDUCING EMITTED RADIATION	79
3.2.11	HORIZONTAL TRANSMISSION DISTANCE	80
3.2.12	EQUIPMENT POSITIONING	81
3.2.13	USING MONITORING EQUIPMENT	83

Chapter 4 Understanding WEP 85

4.1	THE WEP FRAME BODY	86
4.1.1	THE IV	86
4.1.2	THE ICV	87
4.1.3	THE NAKED DEFAULT	87
4.1.4	WEP KEY LIMITATIONS	90
4.2	LOCATING AND OBSERVING WIRELESS LAN TRAFFIC	91
4.2.1	NETWORK STUMBLER	91
4.2.2	MONITORING WITH AIROPEEK	93
4.3	RC4	97
4.3.1	OVERVIEW	97
4.3.2	OPERATION	98
4.3.3	ILLUSTRATIVE EXAMPLE	99
4.3.4	STRENGTHS AND WEAKNESSES	102
4.4	WEP WEAKNESS	102
4.4.1	UNSAFE AT ANY SIZE	102
4.4.2	THE INSECURITY OF 802.11	103
4.4.3	EXPLOITING RC4 WEAKNESS	107
4.4.4	BREAKING WEP	108
4.4.5	AIRSNORT	109
4.4.6	WEPCRACK	110

Chapter 5 Security Risks and Countermeasures 113

5.1	THE SSID	113
5.1.1	OVERVIEW	114
5.1.2	OVERRIDING THE SSID	114

5.1.3	OBTAINING THE SSID	115
5.1.4	COUNTERMEASURES	117
5.2	EAVESDROPPING	117
5.2.1	OVERVIEW	117
5.2.2	THREATS	118
5.2.3	COUNTERMEASURES	118
5.3	MASQUERADE	121
5.3.1	OVERVIEW	121
5.3.2	COUNTERMEASURES	122
5.4	DATA MODIFICATION	124
5.4.1	OVERVIEW	124
5.4.2	COUNTERMEASURES	124
5.5	FILE SHARING	124
5.5.1	OVERVIEW	124
5.5.2	WINDOWS 95	125
5.5.3	WINDOWS 2000	128
5.5.4	COUNTERMEASURES	131
5.6	JAMMING	131
5.6.1	OVERVIEW	131
5.6.2	COUNTERMEASURES	132
5.7	ENCRYPTION ATTACKS	133
5.7.1	OVERVIEW	134
5.7.2	COUNTERMEASURES	135
5.8	SNMP	135
5.8.1	CODING FLAWS	136
5.8.2	SNMP VERSIONS	136
5.8.3	COUNTERMEASURES	141
5.9	BROADCAST MONITORING	141
5.9.1	OVERVIEW	142
5.9.2	COUNTERMEASURES	144
5.10	ACCESSING A MANAGEMENT CONSOLE	145
5.10.1	OVERVIEW	145
5.10.2	COUNTERMEASURES	145
5.11	THEFT OF HARDWARE	146
5.11.1	OVERVIEW	146
5.11.2	COUNTERMEASURES	146
5.12	ROGUE ACCESS POINTS	147
5.12.1	OVERVIEW	147
5.12.2	COUNTERMEASURES	147

Chapter 6 Proprietary Security Enhancement Techniques 149

6.1	MAC ADDRESS AUTHENTICATION	150
6.1.1	IEEE 802.11 AUTHENTICATION	150
6.1.2	IMPLEMENTATION METHODS	151
6.1.3	ACCESS POINT UTILIZATION	151
6.1.4	USING A RADIUS SERVER	151
6.1.5	DATAFLOW	151
6.1.6	LIMITATIONS WHEN USING AN AP	151
6.1.7	LIMITATIONS USING A RADIUS SERVER	152
6.1.8	CHAP	153
6.1.9	VISITOR CONSIDERATIONS	154
6.2	CLOSED SYSTEM OPTION	154
6.2.1	OVERVIEW	155
6.2.2	LIMITATIONS	155
6.3	SYSTEM ACCESS PASS PHRASE	155
6.3.1	OVERVIEW	155
6.3.2	NETWORK ACCESS	156
6.3.3	LIMITATIONS	156
6.4	DYNAMIC KEY EXCHANGE AND WEAK KEY AVOIDANCE	156
6.4.1	DYNAMIC KEY EXCHANGE	157
6.4.2	OVERVIEW	157
6.4.3	LIMITATIONS	157
6.4.4	WEAK KEY AVOIDANCE	158
6.4.5	OVERVIEW	158
6.4.6	LIMITATIONS	158
6.5	PROTECTING WIRELESS CLIENTS FROM THE PUBLIC NETWORK	158
6.5.1	OVERVIEW	159
6.5.2	CISCO ACCESS LISTS	159
6.5.3	SMC NETWORKS BARRICADE PACKET FILTERING	161
6.5.4	LIMITATIONS	163
6.5.5	SUMMARY	165
6.6	ANTENNA ORIENTATION AND SHIELDING	166
6.6.1	OVERVIEW	166
6.6.2	ALTERING SIGNAL STRENGTH	166
6.6.3	LIMITATIONS	167
6.7	MINIMIZING TRANSMIT POWER AND ANTENNA CONTROL	168
6.7.1	POWER MANAGEMENT	168
6.7.2	ANTENNA CONTROL	170

6.7.3	POWER LEVEL CONTROL	170
6.7.4	LIMITATIONS	171
6.8	WIRELESS INTRUSION DETECTION	172
6.8.1	OVERVIEW	172
6.8.2	LIMITATIONS	172
6.9	LEAP	173
6.9.1	OVERVIEW	173
6.9.2	OPERATION	174
6.9.3	CONFIGURATION	174
6.9.4	CONFIGURING THE ACCESS POINT	175
6.9.5	CLIENT CONFIGURATION	175
6.9.6	ENABLING WEP	177
6.9.7	LIMITATIONS	181

Chapter 7 Standards Based Security 183

7.1	THE IEEE 802.1X STANDARD	183
7.1.1	OVERVIEW	183
7.1.2	GENERAL OPERATION	184
7.1.3	DATA FLOW	185
7.1.4	THE EAP PROTOCOL	187
7.1.5	MESSAGE TYPES	188
7.1.6	EAP PACKET FORMAT	188
7.1.7	THE DUAL-PORT AUTHENTICATION MODEL	189
7.1.8	SECURITY LIMITATIONS	189
7.1.9	USING THE CISCO AIRONET 350	193
7.1.10	CLIENT SETUP	193
7.1.11	NETWORK SECURITY	198
7.1.12	USING WINDOWS XP	200
7.1.13	ACCESS POINT SETUP	203
7.1.14	SECURITY SETUP	209
7.1.15	ACCESS	209
7.1.16	SECURITY SETUP OPTIONS	211
7.1.17	CLOSING THOUGHTS	219
7.2	EVOLVING ENCRYPTION	220
7.2.1	TKIP	221
7.2.2	AES	222

7.3 VPNs AND TUNNELING PROTOCOLS 224

- 7.3.1 VPN OVERVIEW 224**
- 7.3.2 NEED FOR SECURITY 225**
- 7.3.3 TYPES OF VPNs 226**
- 7.3.4 APPLICABILITY TO WIRELESS LANs 228**
- 7.3.5 VPN PROTOCOLS 229**
- 7.3.6 PPTP 229**
- 7.3.7 L2TP AND IPSec 232**
- 7.3.8 VPN OPERATIONS 234**

Appendix A Wireless LAN Security Checklist 245**Index 249**

preface

Wireless LANs are becoming ubiquitous. From hotel lobbies to Starbucks coffee shops, to airports and offices, it is difficult not to be able to pick up a wireless LAN signal. Accompanying the growth in the use of wireless LANs is a recognition that as initially designed they are not secure.

The focus of this book is upon wireless LAN security. In this book we will examine how wireless LANs operate, with special attention focused upon the manner in which security occurs under the IEEE 802.11 wireless LAN standard and its extensions, and why the standard and its extensions are weak. We will use this information to note many vulnerabilities associated with the use of wireless LANs and the security risks that can occur via an over-the-air transmission method. Because network managers and LAN administrators, as well as small business and home users of wireless LANs, need to know how to overcome the security limitations of wireless LANs, several chapters in this book are devoted to security enhancement techniques. One chapter is focused upon vendor-specific solutions, while a second chapter examines the use of existing and evolving standards that can be employed to literally harden your wireless LAN.

Throughout this book we will note via the use of vendor products the reason why, as designed, wireless LANs are insecure. This information will enable us to observe how easy it was for two men in a van, who moved from parking lot to parking lot in Silicon Valley, to obtain information about the use of wireless LANs from people operating equipment within the buildings the men focused their antennas upon. Although several news articles about the exploits of these two men appeared in major newspapers, what was significantly lacking was an explanation concerning why they were able to easily understand what was being transmitted and how this third party activity could be prevented, topics that I will discuss in this book.

While the primary focus of this book is upon technical issues, upon occasion we will also focus upon common sense items. For example, by understanding the default settings of IEEE 802.11 wireless LAN functions and simply changing a few settings, it becomes possible to make it more difficult for a third party to both monitor and understand data being transmitted over-the-air. As another example of applying common sense to security, the positioning of

equipment and the use of shielding can be employed to block signals. Thus, if a third party cannot receive a signal, they obviously cannot intercept or alter the signal.

Although there are several common sense approaches to securing a wireless LAN, unfortunately we need more than common sense to make wireless LANs secure. Thus, we will examine a number of techniques that can be employed to literally harden our wireless communication. Through the use of a number of computer screen captures I will illustrate tools and techniques you can consider to secure your wireless communications.

As a professional author I look forward to any comments you may have concerning the material presented in this book. Please feel free to contact me directly or via my publisher, whose address is contained on the copyright page of this book. Let me know if I omitted an item of interest, if I spent too many pages on a particular topic, or any other comments you wish to share with me. You can contact me directly via email at gil.held@yahoo.com.

Gilbert Held
Macon, GA

acknowledgements

The creation and publication of a book represents a team effort. From the preparation of a manuscript through its publication requires the efforts of many people that I would be remiss if I did not acknowledge.

Many books commence with a proposal and this book is no exception. That proposal is reviewed, sometimes proposals are revised, and many times a number of emails and other correspondence is required prior to a publisher proceeding to issue a contract. I would like to thank Birgit Gruber and Dr. Sally Mortimore for their efforts in administering my initial proposal and shepherding it through the administrative process required to initiate a contract.

As a frequent lecturer who travels to many of the more interesting areas of the globe, many years ago I realized that it was rather difficult to recharge my notebook. Regardless of the set of electrical adapters I would take with me, the round, triangular and concentric circular electrical sockets typically would not mate with my adapters. After a considerable amount of frustration I returned to the use of the most reliable writing instrument – a pencil. Unfortunately, my handwriting may not be the best, especially when writing during air turbulence at 30,000 feet. Thus, once again I am indebted to Mrs. Linda Hayes for converting my handwritten draft into the electronic manuscript required by my publishers.

Once a manuscript is submitted for publication a series of behind the scene operations occur. First, the manuscript is reviewed to ensure all material is present. During the editing process questions that may require clarification are sent to the author and responses are incorporated into the manuscript. Next, the manuscript must be typeset, a cover is designed and a printer creates the book you are now reading. During this production process a large number of people literally work behind the scenes and I appreciate their efforts.

Last but not least, the creation of a book is a time-consuming effort. This is especially true when writing a book covering wireless LAN security that required the setup of equipment in my home to illustrate many concepts. Thus, I am also indebted to my wife Beverly for her support and understanding while I spent many long evenings and weekends writing the manuscript that resulted in this book.

chapter one

Introduction to Wireless LANs

Like any introductory chapter, our goal here is to become acquainted with basic concepts. Because this book is oriented towards wireless LAN security, we need to obtain a firm understanding of the components used in a wireless LAN and their relationship to wired networking devices to appreciate wireless security issues.

Because many network managers and LAN administrators cannot afford the time required to read a book, we will begin this chapter with a section titled Securing the Insecure. This section will note that wireless LAN security as defined by the IEEE 802.11 wireless LAN standard is weak and easily compromised. Methods that can be used to overcome existing security limitations will then be described. This preview of methods and techniques is presented as ‘food for thought’ and will be considerably expanded upon in the remainder of this book.

Once we obtain an appreciation of methods and techniques we should consider to secure any existing wireless LAN our organization may be operating, we will focus upon the basic architecture associated with IEEE 802.11 wireless LANs. In doing so we will note the general relationship of different types of wireless networking devices that are used to construct a wireless LAN. Once we obtain an appreciation of the types of devices associated with the construction of wireless LANs and obtain an overview of the alphabet soup of wireless LAN standards, we will conclude this chapter with a preview of succeeding chapters in this book. This preview can be used as is or in conjunction with the table of contents and index to locate information of immediate concern. Now that we have a basic roadmap concerning the focus of the two sections in this chapter, let’s grab a Pepsi, Coke or another beverage and begin our journey into the wonderful world of wireless LANs.

1.1 Securing the insecure

Most books, and this one is no exception, use a series of chapters to present a topic of interest to readers. Because the basic method of security provided under the Institute of Electrical and Electronic Engineers (IEEE) 802.11 wireless LAN standard and its 'a' and 'b' extensions is relatively weak and easily compromised, we will discuss methods that can be used to secure the insecure in this section. We shall discuss and describe a variety of security enhancement methods in this section while deferring a detailed description of those methods to later chapters. The rationale for this action is based upon the need of many network managers and LAN administrators who are familiar with wireless LAN technology, but have an immediate requirement to obtain some practical security solutions for their organization without having to read an entire book. However, for readers that want to fully understand why Wired Equivalent Privacy (WEP), which provides wireless LAN security, is weak and how and why security enhancements discussed in this section function, the remainder of this book provides those details.

1.1.1 AAE and A Functions

There are three, and for some organizations four, functions that are necessary to provide a high level of security. Those functions are authentication, authorization, encryption and accounting. Very often the omission of encryption results in the remaining three security related functions being referred to as triple A or AAA.

1.1.2 Authentication

Authentication verifies the identity of a user. Under WEP authentication occurs through the use of a common key configured on clients and an access point. That key performs encryption. Each client and the access point are configured with the same key, resulting in the term 'shared key cryptography' used to refer to the encryption method. An access point can issue a challenge to any station attempting to associate with it. The station then uses its shared key to encrypt a response to authenticate itself and gain access to the network. Because WEP is weak and the shared key can be recovered via passive monitoring of network traffic, this means that IEEE 802.11 wireless LANs do not have a secure method of authentication, but one that can be compromised.

Some proprietary techniques employed by vendors use the MAC address of the wireless PC Card for authentication. Because WEP, which provides encryption services, does not hide source MAC addresses this means that an

unauthorized third party could easily learn and spoof a MAC address and become an uninvited participant on a wireless network. To provide a higher level of authentication you should consider a solution that authenticates the user and not the user's hardware. Examples of potential authentication solutions include the use of a RADIUS server, a secure ID card and other user/password authentication schemes that require a wireless client to be verified by a server prior to gaining access to the network.

1.1.3 Authorization

Authorization represents the permission or denial of access to various network and computer functions based upon the identity of the user. In a wireless LAN environment the 802.11 standard and its extensions do not address authorization.

You can effect network and computer authorization through a variety of hardware and software products. For network authorization you can consider router access lists and firewall configurations as a mechanism to enable or disable the flow of wireless traffic to the corporate intranet and any Internet connection your organization may maintain. In a computer environment you can use operating system functionality, as well as third party products, to enable or disable the ability of users to access directories and files, run different programs and perform other types of computer activities.

1.1.4 Encryption

We previously noted that WEP is weak and can be compromised. In fact, there are several programs that can be obtained via the Internet that enable any unauthorized third party to passively monitor wireless LAN traffic and recover the WEP key in use. Once this action is accomplished, the third party can configure their client station with the WEP key in use and passively record and read all network activity.

Although the details concerning the weakness of WEP will be covered later in this book, there are several solutions to this problem that deserve a mention at this time.

One of the earliest solutions to the weakness of WEP involves dynamically changing encryption keys. Thus, several vendors now support dynamic key changing as a mechanism to preclude the ability of an unauthorized third party from constructing a database of frames using the same key sufficient for successfully running a key recovery program.

Another potential solution to the weakness of WEP encryption involves using a higher level secure protocol at layer 3. Examples of layer 3 secure

protocols that can be considered include Secure Sockets Layer (SSL) or IPSec, the latter is commonly used to create a Virtual Private Network (VPN) over a public network such as the Internet.

When considering the use of a VPN to protect wireless communications, most solutions involve the connection of a firewall between the access point and the wired network infrastructure. The firewall provides a VPN capability to each wireless client at layer 3, commonly using IPSec. This action alleviates the necessity to enable WEP as long as your organization uses IP at layer 3.

1.1.5 Accounting

Although not required to secure a network, accounting commonly represents a function of many security performing devices that can be valuable for setting rules and obtaining historical data which can be used by law enforcement agencies, if the need arises, to prosecute an individual. Many servers can be configured to log access requests as they occur to form a database of different events, such as successful or unsuccessful logon attempts. Using this database the server can be configured to enable or disable future logons based upon the prior history of unsuccessful logons during different predefined periods of time, a situation referred to as a lockout. In addition, the history of activity based upon MAC and layer 3 addresses attempting to access different facilities can be used by prosecutors if you need to alert law enforcement agencies about actual or attempted break-ins.

Now that we have an appreciation for the use of authentication, authorization, encryption and accounting to secure a network we will conclude this section by focusing upon practical methods you can consider to secure your wireless LAN. Each of these methods will be described in considerable detail later in this book, but are mentioned here as a mechanism to assist readers who are currently operating wireless LANs and may require help in plugging security holes prior to taking the time to read the hundreds of pages that follow.

1.1.6 Practical network protection methods

Regardless of the size of your wireless network there are several practical steps you can employ to enhance the level of security of your network. In concluding this section we will briefly discuss each method, with more detailed information presented later in this book.

1.1.6.1 Enable WEP

While WEP can be compromised by default, most products disable its use to include some hardware devices that support dynamic key exchange. Thus, if

you simply accept default settings your transmissions may be occurring in the clear.

1.1.6.2 Default Network Name Change

Each access point and served clients are identified by a network name. Client stations need to be configured with an appropriate network name to gain access to the access point. Because many manufacturers configure their access points with default network names, it is relatively easy to guess a valid name. Thus, changing the default name at least makes it a bit harder for an unauthorized third party to gain access to your network.

1.1.6.3 Disable Network Name Broadcasts

Access points periodically transmit beacon frames that enable clients to note the presence of the access point. By default, access points transmit their network name in beacons, allowing an unauthorized third party to easily note the name of the network. By disabling the broadcast of network names you make it more difficult for unauthorized people to recognize your wireless LAN.

1.1.6.4 Periodically Change Encryption Keys

If you do not have software that automatically changes WEP keys you should consider changing them periodically. As a minimum, changing keys forces an unauthorized third party that recovered a prior key literally ‘back to square one,’ since they will now need to recapture millions of frames to recover the new key in use.

1.1.6.5 Restrict MAC Addresses

Some wireless access points can be configured to restrict access based upon client Media Access Control (MAC) addresses. Although MAC addresses can be learned via passive monitoring, its use as an access mechanism makes it more difficult for an unauthorized third party to gain access to your network.

1.1.6.6 Position and Shield Access Point Antennas

Because an unauthorized third party cannot listen to what they cannot hear, both antenna positioning and shielding can reduce or eliminate radio frequency waves flowing to parking lots and other floors in your building. Most access points have a flexible antenna that can be positioned to minimize its

radiation pattern. In addition, the placement of shielding behind the antenna of an access point can minimize or eliminate radiation to the rear of the device. If the access point is positioned along a wall shielding can be quite effective in preventing an unauthorized third party, lurking in the corporate parking lot, from recording access point communications.

1.1.6.7 Limit DHCP Clients

Most access points support the Dynamic Host Configuration Protocol (DHCP) to dynamically assign IP addresses to clients. If you limit the number of addresses that can be issued to the number of clients in your network, you also limit the ability of an unauthorized third party to gain access to your network.

1.1.6.8 Implement Stronger Authentication and Encryption

The use of the Challenge Handshake Authentication Protocol (CHAP) can be used by itself to authenticate a user or with a MAC hardware address to authenticate both the hardware and the user. Either method will provide a much higher level of authentication than currently supported by the IEEE 802.11 wireless LAN standard. Concerning encryption, using a layer 3 protocol while waiting for the development of more secure encryption techniques or wireless LANs can enhance network security. As we will note later in this book, readily available secure encryption methods include Secure Socket Layer (SSL) and IPSec. Unfortunately, the former is only useful for browser to server activity and does not protect email and other applications unless they are Web enabled, while the latter may be difficult to install and may adversely effect performance.

1.1.6.9 Disable Folder Sharing

If your organization operates a mixture of Windows operating systems, folder sharing can represent a weak link. This is because some versions of Windows have relatively rudimentary controls over access to files and folders that are shared. You should consider moving files that multiple people require access to onto servers located behind a firewall. This action will enable a more restrictive method of access to be employed. Once this is accomplished there is no need to share folders among clients and folder sharing should be disabled. Because the use of a firewall can have several benefits, we will conclude our discussion of practical network protection by turning our attention to the use of this networking device.

1.1.6.10 Use a Firewall

If you place a firewall behind the access point between that device and your wired network, you obtain the ability to take advantage of the security features of the firewall. Those features can include filtering based upon source and destination IP addresses, port numbers and other parameters as well as the use of IPSec to create a VPN over your wireless infrastructure.

1.2 Network architecture

When this author worked in the Washington, DC area many years ago, he became acquainted with one of the earliest types of wireless LANs which employed diffused infrared (IR) transmissions, bouncing IR off the ceiling as a mechanism to transmit data within an office environment. This IR based LAN was proprietary to a specific vendor and until 1997 other wireless LANs developed by commercial organizations were also proprietary. In 1997 the Institute of Electrical and Electronics Engineers (IEEE) adopted the 802.11 standard, which represents the first wireless LAN standard to be promulgated by a standards making organization. This standard defined transmission rates of 1 and 2 Mbps for three Media Access Control (MAC) methods – Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS) and infrared.

Although the initial 802.11 standard generated a degree of interest from communications equipment manufacturers, it wasn't until the 802.11b extension to the 802.11 standard was adopted that wireless LANs achieved significant growth. That extension raised the maximum data transmission rate to 11 Mbps, which enabled the technology to become well suited for both home and office applications that included Web browsing and file transfers. Although the IEEE introduced several additional extensions to its 802.11 standard they all support a common network architecture that we will shortly note. Because IEEE compatible wireless LANs account for the vast majority of such products currently manufactured, this book is oriented to security issues associated with IEEE wireless LAN standards.

1.2.1 Basic networking devices

There are four generic types of wireless LAN devices that can be used to form different types of wireless network structure. Those devices are the wireless LAN station, a special type of station referred to as an access point, and two special types of access points commonly known as wireless routers

and wireless bridges. In this section we will note the basic operation and functionality of each type of wireless device. This information will be used to note how such devices can be networked and the different networks' architectures resulting from these devices communicating with one another.

1.2.2 The wireless LAN station

The basic building block of a wireless LAN is the wireless LAN station. The station is a term used to represent any device that incorporates the functionality of the 802.11 standard in the MAC and physical layers to support wireless communications. A station can represent a notebook or desktop computer or devices referred to as access points, bridges and broadband routers.

1.2.2.1 The Network Interface Card (NIC)

Most notebook and desktop PCs obtain their wireless LAN functionality via the use of a Network Interface Card (NIC) and a software driver. The NIC is typically fabricated as a Type II PC Card designed for insertion into a PC Card slot built into a laptop and notebook. Figure 1.1 illustrates an SMC Networks 802.11a Wireless Card Bus Adapter. Note that the left portion of the adapter is inserted into a PC card slot, with the black portion of the adapter that contains a built-in antenna protruding out of the card slot.

As we turn our attention to over-the-air transmission and potential interceptions of signals later in this book, we will note that such signals can be captured at far greater distances than the transmission range noted by manufacturers of 802.11 compatible products. The reason for this results from



Figure 1.1 The SMC Networks 802.11a Wireless Card Bus Adapter (photograph courtesy of SMC Networks).

the use of relatively small omni-directional antennas in 802.11 compatible products as a mechanism to promote portability and reduce cost. In comparison, larger uni-directional antennas that can be focused towards a building where a wireless LAN is operating may be able to use its higher level of antenna sensitivity to recover weak signals considerably beyond the range of conventional 802.11 antennas.

1.2.2.2 NIC Form Factors

In addition to PC Cards, other popular form factors used for the fabrication of wireless LAN network interface cards include a PCI bus based adapter and a USB compatible self-contained NIC. An example of a PCI bus-based adapter is illustrated in Figure 1.2.

The SMC Networks bus-based adapter card, shown in Figure 1.2, is similar to other vendor products in that it consists of a PCI adapter card onto which a PC Card containing the wireless NIC is mounted. If you carefully examine the top portion of Figure 1.2 you will note that the PCI board connectors are inserted into a system expansion slot, thus indicating that the photograph of the board is actually upside down to show the vendor logo. You can also note the black edge on the right portion of the illustration that represents the antenna that will protrude from the rear of a system expansion unit. The



Figure 1.2 Most vendors fabricate a PCI bus based NIC by mounting a PC Card onto a PCI adapter card (photograph courtesy of SMC Networks).

protrusion will occur once the PCI card is installed in the system expansion slot of a desktop computer. For some unexplained reason PCI cards have the full antenna protruding from the back of the system expansion unit while a PC Card form factor NIC usually has most, but not all, of the antenna protruding from the PC Card slot it is installed into.

Because it may not be a simple task to remove the cover of a system unit and obtain an available system expansion slot, some vendors added a self-contained NIC with a USB interface to their product line. This enables a station to obtain a wireless transmission capability without the user having to open the system unit of a desktop or use a PC Card slot on a desktop or laptop.

1.2.3 The access point

An access point represents a second type of wireless station. The access point functions as a two-port bridge, linking a wired infrastructure to the wireless infrastructure. As a layer 2 bridge it operates using learned MAC addresses to perform filtering, forwarding and flooding, operations which we will shortly examine.

Figure 1.3 illustrates the SMC Networks 802.11a Wireless Access Point. The dual antennas mounted on the access point enable the device to select the best possible signal since signals are typically reflected off stationary and moving objects on their path from source to destination, resulting in each transmitted signal having multiple received components. The use of dual antennas is referred to as space diversity.



Figure 1.3 The SMC Networks 802.11a Wireless Access Point uses dual antennas (photograph courtesy of SMC Networks).

1.2.3.1 Operation

We previously indicated that an access point represents a layer 2 bridge that operates using filtering, forwarding and flooding. To illustrate how an access point can learn addresses and simply needs to be powered on, let's assume we both have a wired and wireless infrastructure as illustrated in Figure 1.4.

In examining Figure 1.4, for simplicity let's assume the wireless client stations have MAC addresses A, B and C, while the three wired stations have MAC addresses D, E and F. Of course, in the real world each MAC address consists of 48 bits or 6 bytes. The first three bytes identify the manufacturer of the network interface card used by the wireless station while the last three bytes identify the NIC produced by the manufacturer. The value placed in the first three bytes is assigned to manufacturers by the IEEE. If a manufacturer is successful and needs additional manufacturer IDs, they would then return to the IEEE to seek additional three byte codes.

Returning our attention to Figure 1.4, let's examine the series of operations shown in the table portion of the figure to obtain an appreciation for the manner in which an access point functions as a two-port bridge and automatically constructs a port/address table as well as operates by following the so-called 3F rule – flooding, filtering and forwarding.

Flooding

For the first operation let's assume station A transmits to station B. If the access point was just powered on, its port/address table is empty. The access

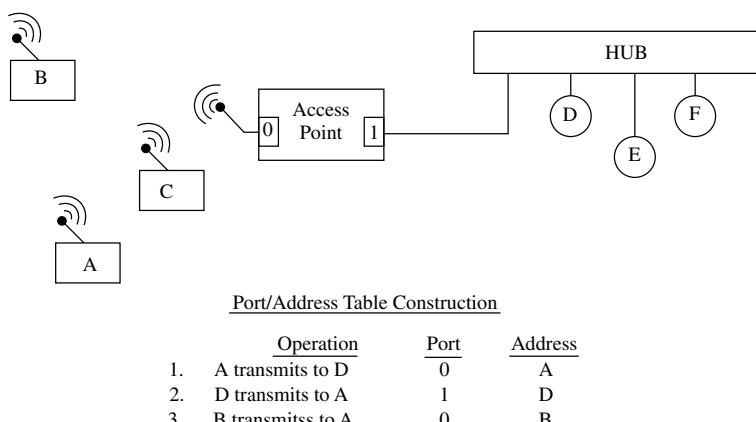


Figure 1.4 An access point constructs a port/address table by examining the source addresses in frames.

point receives a frame with source address A and destination address D. Since the access point cannot match the destination address to an entry in its port/address table, it floods the frame, transmitting it onto all other ports than the port it was received on. In this example this means the access point transmits the frame onto port 1. In doing so it notes that the source address (A) was received on port 0 and updates its port/address table by entering the association of address A with port 0. Thus, the entry becomes:

Port	Address
0	A

Forwarding

If we assume that station D responds to the transmission from A, the access point receives a frame on port 1 with a destination address of A and a source address of D. When the access point checks the entries in its port/address table, it notes that address A is associated with port 0 and forwards the frame out to port 0, which is onto the wireless LAN. The access point also checks its port/address table to determine if address D was previously learned. Since it wasn't, the access point updates its port/address table by associating address D with port 1 as a new entry in the table. Thus, at this point in time, the contents of the port/address table are as follows:

Port	Address
0	A
1	D

Filtering

In the third example, shown in the lower portion of Figure 1.4, station B transmits to station A via the access point. As we will note later in this chapter, this type of transmission, under which wireless stations communicate with one another via an access point, is referred to as infrastructure networking. When station B transmits to station A, the access point searches its port/address table for the destination address (A). In this example the access point previously learned that address A is associated with port 0. Thus, the access point will not forward the frame onto the wired infrastructure, filtering the frame from flowing out of port 1. Instead, the access point rebroadcasts the frame onto port 0. Thus, the access point automatically creates its port/address table entries via noting the source MAC address of each frame and the port it arrived on.

It should be noted that this last operation, the rebroadcast of a filtered frame, is only applicable to the wireless port of an access point and differs from a conventional bridge that does not rebroadcast frames which are filtered.

Access points function as a relay station, resulting in frames transmitted from one wireless station to another being rebroadcast by the access point.

Because memory is finite an access point typically records the time it learned an association between a MAC address and a port. That time can be considered to represent a third column in a port/address table. Periodically, the access point will examine the time of occurrence of entries in the port/address table, removing old entries as a mechanism to allow new entries to be added to the table.

The series of IEEE standards support two types of Radio Frequency (RF) communications (FHSS and DSSS) and IR communications. RF communications can occur either in the 2.4 GHz or 5 GHz band, with the lower band supported by the 802.11 and 802.11b standards, 5 GHz operations are supported by the 802.11a standard. While a station normally supports one communications method in one frequency band some access points are manufactured to support communication in both frequency bands. This is normally accomplished by an access point being fabricated to accept two PC Cards, one that supports 2.4 GHz operations while the other supports 5 GHz operations.

1.2.4 The wireless bridge

The wireless bridge represents a special type of access point. This type of access point typically consists of a separate base unit and antenna that are connected to one another by a low loss cable.

1.2.4.1 Operation

The access point base unit of a wireless bridge functions as previously described when we discussed the stand alone access point. The key difference between these two devices is in the separation of the antenna from the base unit and its directional capability. Typically the wireless bridge antenna is designed for mounting on the edge or roof of a building. Its high level of receiver sensitivity provides a line of sight communications capability that permits communication between two geographically separated locations that can be between 4 and 7 km apart.

1.2.5 The wireless router

Building upon the functionality of the access point, several vendors introduced wireless routers that add a routing capability to an access point. In addition to providing support for basic routing, wireless routers typically

include support for the Dynamic Host configuration Protocol (DHCP) and Network Address Translation (NAT).

1.2.5.1 DHCP

DHCP provides a router with the ability to dynamically issue IP addresses to each station. In addition to assigning stations with an IP address, the router supporting DHCP will also dynamically issue the gateway and DNS server addresses to each station. This action simplifies the network configuration process associated with each station since the workstation operator only needs to click on a radio button on a configuration screen instead of having to enter specific IP addresses into their network setting screens. Figure 1.5 illustrates the simplicity of the configuration process when a router functions like a DHCP server. In the left portion of Figure 1.5 the Agere System's Orinoco PC Card is selected. Selecting the button labeled 'Properties' (shown in the right middle area of the Network dialog box) results in the display of the TCP/IP Properties dialog box, which is shown in the right portion of Figure 1.5. If you carefully examine that dialog box you will note the radio button associated with 'Obtain an IP address automatically' is selected. This action alleviates the

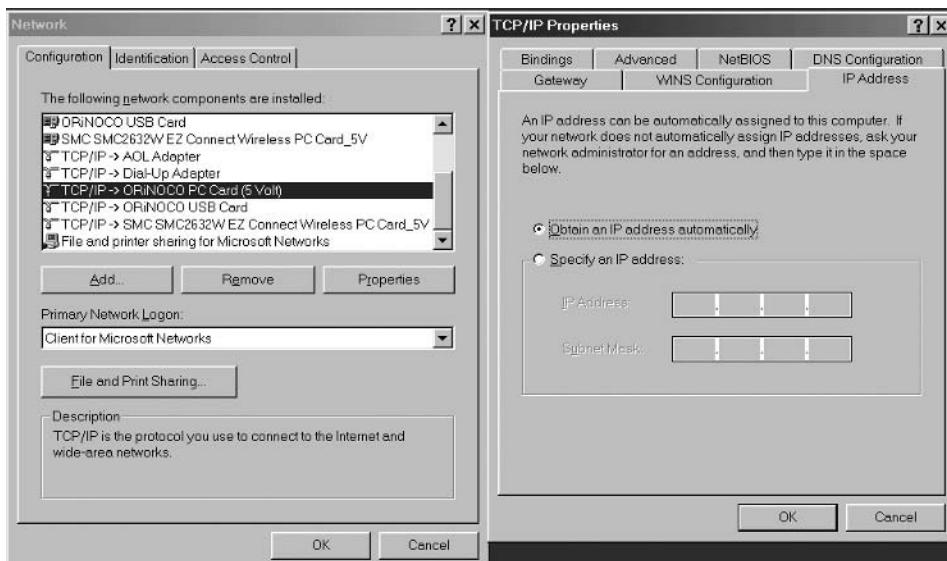


Figure 1.5 Configuring TCP/IP to obtain IP addresses from a wireless router that supports DHCP.

need to enter a specific station IP address, gateway address and DNS address as well as their associated subnet masks.

While it is possible for DHCP to be configured to use any block of IP addresses, in a wireless environment one of three blocks of special addresses reserved for private networks are commonly used. Under RFC 1918 the Internet Assigned Numbers Authority (IANA) reserved three blocks of IP addresses for use on private networks. Those address blocks represent Class A, B and C address as indicated below:

10.0.0.0 – 10.255.255.255
172.16.0.0 – 172.31.255.255
192.168.0.0 – 192.168.255.255

Although RFC 1918 addresses cannot be directly used on the Internet they facilitate the assignment of IP addresses on internal networks. Then, through the process of network address translation RFC 1918 addresses can be translated into a public IP address that can be used on the Internet.

1.2.5.2 Network Address Translation (NAT)

A second features that goes hand-in-hand with DHCP implemented on wireless routers is Network Address Translation (NAT). NAT was originally developed as a mechanism to economize upon the use of IP addresses, since it permits multiple hosts to share the use of a common IP address. A second function associated with ‘NAT’ which is mostly applicable to wired stations’ is that you obtain a degree of security as its use hides host IP addresses from view, preventing a direct attack on a station.

There are several methods by which NAT can be performed. One method results in the translation of host addresses behind a router into a block of addresses used by the router. This action results in a 1 to 1 address mapping which would enable up to 254 active sessions when a router supports a Class C block of addresses. Because multiple Class C or even a Class A or B network can reside behind the router performing NAT, it is possible that stations contending for the use of a public IP address may not obtain one. Instead, when all public IP addresses are in use stations behind the router performing NAT will have to wait for a previously in use address to become available for reuse.

A second and more popular method of NAT involves the translation of multiple addresses behind the router to a single IP address assigned to the router. The top portion of Figure 1.6 illustrates an example of NAT under which wireless and wired stations are shown assigned the Class C private use

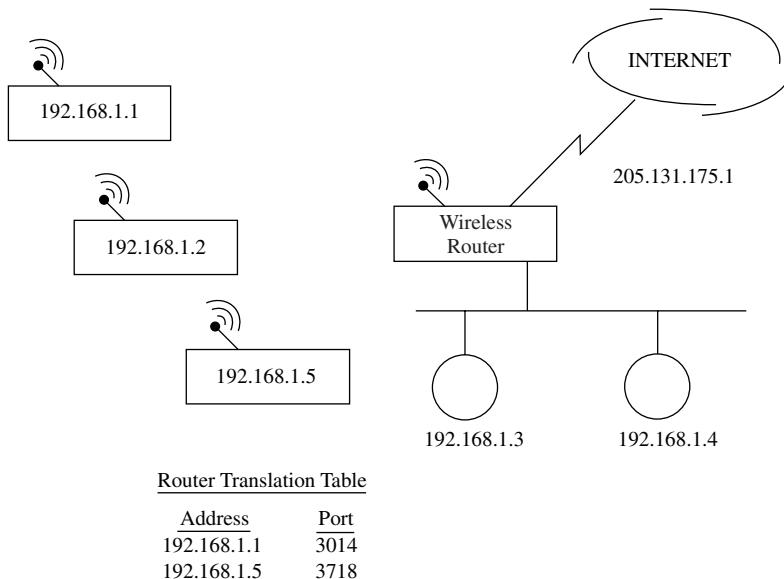


Figure 1.6 Network Address Translation enables several wired and wireless hosts to share a single IP address.

addresses of 192.168.1.1 through 192.168.1.5, while the router is assigned the IP address of 205.131.175.1. When the router receives a frame from a station it notes its private IP address and readdresses the frame, changing the source address to 205.131.175.1 while using a high source port number instead of a randomly selected number. The selected port number is placed into a table along with the private IP address and functions as a mechanism to identify the original private IP address.

In the lower portion of Figure 1.6 an example of the occurrence of two entries in the router translation table is shown. The first entry assumes that the station at IP address 192.168.1.1 went to surf the Web or perform another Internet related activity. When this occurred the router assigned that IP address to port 3014 and converted the private 192.168.1.1 address into the public IP address of 205.131.175.1, using the new port number to keep track of the translation. In the second example, the station whose assigned private IP address is 192.168.1.5 accesses the Internet resulting in the router translating that IP address to port 3718. For both stations the router uses the public address of 205.131.175.1; however, different port addresses are employed as a mechanism to direct responses to their appropriate destination. For example, when a frame flows to the router from the Internet the router examines the

destination port number against the table of private addresses and associated port numbers. The router then rewrites the frame using the private IP address associated with the destination port number.

In examining Figure 1.6 note that the wired and wireless stations that are configured with 192.168.1.0 network addresses have addresses that should never be used on the Internet. This results from the fact that RFC 1918 addresses are for private networks and their use as Internet addresses could result in multiple organizations having the same host addresses. This would obviously result in router confusion when attempting to deliver packets where multiple hosts and multiple networks have the same addresses.

By combining DHCP and NAT a wireless router allocates a block of RFC 1918 addresses to wireless and wired stations and then translates those addresses to a single IP address. That IP address is commonly the address assigned to an organization by their Internet Service Provider (ISP). Although NAT provides a degree of security, and allows an organization to connect multiple devices to the Internet through the use of a single IP address, it has several drawbacks. First, many multichannel applications, such as FTP, will not work or may not work correctly unless the NAT process was modified by the developer. Secondly, the NAT process consumes router resources, since frames must be ‘rewritten’ with new a IP destination address and port number. Thus, the translation process requires memory to hold frames and the contents of a state table as well as processing power, which is required to perform the translation of each frame.

1.2.5.3 Other Features

Figure 1.7 illustrates the SMC Networks Barricade wireless router. This router includes four 10/100 Ethernet ports, three of which represent Ethernet switch ports while the fourth supports a connection to a high speed communications device, such as a DSL or cable modem. The SMC Networks Barricade router supports both DHCP and NAT. In addition, this router includes a configurable firewall filtering capability, which enables an administrator to adjust the flow of packets that can be passed through the router. Other vendor products offer similar features, with some products including additional switch ports. Other products provide a content filtering capability that enables administrators to block access to either specific Web pages or Web pages based upon their content.

Another difference between wireless routers concerns the number of stations they can support. Some routers only support a small subset of RFC 1918 Class C addresses, while other routers place no restrictions on the number of IP



Figure 1.7 The SMC Networks Barricade wireless router includes three 10/100 Mbps switch ports and supports DHCP and NAT (photograph courtesy of SMC Networks).

addresses they can issue and, in fact, allow a selection of Class A, B or C addresses to be made.

Now that we have an appreciation for the basic devices used to construct a wireless LAN and extend its transmission distance, let's turn our attention to the primary focus of this section and examine how those devices are used to support different network architecture.

1.2.6 The Basic Service Set

The basic building block of an IEEE 802.11 wireless LAN is referred to as a Basic Service Set (BSS). A BSS can be viewed as an area of communications coverage that permits member stations to exchange information. There are

two types of BSS that correspond to the two transmission methods supported by wireless LANs – peer-to-peer and infrastructure.

1.2.6.1 Peer-to-Peer Networking

A group of two or more wireless stations that communicate with one another without the use of an access point form an Independent Basic Service Set (IBSS). Figure 1.8 illustrates an example of this network topology. Note that each station can communicate directly with another station without having to use the facilities of an access point. This type of networking that permits peers to communicate directly with one another is referred to as peer-to-peer networking.

1.2.6.2 Infrastructure Networking

The second type of network structure supported by IEEE 802.11 wireless LANs requires stations to communicate through the use of an access point. This type of network structure results in the use of an access point functioning as a relay device between wireless stations or wireless stations and a wired infrastructure. The use of an access point results in the network structure referred to as an infrastructure and the Basic Service Set being referred to as an Infrastructure Basic Service Set.

Figure 1.9 illustrates an example of an IBSS. Because the use of an access point results in wireless stations transmitting to the Access Point (AP) that

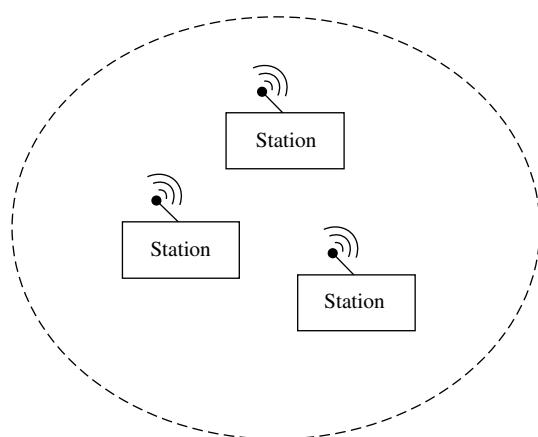


Figure 1.8 An Independent Basic Service Set. In an independent Basic Service Set stations communicate directly with one another.

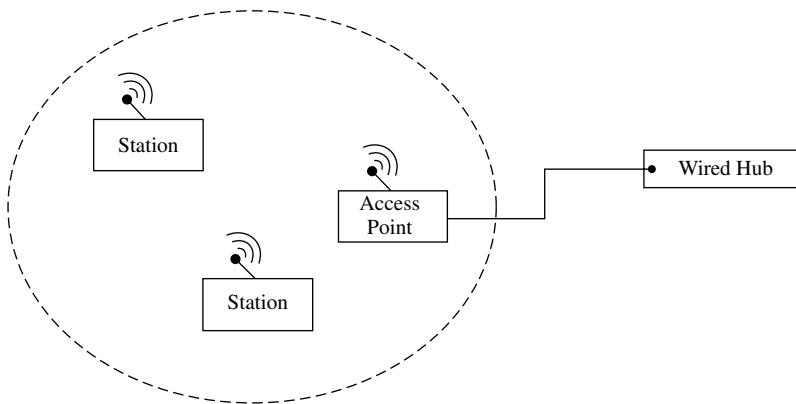


Figure 1.9 An Infrastructure Basic Service Set.

relays each frame, it is possible for an infrastructure BSS to have an area of coverage quadruple or four times the coverage of an independent BSS. This results from the fact that the relay function of the AP can double the transmission distance within an infrastructure BSS. Since the area of a circle is πr^2 where r is the radius, then doubling the radius results in the area of coverage increasing by a factor of four.

1.2.7 The Extended Service Set (ESS)

Because signals attenuate as they flow through the air the range of coverage of an Infrastructure Basic Service Set has a finite limit. To extend the area of coverage requires the installation of one or more additional access points, with each access point creating another Infrastructure Basic Service Set. The connection of two or more access points occurs through the use of a Distribution System (DS).

1.2.7.1 The Distribution System (DS)

The function of the DS is to interconnect access points and the stations in their respective Infrastructure Basic Service Sets. In addition, the DS permits frames to follow mobile stations as they move from one BSS to another.

The connection of two or more Infrastructure Basic Service Sets results in the formation of an Extended Service Set (ESS). Figure 1.10 illustrates the relationship between an ESS, two BSS' and a DS. In examining Figure 1.10 note that access points communicate with one another via the DS that can be considered to represent the backbone of the network. Although the DS

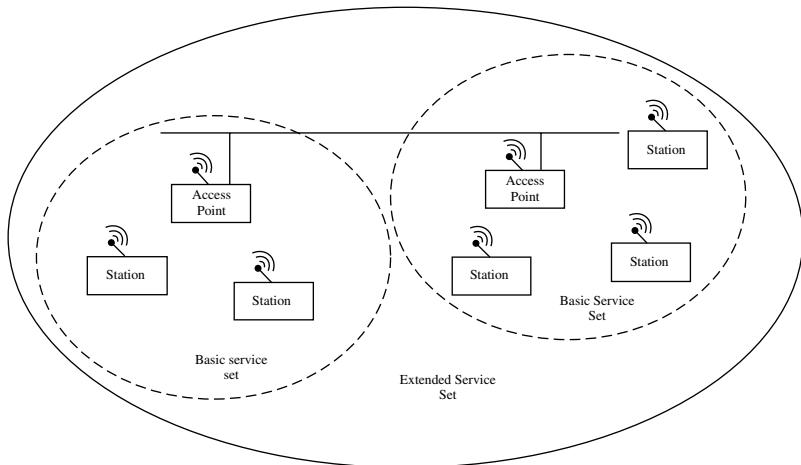


Figure 1.10 An Extended Service Set.

will normally be a wired LAN, the standard does not define a media for the DS. Thus, the DS could represent a wireless relay in the form of another access point.

Although each BSS shown in Figure 1.10 covers a different area, this does not have to be the case. BSS' can partially or fully overlap, with the latter used to provide redundancy. Under the IEEE 802.11 standard and its extensions, BSS' can overlap by operating on different frequency channels. To ensure stations communicate with the correct access point that functions as a hub within a BSS, a special identifier referred to as a Station Set ID (SSID) is employed to identify each access point. The SSID is also referred to as a Basic Service Set ID (BSSID) and is normally the MAC address of the access point. However, some wireless access points can be configured to set the SSID to different strings of characters. As we will note later in this book, the SSID represents a very poor password for providing stations access to a wireless infrastructure.

1.2.8 Station Services

Under the IEEE 802.11 standard several types of services are defined that provide both security and data delivery functionality. One of those services is authentication, which provides a mechanism to control access to a wireless LAN. Although authentication can rightfully be considered to represent a security mechanism, it also enables a station to access a particular access

point when two or more APs provide service within a given geographic area. Thus, authentication represents both a security and an access control feature.

A second station service can be viewed as a ‘tear-down’ of an existing connection. This type of service is referred to as deauthentication. Two additional station services are privacy, under which stations can be configured to support an optional Wired Equivalent Privacy (WEP) algorithm, and data unit delivery.

Under the IEEE 802.11 standard any station that requires the use of the wireless LAN to transport data must be authenticated prior to being able to transfer data. The 802.11 standard defines two types of authentication – open system and shared key.

1.2.8.1 Open System Authentication

Open system authentication represents the default authentication method supported by the IEEE 802.11 standard. Under this authentication method a station transmits an authentication request to an access point. The access point processes the request and determines whether or not to allow the station to proceed. Based upon the response received from the access point (success or failure), the station will either continue or terminate its access.

Under open system authentication, a station can authenticate with any other station or access point as long as the receiving station is configured to support this method of authentication and has resources available to communicate. Thus, open system authentication represents a null authentication method and requires the development of an application layer program to enhance its operation.

1.2.8.2 Shared Key Authentication

The second type of authentication supported by the IEEE 802.11 standard is shared key authentication. Under shared key authentication either a 40 bit or 104 bit key in the form of 10 or 26 hex characters is distributed to each station out-of-band. Here the term ‘out-of-band’ references the fact that the key is distributed to stations by a method other than wireless communications. The key is used both to enable security in the form of the WEP algorithm and to provide authentication. Once the applicable key is distributed to stations the access point generates a ‘random’ 128 bit text challenge. Each station encrypts a challenge using the previously configured shared key and responds to the access point. The access point will decrypt the challenged text using the same shared key and compare it to the challenged text it previously transmitted to the station. If a match occurs, the AP will respond indicating authentication was

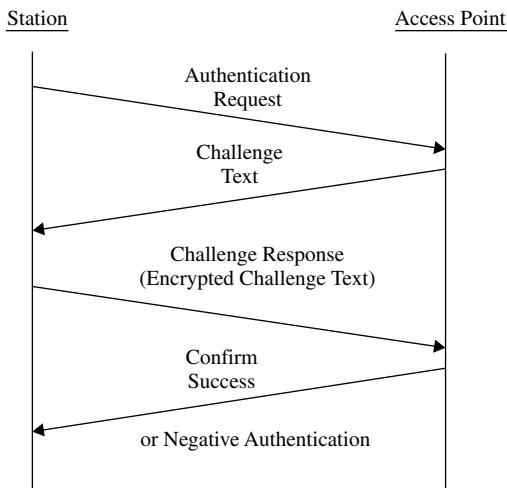


Figure 1.11 The shared key authentication process.

successful. If not, the access point will respond with a negative authentication. Figure 1.11 illustrates the shared key authentication process.

1.2.8.3 Deauthentication

Deauthentication represents a station service used to terminate an existing authentication. This service can be invoked by either authenticated party and represents a notification that cannot be refused.

1.2.8.4 Privacy

A third station service that warrants a brief discussion in this section is privacy. Under the IEEE 802.11 standard and its extensions privacy represents an optional station service in the form of the WEP algorithm. WEP is designed to provide a level of security equivalent to a wired LAN where data flows non-encrypted. Thus, it is important to note that WEP was never designed for providing secure communications similar to what we would expect when transmitting data via a VPN overlaid over the Internet. It is also important to know that as an option, WEP by default is normally disabled. This means that unless you configure your stations to support WEP and configure an applicable key for each station, all messages will be transmitted in the clear. In fact, many of the highly publicized trade journal and newspaper articles covering the insecurity of wireless LANs result from the fact that many network managers

and LAN administrators accept all default settings, which effectively results in their wireless network being naked.

1.2.8.5 Operation

IEEE wireless LANs operate using a modified form of Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), referred to as the Distributed Coordination Function (DCF). To obtain an appreciation of the manner by which DCF operates let's first briefly review Ethernet's Carrier Sense Multiple Access with Collision Detection (CSMA/CD) and how CSMA/CA differs from that access protocol.

CSMA/CD

CSMA/CD can be considered to represent a 'listen, then talk' protocol. Stations on a wired LAN listen to the medium to determine if a transmission is in progress. If no transmission is detected a station that has data to send can then transmit. Because two stations with data to transmit could listen to the medium at the same time and hearing no activity use the medium, this action would result in a collision. When a collision occurs each station responsible for the collision would wait a random amount of time prior to attempting to retransmit.

CSMA/CA

Under the CSMA/CA access protocol attempts are made to avoid collisions before they occur. To facilitate this, stations must wait a predefined amount of time after the medium becomes available prior to being able to transmit. This time is referred to as a slot time, which is measured in milliseconds. When a collision occurs, each station in a CSMA/CA network must wait a random amount of time after the medium is clear prior to attempting to send the data again.

DCF

Under the IEEE 802.11 standard the Distributed Coordination Function (DCF) access method defines three types of time gaps that must occur between different types of frames. In addition, DCF also reduces the potential effect of collisions by employing an explicit acknowledgement (ACK) frame. A receiving station transmits an ACK to the sending station as a confirmation of the correct arrival of a data frame. If the ACK frame is not received by the sending station, it will assume that a problem occurred and retransmit the frame after waiting a random amount of time.

1.2.8.6 Interframe Spaces

Under the IEEE 802.11 standard there are three different time gaps that are referred to as interframe spaces (IFS). The value or duration of the IFS is based upon the transmission method.

The shortest time gap is known as the Short IFS (SIFS), which is used as a delay interval when an immediate response action occurs, such as a receiving station transmitting an ACK. A second time gap interval is the Point Coordination Function IFS (PIFS). The PIFS represents the time delay of a station accessing a medium after it has been polled and approved to transmit. The Point Coordination Function represents a polling method of station access that although defined by the standard, has yet to be incorporated into vendor products.

The third time delay is the Distributed Coordination Function IFS (DIFS). DIFS represents the standard delay interval between the transmission of data frames. Table 1.1 lists the interframe space values for the three time gaps for the three transmission methods supported by IEEE wireless LANs.

1.2.8.7 Timing Relationship

To illustrate the relationship of the interframe spaces, let's assume Station A transmits two frames to station B using Direct Sequence Spread Spectrum (DSSS). Station A will first listen to the medium (carrier sensing) prior to being able to transmit. The station must wait the DIFS gap interval or 50 milliseconds prior to transmitting. Assuming station B receives the transmission, it returns an ACK in the SIFS delay gap that informs station A that the transmission was successful. After receiving the ACK, station A waits the DIFS interval after which it waits an additional backoff period of time, represented by a random number of time slots multiplied by 20 microseconds, and listens for activity. If no activity is detected Station A transmits a second frame and station B responds during the second SIFS gap. Figure 1.12 illustrates the timing relationship as Station A transmits to Station B and Station B acknowledges their receipt.

TABLE 1.1 Interframe space duration in milliseconds

Interframe Space	DSSS	FHSS	Infrared
SIFS	10	28	7
PIFS	30	78	15
DIFS	50	128	23

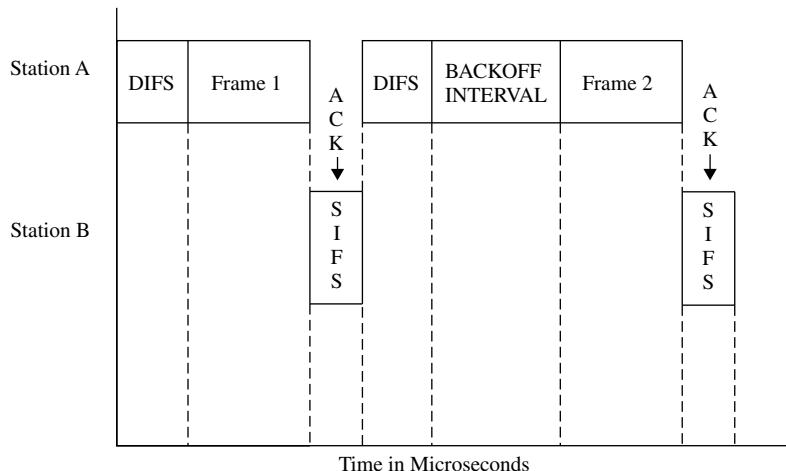


Figure 1.12 Transmission and interframe spacing relationships.

1.2.8.8 Virtual Carrier Sensing

One interesting standard that can minimize certain types of collisions is Virtual Carrier Sensing (VCS). Under VCS two special types of frames are used to alleviate collisions resulting from what is referred to as the hidden node problem.

Hidden node problem

An example of the hidden node problem is shown in Figure 1.13 in which Station A, which is hidden by an obstruction from Station B, is transmitting to Station C. If Station B has data to transmit it would not hear the transmission from Station A due to the obstruction. Thus, when Station C transmits a collision at Station B will occur.

The solution to this hidden node problem is obtained through the use of Request To Send (RTS) and Clear To Send (CTS) frames. Using the VCS option a station with a data frame to transmit would first transmit a RTS frame. That frame includes a duration field that indicates the time required to transmit the data frame and receive an ACK. The destination station and other stations that can receive the RTS signal are alerted that the station issuing the RTS needs to reserve the medium for the specified period of time, storing this information in an area referred to as a Net Allocation Vector (NAV). The receiving station will respond to the RTS with a CTS frame. The CTS frame alerts all stations that the medium is reserved and they should suspend transmission for the

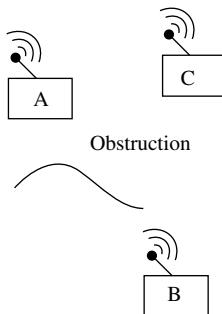


Figure 1.13 The hidden node problem occurs when one station cannot hear the transmission of another station.

duration in their NAV. The originating station that issued the RTS can then proceed and transmit its data frame.

Although the use of RTS/CTS frames eliminates hidden node collisions it adds a considerable amount of overhead that can degrade network performance. This is why by default the use of RTS/CTS frames is disabled. When enabled, short data frames will be transmitted without the use of RTS/CTS frames as a mechanism to minimize overhead. Frames longer than the RTS threshold are transmitted using the RTS/CTS frame sequence, with shorter frames directly transmitted.

RTS and CTS frames as well as the previously mentioned ACK frame represent control frames. Under the IEEE 802.11 standard three types of frames are presently defined. Those frame types are control, management and data which we will focus upon in the next chapter of this book. However, before doing so we will conclude this chapter with a brief overview of IEEE wireless LAN standards and a preview of succeeding chapters. This preview can be used as is or in conjunction with the table of contents and index to locate information of immediate interest.

1.3 IEEE wireless LAN standards

In concluding our overview of wireless LANs we will turn our attention to the literal family of IEEE wireless LAN standards. Those standards were developed under the IEEE 802.11 umbrella and define the operation of wireless LANs. The selection of the IEEE for defining wireless LAN standards dates to the selection of that organization by the American National Standards Institute (ANSI) to develop LAN standards. Thus, as the delegated developer

of LAN standards it was quite natural for the IEEE to develop wireless LAN standards.

1.3.1 The basic IEEE 802.11 standard

The initial effort of the IEEE in developing wireless LAN standards resulted in the 802.11 specification. Dating from 1999, this standard can be considered to represent the foundation of IEEE wireless LAN standards.

1.3.1.1 Physical Layers

The IEEE 802.11 standard defined three physical layers that could transport the frames defined for MAC operations. Physical layer operations included two Radio Frequency (RF) methods that were originally developed for military operations to overcome enemy jamming of RF communications. Those two physical layer methods are FHSS and DSSS.

Frequency hopping spread spectrum

Under FHSS a pseudo-random sequence is used to switch frequencies, enabling a station to literally hop from one frequency to another. Of course, each wireless LAN device operating in this manner switches frequency using the same algorithm. Although the use of FHSS in wireless LANs should not encounter jamming, communications can encounter interference from other devices operating in the 2.4 GHz frequency band. Because a wireless LAN station using FHSS only spends a short time (referred to as dwell time) on each frequency prior to hopping to the next, this technique minimizes the effect of communications interference.

Direct sequence spread spectrum

DSSS represents another broadband RF communications method originally developed to overcome jamming in a military communications environment. Under DSSS a spreading code is used to spread each data bit into a sequence of multiple bits that are modulated for transmission over a broad range of frequencies. At the receiver the same spreading code is used to ‘de-spread’ the received bits to determine the data bit transmitted. Under the IEEE 802.11 standard an 11 bit spreading code is used. However, for illustrative purposes we will examine the use of a 5 bit spreading code.

To illustrate the operation of DSSS assume the 5 bit spreading code ‘10110’ is used and the data bit is a binary 1. The data bit is modulo 2 added to the bits in the spreading code, resulting in the bit sequence:

Spreading code	10110
Databit	11111
Data to be modulated	01001

Thus, the bit sequence 01001 is modulated.

At the receiver the received demodulated spread sequence is modulo 2 added bit by bit to the same spreading code as shown below:

Received bits	01001
Spreading code	10110
Resulting data bit	11111

In this example the five resulting data bits are all set to a binary 1, resulting in the ‘de-spread’ data bit assumed to have a value of binary 1. If a transmission error should occur a ‘majority rules’ rule is applied. That is, the value of each resulting bit is examined and the setting in the majority is used. Thus, if the resulting bits were ‘11011’ or ‘01101’ or ‘10111,’ because more bits were set to 1 than a value of zero, the ‘de-spread’ bit value would be assumed to be 1.

Infrared

The third physical layer supported by the IEEE 802.11 standard is diffused infrared (IR). Unlike FHSS and DSSS that are based upon RF communications, IR occurs near visible light and is not regulated by the Federal Communications Commission or other governmental agencies. The IEEE 802.11 standard supports data rates of 1 Mbps and 2 Mbps for all three physical layers. Although equipment was manufactured that supports both RF physical layers, to the best knowledge of this author no equipment has been manufactured to support the IEEE IR standard.

1.3.1.2 WEP

Included in the IEEE 802.11 standard is a feature designed to provide wireless LANs with an equivalent level of privacy commensurate with non-encrypted data flowing over a wired LAN infrastructure. Referred to as Wired Equivalent Privacy (WEP), a secret key must be configured on each station that is used to generate a pseudo-random number sequence. That sequence is then used to encrypt and decrypt data.

There are two versions of WEP, referred to as WEP and WEP 2.0. The original version of WEP uses a 40 bit (10 hex character) secret key. A 24 bit

Initialization Vector (IV) is added as a mechanism to seed the random number generator, with the IV transmitted in the clear. Under WEP 2.0 a 104 bit (26 hex digit) secret key is used with the same 24 bit IV.

Shortly after the 802.11 standard was issued doubts began to arise over the security of WEP. During 2000 and 2001 several papers were published that denoted weaknesses in the use of an in-the-clear IV as well as the RC4 algorithm used to perform encryption. As a result of those weaknesses vendors introduced a series of proprietary methods to overcome the deficiencies of WEP while the IEEE began work on an extension to the standard to enhance wireless LAN security, topics that will be covered in considerable detail throughout this book. Now that we have a basic appreciation for the 802.11 standard, let's turn our attention to its extensions.

1.3.2 802.11b

The 802.11b extension was one of two extensions to the 802.11 standard that was published shortly after the basic standard, the other being the 802.11a extension. Because the 802.11b extension operates in the same frequency band as the basic standard, we will discuss it prior to the 802.11a extension.

The 802.11b extension specifies the use of DSSS at 1, 2, 5.5 and 11 Mbps. 802.11b products currently are in volume production and the installed base of such products considerably exceeds 802.11a equipment.

1.3.3 802.11a

The 802.11a extension to the 802.11 standard uses a frequency division multiplexing scheme referred to as Orthogonal Frequency Division Multiplexing (OFDM). A second difference is the fact that this extension defines a physical layer standard for wireless LANs operating at data rates up to 54 Mbps. Remembering physics and the fact that high frequencies attenuate more rapidly than low frequencies explains one of the problems associated with the use of 802.11a compatible equipment. That is because the transmission range is less than 802.11b equipment, the former requires more access points to serve a given area than when 802.11b equipment is used.

1.3.4 802.11c

This extension to the 802.11 standard is focused upon MAC bridges for wireless LANs. The task group completed its effort several years ago and its work was merged into the IEEE 802.1d standard.

1.3.5 802.11d

The 802.11d extension to the 802.11 standard represents a supplement to the MAC layer. This supplement is designed to support the worldwide use of 802.11 wireless LANs as it enables access points to communicate at different power levels commensurate with the regulations of other countries.

1.3.6 802.11e

The 802.11e extension to the IEEE 802.11 standard represents another supplement to the 802.11 MAC layer. This supplement is designed to provide a Quality of Service (QoS) support for wireless LANs using a method referred to as a Hybrid Coordination Function (HCF). The 802.11e supplement will apply to the 802.11 a, b and g extensions enabling classes of service to be provided for voice, data and video applications.

1.3.7 802.11f

The goal of the 802.11f extension to the 802.11 standard is to provide access point interoperability. Currently, when a user roams between access points manufactured by different vendors due to the differences in handoff between vendor products, it is possible to lose packets. Under the 802.11f extension multi-vendor interoperability will occur through the support of the Inter-Access Point Protocol (IAPP).

1.3.8 802.11g

The goal of the 802.11g extension to the 802.11 standard can be considered as a high speed extension to 802.11b. Equipment that supports the 802.11 g extension will operate in the 2.4 GHz frequency band using OFDM to obtain data rates up to 54 Mbps as well as being backward compatible with 802.11b equipment.

1.3.9 802.11h

The 802.11h extension to the 802.11 standard addresses interference problems in Europe, where the 5 GHz frequency band used by the 802.11a extension is shared with radar and satellite communications. The 802.11h extension adds a feature called Dynamic Frequency Selection (DFS) and another feature called Transmit Power Control (TPC). DFS enables an 802.11a device to detect communications interference and switch to the use of an alternative communications channel. Through the use of TPC a client close to an 802.11a

access point will automatically reduce its transmission power, resulting in less potential interference to other devices communicating in the 5 GHz frequency band.

1.3.10 802.11i

Recognizing the limitations of WEP resulted in the development of the 802.11i extension to the 802.11 standard. This supplement to the MAC layer is being developed to enhance wireless LAN security and will apply to 802.11 physical standards defined by the a, b and g extensions.

The 802.11i supplement defines two new encryption methods as well as an authentication method. This authentication method uses port-based authentication defined by a prior IEEE standard (802.1x) which was in turn based upon an Internet RFC. The two encryption methods designed to replace WEP include the Temporal Key Integrity Protocol (TKIP) and the Advanced Encryption System (AES). TKIP represents an interim solution that should be accomplished by firmware upgrades to existing products. In comparison, the use of AES will more than likely be accomplished through new silicon containing an AES cipher.

1.4 Book preview

In this section we will briefly tour the remainder of this book on a chapter by chapter basis. Although this book was written with a view towards presenting information in a logical manner, it was also written to make chapters as independent as possible from one another. This modular independence permits readers to turn to a specific chapter for information of immediate interest, although this author recommends that this book be read in chapter order sequence to obtain maximum benefit from the information presented. That said, let's begin our tour of the material to be presented in succeeding chapters.

1.4.1 Frame formats and basic security operations

In Chapter 2 we will probe deeper into IEEE 802.11 wireless LAN operations. We will first focus upon the three types of frames supported by the standard and the fields within different types of frames. As we examine the fields within the data frame we will note why the standard is restricted to supporting only one type of encryption which some people consider to represent a design flaw. In the second section we will turn our attention to basic security operations. In

this section we will discuss and illustrate the role of the Service Set ID (SSID) as a password and obtain an overview of how WEP operates and is enabled.

1.4.2 Understanding wireless signals

In the third chapter we will turn our attention to wireless signals as the transmission of data over the air makes it subject to various types of security related problems. We will briefly examine the wireless radio frequency spectrum to include the two bands used by IEEE 802.11 wireless LANs. Once this is accomplished we will note the use of various types of signal strength indicators and examine antenna sensitivity. This information will form a foundation for understanding one of the key tenets associated with the security of wireless LANs – that is, if a third party cannot hear your transmission they cannot intercept nor alter information. In concluding this chapter we will discuss the placement of access points, wireless stations and shielding as a mechanism to enhance signal security.

1.4.3 Understanding WEP

Because over-the-air transmission can be intercepted, the designers of the IEEE 802.11 standard incorporated a privacy mechanism that was designed to provide wireless LANs with a level of privacy equivalent to the flow of data on a wired network. That privacy mechanism is formally referred to as WEP. In Chapter 4 we will examine WEP in detail and look at why it is vulnerable.

1.4.4 Security risks

Building upon the first four chapters in this book, Chapter 5 will focus upon various types of threats that can adversely effect wireless LANs. We will note threats to wireless LANs that can originate both via the air and through a wired connection from an access point to another network or the Internet. Some of the threats we will examine include monitoring, insertion attacks, masquerading, file sharing, different types of encryption attacks, jamming and even how the theft of hardware can adversely effect your network.

1.4.5 Proprietary security enhancement techniques

Once we have an understanding of how wireless LANs operate and their vulnerabilities, it is time to consider how we can overcome those vulnerabilities. In Chapter 6 we will focus upon a series of proprietary security enhancement techniques implemented by different vendors in recognition of the limitations

of WEP. We will look at hardware and software solutions from several vendors and how those solutions can be employed to secure your wireless LAN.

1.4.6 Standards based security

In the concluding chapter we will examine both recently released standards as well as some older ones that can be used to enhance the security of wireless LANs. Concerning the former, we will primarily focus upon the IEEE 802.1x standard which is now supported in the Windows XP operating system. Concerning the latter, we will examine several standards based alternatives to the use of WEP, such as the creation of a VPN that operates at layer 3 of the International Standards Organization (ISO) Open System Interconnection (OSI) Reference Model as well as the use of IPSec and other standardized layer 3 techniques.

chapter two

Frame Formats and Basic Security Operation

The purpose of this chapter is twofold. In the first section we will become acquainted with the manner in which IEEE 802.11 wireless LANs include their ‘a’ and ‘b’ extensions transport data. In doing so we will focus upon the different types of frames used by wireless LANs to include the functions of different frame fields. By obtaining an understanding of the manner in which data, management and control information is transported, we will be able to better understand threats to wireless LANs and methods that can be used to enhance security. In the second section we will look at basic wireless LAN security operations. In this section we will examine the manner in which Wired Equivalent Privacy (WEP) functions. As we examine basic wireless LAN security we will also note several limitations of WEP which can provide a false sense of security.

2.1 Frame formats

Like wired LANs, wireless LANs transport information in protocol data units referred to as frames. IEEE 802.11 wireless LANs operate at the second layer in the OSI Reference Model, the data link layer, with each frame containing a header, a variable length body, and a trailer in the form of a 32 bit cyclic redundancy code contained in a Frame Check Sequence (FCS) field. In this section we will first look at the format of the basic wireless LAN frame and the composition and use of the fields in that frame.

2.1.1 Basic frame format

The IEEE 802.11 wireless LAN frame format is illustrated at the top of Figure 2.1. The first seven fields are considered to represent the Media Access Control (MAC) header. As we note later in this section when examining different types of frames used by wireless LANs, not all of the fields in the header shown in Figure 2.1 are required in certain types of frames. In addition, several types of frames do not transport information and therefore do not include a frame body. The lower portion of Figure 2.1 illustrates the subfields contained within the two byte frame control field. Thus, in beginning our examination of the format and composition of the wireless LAN frame we look at the two byte frame control field and its subfields.

2.1.2 Frame control field

Every IEEE 802.11 wireless LAN frame includes a 16 bit frame control field. As its name implies, the purpose of this field is to convey control information between stations. This field, shown in the lower portion of Figure 2.1, has 11 subfields whose use we will now examine.

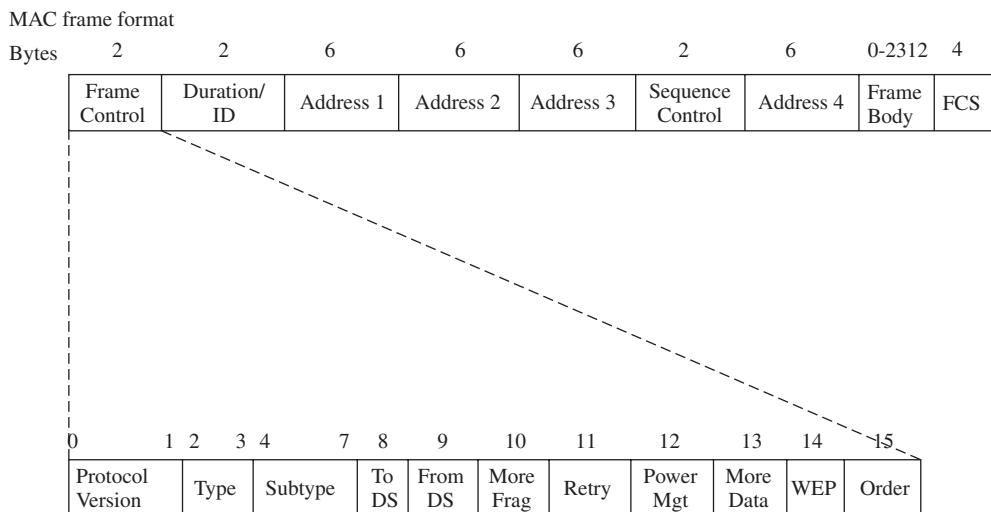


Figure 2.1 The basic format of IEEE 802.11 wireless LAN frames.

2.1.2.1 Protocol Version Subfield

The Protocol Version subfield is 2 bits in length, permitting up to four versions of the protocol to be identified. The IEEE 802.11 standard commenced using a protocol version of 0, with the other values reserved for future use.

2.1.2.2 Type and Subtype Subfields

The Type and Subtype subfields are 2 and 4 bits in length, respectively. The value of the type frame identifies the basic type or category of a frame, while the value of the Subtype field identifies the function of the specified type of frame. Table 2.1 defines the relationship between Type and Subtype fields and the type of frame and its function.

In examining the entries in Table 2.1 we note that presently there are three basic types of frames (management, control, data) defined, with the type field value of 11 reserved for future use. If you focus upon the column labeled 'Function' in Table 2.1, you will observe how the Type and Subtype field values are used to define different functions, such as authentication that was briefly described in Chapter 1, in addition to beaconing and other functions that will be described later in this section.

2.1.2.3 To^DS Subfield

The To^DS subfield is 1 bit in length. The function of this field is to indicate if a data type frame is destined for a Distribution System (DS). As a reminder from Chapter 1, the DS represents a backbone that interconnects access points. That backbone can be formed through the use of a wired or even another wireless infrastructure. The function of this field is to inform an access point that the frame needs to be forwarded onto the DS. When set to 1, this indicates that a data type frame is destined for the DS. The To^DS field is set to a value of 0 in all other frames.

2.1.2.4 From^DS subfield

The function of the From^DS subfield is to indicate that a data type frame has exited from a DS. This 1 bit subfield is set to 1 when a data type frame exits a DS, it is set to 0 in all other frames.

The To^DS and From^DS fields are each 1 bit in length. Together, they provide four combinations that are identified in Table 2.2.

TABLE 2.1 Relationship of Type and Subtype fields and the type of frame and its functionality

Type Value	Type of Frame	Subtype Value	Function
00	Management	0000	Association Request
00	Management	0001	Association Response
00	Management	0010	Reassociation Request
00	Management	0011	Reassociation Response
00	Management	0100	Probe Request
00	Management	0101	Probe Response
00	Management	0110–0111	Reserved
00	Management	1000	Beacon
00	Management	1001	Announcement
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101–1111	Reserved
01	Control	0000–1001	Reserved
01	Control	1010	Power Save (PS)-Poll
01	Control	1011	Request to Send (RTS)
01	Control	1100	Clear to Send (CTS)
01	Control	1101	Acknowledgement (ACK)
01	Control	1110	Contention Free (CF)-End
01	Control	1111	CF-End+CF-ACK
10	Data	0000	Data
10	Data	0001	Data+CF-ACK
10	Data	0010	Data+CF-Poll
10	Data	0011	Data+CF-ACK+CF-Poll
10	Data	0100	Null Function (No Data)
10	Data	0101	CF-ACK (No Data)
10	Data	0110	CF-Poll (No Data)
10	Data	0111	CF-ACK+CF-Poll (No Data)
10	Data	1000–1111	Reserved
11	Reserved	0000–1111	Reserved

TABLE 2.2 To/From DS values for data type frames

To DS	From DS	Meaning
0	0	Data frame flows from one station to another within the same IBSS.
1	0	Data frame destined for DS.
0	1	Data frame exiting DS.
1	1	Wireless DS frame being distributed from one AP to another.

In examining the entries in Table 2.2 we note that the settings of the To^DS and From^DS 1 bit subfields in the control field indicate how a frame flows in a wireless LAN. That is, when both subfields are not set, the frame is flowing within the same IBSS and does not flow to or from a DS. When both subfields are set, the frame is flowing via a DS from one Access Point (AP) to another AP, while the setting of one of the two subfields indicates if the frame is flowing from the DS or towards the DS. Because frames can flow to or from access points that do not represent their actual source or destination, a mechanism is required to differentiate between the address of an access point and the source and destination addresses contained in a frame. That mechanism, as we will shortly note, is accomplished by the use of four MAC addresses in the data frame.

2.1.2.5 More Fragments Subfield

Continuing our tour of the subfields within the Control field, the More Fragments field represents another 1 bit field. This subfield is set to 1 in all data or management frames to indicate another fragment of the frame follows. Figure 2.2 illustrates an example of the use of the More Fragments subfield. In this example, a frame is shown fragmented into four sections. The first three fragments have the More Fragments subfield set to a value of 1, while its value is set to 0 in the last fragment. Thus, the value of this field notes if an additional fragment follows or if the last fragment of the frame was reached.

2.1.2.6 Retry Subfield

The Retry subfield is also 1 bit in length. When set to 1 this field indicates that the frame represents a retransmission and permits a receiving station to ignore duplicate frames.

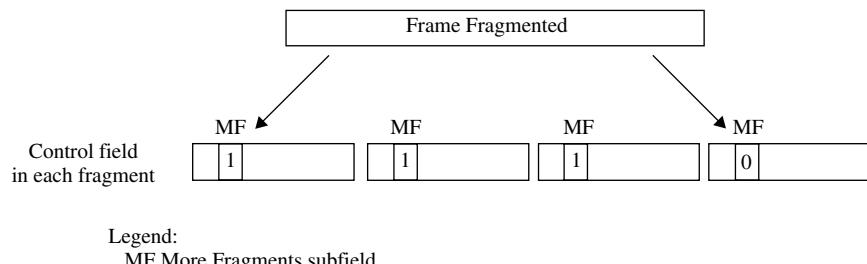


Figure 2.2 The More Fragments subfield indicates an additional fragment follows or the last fragment on the frame.

2.1.2.7 Power Management Subfield

Under the IEEE 802.11 standard, stations can either be in an active mode or a power save mode. This 1 bit field is used to indicate the power management mode of a station. A value of 1 indicates that a station is in a power save mode while a value of 0 indicates that the station is in an active mode. When a frame is transmitted by an access point this field is always set to a value of 0. Power management is only applicable when stations are operating in an infrastructure mode. As we will note when we discuss the use of the More Data subfield when, in the power save mode, an access point will temporarily store frames destined for a station that is ‘sleeping’ by buffering such frames. At predefined time intervals an access point will transmit a beacon to all stations. The beacon frame includes a list known as a Traffic Indication Map (TIM) of all stations that have buffered frames at the access point that are awaiting delivery. Through the use of an interval timer, each station literally wakes up to listen to a beacon frame. When a beacon occurs, stations in the sleep mode will switch to an active listening mode and examine the contents of the beacon frame. If the station determines that there are buffered frames awaiting delivery it will transmit a request to the access point. Otherwise, the station will return to its sleep or low power mode of the operation.

2.1.2.8 More Data Subfield

The More Data subfield works in conjunction with the Power management subfield. When a station informs an access point that it is in a power save mode the AP will buffer frames for delivery to the station. When the More Data field is set to a value of 1 this indicates that at least 1 additional frame remains to be transmitted by the AP.

2.1.2.9 WEP Subfield

The WEP subfield is 1 bit in length. When set to a value of 1 this field indicates that the frame body is encrypted. The WEP subfield can only be set to 1 for data type frames and management frames that have an authentication subtype value. Because the length of the WEP subfield is 1 bit, it is only possible to support one encryption method within an IBSS. This means that all stations within the IBSS must either not use WEP encryption or be configured to support the same method of encryption. Because both 64 bit and 128 bit keys can be used, when WEP is enabled all stations must be configured in the same manner. This also means that an organization with a mixture of wireless

Network Interface Cards (NICs), some of which only support 64 bit keys, must use the lowest common denominator even if most NICs support 128 bit keys.

2.1.2.10 Order Subfield

The Order subfield represents the last subfield in the Control field. This 1 bit field is set to 1 in any data type frame that is being transmitted using the Strictly Ordered service class. This action prevents a change in the delivery order of frames.

2.1.2.11 Duration/ID Field

The Duration/ID field is 16 bits in length. When included in a Power Save (PS)-Poll frame this field conveys the identity of the station that transmitted the frame. In all other frames this field contains a duration value in microseconds that is used in Request To Send, Clear To Send and Acknowledgement frames. The value contained in this field indicates the number of microseconds a station requires to transmit either a data frame, a control frame, or a management frame. Later on in this section we will discuss the use of the duration field in several control frames.

2.1.2.12 Address Fields

As indicated in Figure 2.1, there are four address fields in the basic IEEE 802.11 wireless frame. The four addresses all represent 48 bit MAC addresses. The first address field conveys the destination address which indicates the final recipient of the frame. The second address field represents the source address of the station that initiated the frame. The third address is the receiver address, which identifies the intended immediate recipient of the frame, while the fourth address is the transmitter address which identifies the station that transmitted the frame. It is important to note that unlike a wired LAN which only has destination and source addresses, the four addresses in the basic wireless frame permits a distinction to be made between a station that originates a frame and one that transmits it over the air, as well as a station that will be the ultimate recipient of a frame and a station that is to receive the frame over the wireless medium. It should also be noted that several types of frames only require two addresses – receiver and transmitter. Such frames control the flow of information over the wireless medium and therefore only flow between wireless stations. When we examine control and management frames we will note they only use two address fields.

2.1.2.13 Sequence Control Field

The Sequence Control field is 16 bits in length. This field consists of two subfields – a 4 bit Fragment Number and a 12 bit Sequence Number as illustrated in Figure 2.3. The 4 bit fragment number permits a maximum of 16 fragments. The 16 bit Sequence Number field uses numbers that are assigned from a modulo 4096 counter, commencing at 0 and incrementing by 1. The More Fragments subfield in the Control field is used in conjunction with The Sequence Control field. That is, the More Fragments subfield is set to a value of 1 to indicate more fragments follow whereas when set to a value of 0 this field indicates that the current fragment is the last.

2.1.2.14 Frame Body Field

If you examine Figure 2.1 you will note that the frame body can vary from 0 to 2312 bytes in length. The minimum length of 0 means that there is no frame body. The maximum length results from the need of the frame body to accommodate a data unit expansion when encryption occurs. That expansion includes a 32 bit Initialization Vector (IV) of which, as we will note later in this chapter, only 24 bits are used to seed encryption.

2.1.2.15 FCS Field

The last field in each IEEE 802.11 frame is the Frame Check Sequence (FCS) field. This field contains a 32 bit Cyclic Redundancy Check (CRC) computed using the following polynomial:

$$G(x) = x^{32} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

As a refresher for readers not familiar with CRCs, the data is considered to represent a long binary number, which is divided by the polynomial $G(x)$. The $G(x)$ value is equivalent to the binary number:

1000000001100000100011101101101

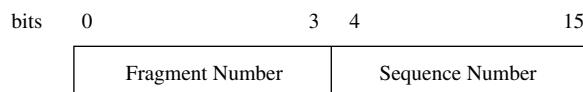


Figure 2.3 The Sequence Control field.

As a result of the division process the quotient is discarded and the remainder is used as the CRC.

2.1.3 Control frames

As previously indicated in Table 2.1, there are three types of 802.11 frames presently defined. Those frame types are data, control and management. In this section we will focus upon several control frames and become acquainted with the hidden node problem and the manner in which the use of certain control frames alleviates this problem.

There are six control frames defined under the IEEE 802.11 standard. Those control frames include two that are used to minimize the affect of a hidden node. First let us examine the hidden node problem and then review the format and function of certain control frames defined by the standard.

2.1.3.1 Hidden Node Problem

A common problem associated with wireless LANs are collisions caused by an obstruction that hides the transmission of one node from another. When this situation arises the transmission from the hidden node is not heard by another station, which assumes it can transmit. Unfortunately, this action can result in a collision occurring at a receiver that can hear both transmissions. A second cause of the hidden node problem can be the distance between stations. In an infrastructure network environment it is possible to locate stations so that they can all communicate with an access point, but one or more stations are beyond the range of other stations as illustrated in Figure 2.4. When this situation arises it is possible that one station may not be able to hear the transmission of another station and then transmit, resulting in a collision at a receiver. In Figure 2.4 it can be seen that station A's transmission cannot be heard by station B nor by station C. However, if either station B or station C has data to transmit while station A is communicating with the access point, they will not hear the transmission. Thinking the medium is available they will proceed and transmit data, resulting in the occurrence of a collision.

As a mechanism to alleviate the hidden node problem, the IEEE 802.11 standard includes an option referred to as Virtual Carrier Sensing (VCS). VCS uses two special types of control frames to solve the hidden node problem. Those frames are the Request To Send (RTS) and Clear To Send (CTS) frames. To understand how this option alleviates the hidden node problem let's look at the composition and utilization of each of these control frames.

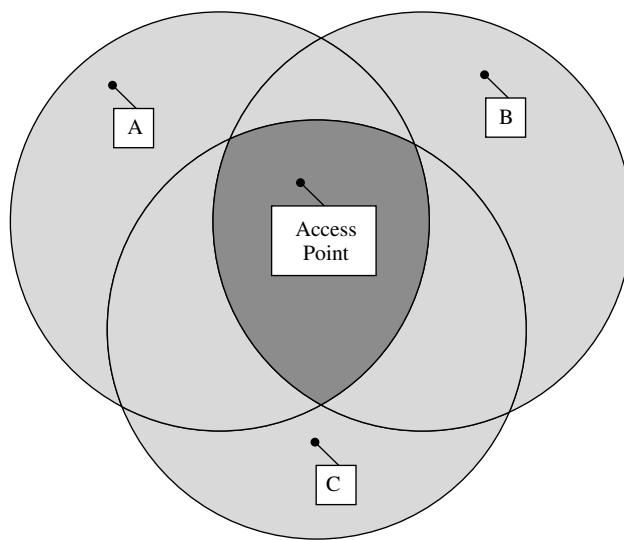


Figure 2.4 The hidden node problem can result from the distance between stations.

2.1.3.2 RTS Frame

The top portion of Figure 2.5 illustrates the format of the RTS frame. A station that has data to transmit which is configured to support the RTS/CTS option will transmit an RTS frame during the Short Interframe Space (SIFS) time gap. The station will enter a value in the duration field in the RTS frame which denotes the length of time required to transmit its actual data frame and receive a responding ACK (acknowledgement) frame.

Request to Send

Bytes:	2	2	6	6	4
	Frame Control	Duration	Receiver Address	Transmitter Address	FCS

Clear to Send

Frame Control	Duration	Receiver Address	Transmitter Address	FCS
---------------	----------	------------------	---------------------	-----

Figure 2.5 RTS and CTS frame formats.

When a station transmits an RTS frame, all stations that hear the frame are alerted to the fact that the transmitting station needs to reserve the medium for the specified period of time. Those stations then store the duration into their Net Allocation Vector (NAV), which functions as a buffer for a timer that precludes a station from transmitting whenever the NAV has a value greater than zero. The destination station will respond to the RTS with a CTS frame, so let's turn our attention to that.

2.1.3.3 CTS Frame

The lower portion of Figure 2.5 illustrates the format of the CTS frame. The receiver address of the CTS frame is copied from the transmitter address of the prior RTS frame, with the duration field value representing the value of the RTS Duration field less the time required to transmit the CTS frame and some internal overhead.

Although the RTS frame caused stations to store the duration value in their NAV, those stations do not use the stored value until the receiver issues a CTS frame in response to the RTS frame. When stations hear the CTS frame, this tells them to suspend transmission for the duration defined by the RTS frame, enabling the originating station to transmit its data.

2.1.3.4 ACK Frame

The ACK frame represents a third commonly used 802.11 control frame. Figure 2.6 illustrates the format of the ACK frame.

The ACK frame is similar to the CTS frames which have values based on previously received frames. For example, the Receiver Address of the ACK frame is copied from the Address 2 field of the previously received frame that the ACK acknowledges. Under the modified CSMA/CA access control method used by IEEE 802.11 wireless LANs, a receiving station transmits an ACK frame to the transmitting station as a mechanism to confirm the arrival of a data frame. However, instead of sending a negative acknowledgement (NAK) frame, timing is used to indicate a transmission problem. That is, instead of transmitting a NAK the receiving station does nothing. The absence of an ACK is used to indicate that the transmitted frame was either received in error

Frame Control	Duration	Receiver	FCS
---------------	----------	----------	-----

Figure 2.6 ACK frame formats.

or not received, resulting in the originating station assuming that a problem occurred and retransmitting the previously transmitted frame.

2.1.3.5 Other Frame Types

There are three additional control frames we will briefly mention. Those control frames include a Power Save-Poll (PS-Poll) frame, Contention Free-End (CF-End) frame and a Contention Free-End plus Contention Free-ACK (CF-End+CF-ACK) frame. In a PS-Poll frame the Duration/ID field contains the Station ID. The function of this frame is to retrieve the power save status of the indicated station. The CF-End and CF-End+CF-ACK frames are used in an optional IEEE 802.11 access method referred to as a Point Coordination Function (PCF). This access method uses a Point Coordinator (PC) which is responsible for acting as a ‘traffic cop’ with respect to network access, polling the stations within the service set. The PCF employs an access priority method that creates a Contention-Free (CF) access period by transmitting CF-End frames, with stations responding with a CF-END+CF-ACK frame. Because these frames are not involved with security, we will not probe deeper into their use or their composition.

2.1.4 Management frames

A third type of IEEE 802.11 defined frame is the management frame. There are several types of management frames that can directly or indirectly affect certain security-related aspects of IEEE 802.11 wireless LANs that we examine in this section. However, prior to doing so we need a frame of reference, no pun intended, so let’s begin our examination of management frames with a discussion of the manner by which stations join a wireless LAN, a process referred to as association. Once this is accomplished we will examine the management frames involved in the association process.

2.1.4.1 The Association Process

The initial communication between two stations in an independent BSS, or between a station and an access point within an infrastructure BSS, is referred to as an association. The association process is accomplished through one of two types of scanning. The first type of scanning, which is referred to as passive scanning, results in a station listening to each IEEE 802.11 channel for a predefined period of time. The station listens for a special type of management frame referred to as a beacon. Access points periodically broadcast beacon frames that identify the AP and define its capabilities. Included within the

beacon is an identifier referred to as a Service Set Identifier (SSID) which functions as an elementary password. Because it is possible to have multiple access points within a geographic area, stations require the ability to associate themselves with a predefined AP. To do so you configure your station with the SSID of the access point you wish to communicate with.

Figure 2.7 illustrates the editing of the Orinoco wireless LAN software utility configuration program to change the network name, a term Agere Systems uses to reference the SSID to ‘any.’ By specifying the name ‘any’, you can usually attach to most wireless LAN access points, a vulnerability we will discuss in more detail later in this book.

A second scanning method results in a station transmitting a probe frame on each channel, waiting for all access points within hearing of the probe to respond with a probe response frame. This type of scanning is referred to as active scanning. Like a beacon frame, the probe frame contains an SSID and additional information, which we will shortly consider.

Regardless of the type of scanning used, once a station recognizes an access point it will transmit an associate request frame. This frame will denote the

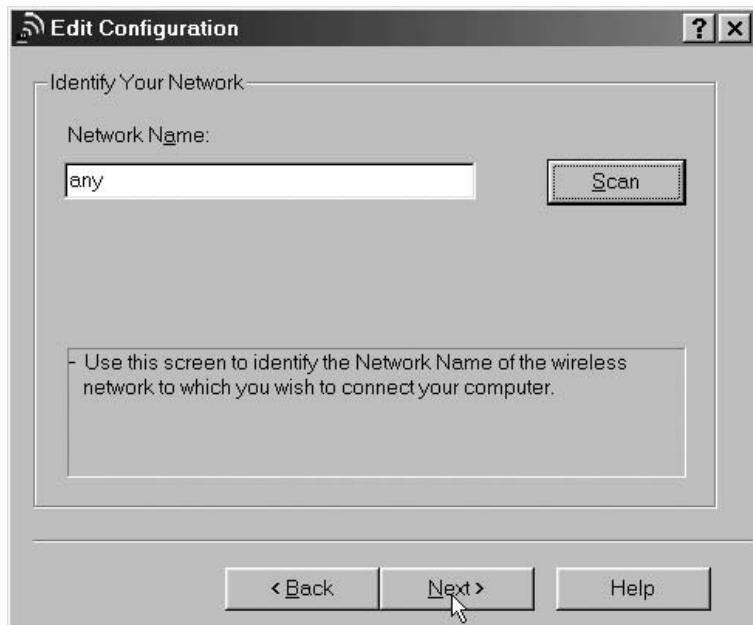


Figure 2.7 Through the use of the network name ‘any’ you can usually connect to most access points even if you do not know the SSID.

capabilities of the station and the data rates it supports. The access point will respond with an associate response frame. The associate response frame includes a status code and station ID for the station. Upon receipt of the associate response frame the station becomes part of the network and can begin transmitting.

Figure 2.8 illustrates an example of the association process under both passive and active scanning. The top portion of Figure 2.8 shows the flow of frames when passive scanning is employed. In comparison, the lower portion of Figure 2.8 illustrates the association frame flow when active scanning occurs. Now that we have an appreciation for the manner by which the association process occurs, let's take a look at the general composition of a management frame and how the body of the frame is modified to denote several specific types of such frames.

2.1.4.2 General Frame Format

Figure 2.9 illustrates the general frame format of an IEEE 802.11 management frame. In examining the fields shown in Figure 2.9, the control field consists of the subfields previously described at the beginning of this chapter. The Duration field defines the duration based upon the data rate at which control frames in a frame exchange sequence are transmitted. The BSSID represents

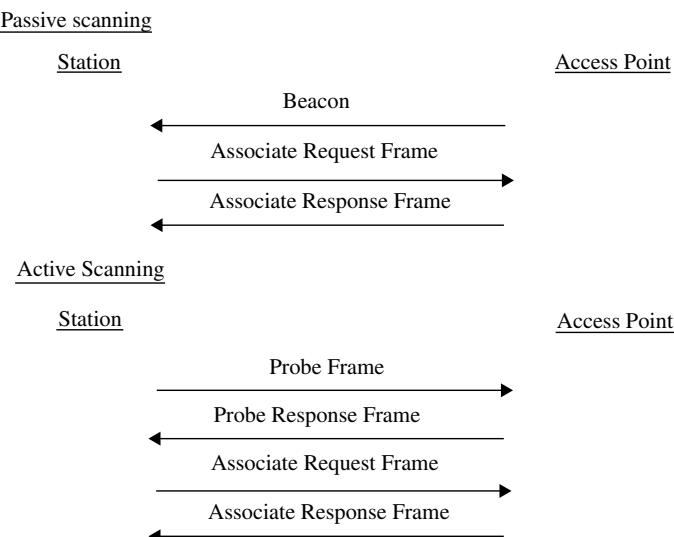


Figure 2.8 Passive and active scanning.

Bytes:	2	2	6	6	6	2	0-2312	4
	Frame Control	Duration	Destination Address	Source Address	BSSID	Sequence Control	Frame Body	FCS

Figure 2.9 General format of an IEEE 802.11 management frame.

the address used by an access point when a frame is generated by an AP. When the Management frame is a Probe Request generated by a station, the BSSID can be either a specific BSSID or a broadcast BSSID. As previously noted, the composition of the Type and Subtype subfields in the Frame Control field defines the type of frame. For example, when set to a value of 001000, this defines a Beacon frame.

For each specific management frame the Type and Subtype fields in the Frame Control field define the frame. The frame body then conveys the information that is provided by the specified management frame. In this section we look at the contents of the frame body of several common types of management frames.

2.1.4.3 Beacon Frame

As previously mentioned, an access point periodically transmits beacon frames as a mechanism to inform stations of its presence. The beacon frame contains a timestamp, an identifier in the form of an SSID, and a variety of capability information. A beacon frame can also be issued by stations within an IBSS. When this situation occurs, the beacon frame will include an IBSS parameter set within the frame body.

Figure 2.10 illustrates the contents of the frame body for a beacon frame. Note that only one of the FH, DS and CF parameter sets are included in a beacon, with the information elements for a particular parameter set based upon a station using Frequency Hopping (FH) or Direct Sequence (DS) spread spectrum or an access point supporting a method of channel access, referred to as Point Coordination Function (PCF). PCF represents a polling method network access option that to the best of this author's knowledge, has yet to be implemented by a vendor. Also note that the TIM field is only applicable for beacon frames generated by an access point.

The capability information field contains five one bit subfields that indicate requested or advertised capabilities. The remaining 10 bits in the field are reserved for future use. The lower portion of Figure 2.10 indicates the subfields within the capabilities information field. An access point will set

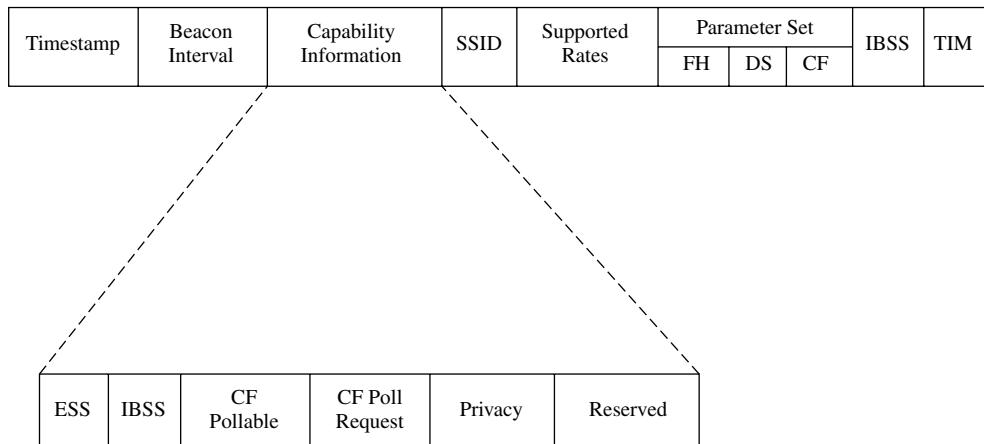


Figure 2.10 The beacon frame body.

the ESS subfield to 1 and the IBSS subfield to 0 when transmitting Beacon or Probe Response management frames. In comparison, stations within an IBSS will reverse the prior settings, with the ESS subfield set to 0 and the IBSS subfield set to 1 when it transmits a Beacon or Probe Response management frame. Because the probe response frame follows a probe request frame, we'll look at them both in their logical order. We first examine the probe request frame and then follow this with an examination of the probe response frame.

2.1.4.4 Probe Request Frame

A probe request frame is transmitted by a station performing active scanning during an association process. Like a beacon frame, a probe request frame represents a management frame. The frame body of a probe request frame is fairly simplistic, containing the SSID and the supported data rates of the station issuing the frame.

2.1.4.5 Probe Response Frame

An access point that receives a probe request frame will respond to the station issuing the frame with a probe response frame. This management frame has a frame body very similar to the body of the beacon frame previously shown in Figure 2.9. The difference between the two resides in the omission of the TIM from the probe response frame.

2.1.4.6 Association Request and Response Frames

Once a station notes the presence of an access point it can negotiate access to the AP. This negotiation process results in the transmission of an associate request frame from the station to the AP. The access point will respond with an association response frame.

The top portion of Figure 2.11 illustrates the frame body of an association request frame. The lower portion of Figure 2.11 shows the frame body of the corresponding association response frame.

The status code field in the association response frame indicates if the operation was successful or if not, the cause of the failure. Because status codes are applicable to both association and authentication, the range of status codes encompasses both functions. Table 2.3 lists the presently defined status codes. Of course, in an association response frame the entries permissible for the status code field cannot take on values associated with authentication operations and vice versa.

Returning to the association response frame, the association ID field contains a value assigned by an access point during the association process. The value of this field represents a 16 bit identifier the AP assigns to a station.

2.1.4.7 Disassociation Frame

Once a station is associated with another station or access point either party can break the association. To do so the station or access point will transmit a disassociation frame which must be honored. The frame body of a disassociation frame only contains a reason code field, which indicates the reason for terminating the previously established association. One of the hidden weaknesses of the IEEE 802.11 standard is the

Association Request Frame

Capability Information	Listen interval	SSID	Supported Data Rates
------------------------	-----------------	------	----------------------

Association Response Frame

Capability Information	Status Code	Association ID	Supported Data Rates
------------------------	-------------	----------------	----------------------

Figure 2.11 The frame body of the association request and association response frames.

TABLE 2.3 Status code values

Value	Meaning
0	Successful
1	Unspecified failure
2–9	Reserved
10	Cannot support all requested capabilities in the Capability Information field
11	Reassociation denied due to an inability to confirm that an association exists
12	Association denied due to reasons outside the scope of the standard
13	Responding station does not support specified authentication
14	Received an authentication frame with an out of order sequence number
15	Authentication rejected because of challenge failure
16	Authentication rejected due to timeout while waiting for the next frame
17	Association denied due to AP being unable to handle additional stations
18	Association denied due to requesting station not supporting all of the data rates in the BSS rate set parameter
19–65535	Reserved

lack of reauthentication for verifying the identity of a station transmitting a disassociation frame. As we will note in Chapter 7, this weakness theoretically enables an unauthorized third party to disassociate a client station from an in-progress session, spoof their address, and in effect hijack their session.

2.1.4.8 Reassociation Frames

Two additional management frames that warrant a brief mention are reassociation request and reassociation response frames. The reassociation request frame is similar to the association request frame whose body was previously shown in Figure 2.11. The difference between the two is the inclusion of a current AP address field in the reassociation request frame. This field occurs before the SSID field shown in Figure 2.11. In comparison, the reassociation response frame's frame body is the same as an association response frame body.

2.1.5 The authentication process

A second function performed when a station attempts to join a wireless LAN is authentication. Authentication follows association and represents the procedure an access point and associated station perform to verify that a station has permission to gain access to the wireless network.

IEEE 802.11 wireless LANs support two authentication methods – open system and shared key – as described in Chapter 1. In Chapter 1, open system authentication can be considered to represent a null authentication method, whereas shared key results in the use of a preconfigured WEP key to encrypt challenge text which the AP transmits to the station via an authentication frame.

2.1.5.1 Authentication Frame

Figure 2.12 illustrates the frame body of an authentication frame. Note that the authentication algorithm is set to a value of 0 for open system authentication or a value of 1 for shared key authentication. Also note that the authentication transaction sequence number field defines the type of authentication (open system or shared key), status code (reserved or status) and the presence or absence of challenge text.

2.2 WEP and privacy

In concluding this chapter we turn our attention to a third function that can occur when a station becomes part of an IEEE 802.11 wireless LAN. That function is referred to as privacy within the 802.11 standard; however, it is more commonly known in most literature as WEP.

2.2.1 Misconceptions

The goal behind WEP was to provide wireless LANs with a level of privacy equivalent to a wired infrastructure. It is important to recognize this goal, as many trade publications featuring articles discussing WEP problems fail to state this. When you consider the design goal of WEP you realize that it

Authentication Algorithm Number	Authentication Transaction Sequence #	Status Code	Challenge Text
---------------------------------	---------------------------------------	-------------	----------------

Figure 2.12 Authentication frame body.

is not intended to represent a totally secure method of communication, nor is it intended to provide a cryptographic method of transporting data that is unbreakable. Simply stated, WEP was designed to provide a wireless LAN with a level of privacy equivalent to data that flows in plaintext over a wired infrastructure, no more, no less. If you recognize this fact it will come as no surprise that WEP has some serious limitations. However, prior to discussing those limitations we first need to become familiar with WEP, which is the focus of this section. As we obtain an appreciation for the manner in which WEP operates we will discuss its limitations in this and succeeding chapters.

2.2.2 Development constraints

WEP was developed as a mechanism to provide data confidentiality and prevent non-authorized wireless LAN stations from being able to easily listen to the contents of an in-progress over-the-air transmission. In designing WEP, the algorithm was created to be self-synchronizing. This means that transmission is synchronized on a frame by frame basis and ensures that the loss of a frame does not adversely effect the encryption and decryption of succeeding frames.

A second design goal of WEP was to allow it to be exportable. Due to the fact that the U.S. government places limitations on the key length of encryption algorithms that can be exported, this served as another constraint during the development of WEP.

2.2.2.1 Operation

WEP is similar to other encryption algorithms in that an encryption function (E) operates on plaintext (P) to generate ciphertext (C). WEP uses the RC4 algorithm, which will be described later in this book. Assuming the cryptographic algorithm uses the key sequence k , the encryption process is represented by:

$$E_k(P) = C$$

In a reverse manner, the decryption (D) process operates on ciphertext (C) to reconstruct the plaintext (P) as indicated below:

$$D_k(C) = P$$

Under WEP the key used for encryption is also used for decryption, a technique referred to as a symmetrical key. The actual distribution of keys to access points and stations is not part of the standard and is normally accomplished by users manually configuring an access point and stations with a common key.

<u>Encryption</u>		
Key →	Plaintext Random Sequence	01101011 10110010
Ciphertext		11011001
<u>Decryption</u>		
Ciphertext	Key → Random Sequence	11011001 10110010
	Reconstructed Plaintext	01101011

Figure 2.13 The encryption and decryption process.

The WEP key is similar to other encryption keys in that it is used by an algorithm to create an infinite pseudo-random sequence of binary 1s and 0s. That sequence is XORed with the data to form encrypted text.

Figure 2.13 illustrates an example of the encryption and decryption process. In the top portion of Figure 2.13 a WEP key is shown generating a pseudo-random sequence of binary 1s and 0s that are XORed with plaintext to generate ciphertext. As a refresher, XORing is the same as a modulo 2 operation. The ciphertext is then transmitted. The recipient uses the same key to generate the same pseudo-random sequence of binary 1s and 0s as illustrated in the lower portion of Figure 2.13. The receiver uses the pseudo-random sequence in another XOR operation to reconstruct the plaintext as illustrated in the lower portion of the figure.

2.2.2.2 The Initialization Vector (IV)

Because wireless transmission has a higher probability of frames becoming lost than wired LANs, it is impractical to use an infinite pseudo-random sequence to encrypt data. Instead, a 24 bit Initialization Vector (IV) is concatenated with the key to generate a seed as input to a pseudo-random number generator. Although the WEP key remains constant, the IV will periodically change, with each new IV resulting in the generation of a new seed.

Although the WEP standard consists of over 400 pages of detailed information, the manner by which the IV changes is left to the implementer. The IV can change as frequently as with each data unit or on a less frequent basis. The IV is transmitted in the clear since its value must be known by the recipient to be able to create the correct seed necessary to generate the pseudo-random sequence required to decrypt the ciphertext. Since it is a relatively

easy process to change the IV after each frame, just about all vendors of IEEE 802.11 hardware implement WEP in this manner.

2.2.2.3 The WEP Data Unit

As previously noted, the IV is used with the WEP key to generate a seed for creating the pseudo-random sequence used for encryption and decryption. Because it is possible for a third party to intercept communications and alter data even without being able to decrypt information, WEP also performs an integrity check upon the data. The process used to protect data against unauthorized modification uses an algorithm that operates upon the plaintext to generate a Cyclic Redundancy Check (CRC). This algorithm generates a 4 byte Integrity Check Value (ICV), which is concatenated to the end of the plaintext. Then, the plaintext and the ICV are encrypted as illustrated in Figure 2.14.

In examining the WEP data unit shown in Figure 2.14, note that the IV is not encrypted since the receiver must be able to use it with its preconfigured key to generate the applicable pseudo-random bit sequence. At the receiver the same integrity algorithm is used to compute a locally generated ICV after the plaintext is restored. The locally generated ICV is compared to the transmitted ICV. If they are both equal the integrity check is considered to be without error. Otherwise an error is assumed to have occurred which is then processed by MAC management.

As indicated in Figure 2.14, the 32 bit IV consists of 3 subfields. Those subfields include a 24 bit initialization vector, a 2 bit key ID field and a 6 bit

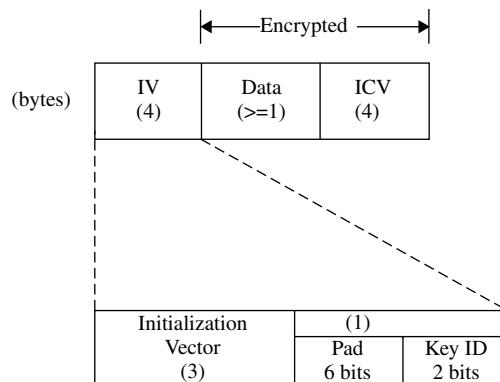


Figure 2.14 The WEP Data Unit.

pad field. The 2 bit key ID field is used to select one of four possible WEP keys that can be configured for use by a station.

Figure 2.15 illustrates the entry of a string of text referred to as a passphrase to generate four WEP keys. Normally a user might use one key at work, a second at home, and configure the other two keys for use when traveling to remote locations. Only one of the four WEP keys will be used and the other three keys do not have to be configured. The use of a 6 bit pad field and a 2 bit key ID field reduces the length of the IV field to 24 bits and represents a major limitation of WEP. Thus, in concluding this section we will look at why the basic design of WEP and the deficiencies in the wireless protocol make transmission a risky business.

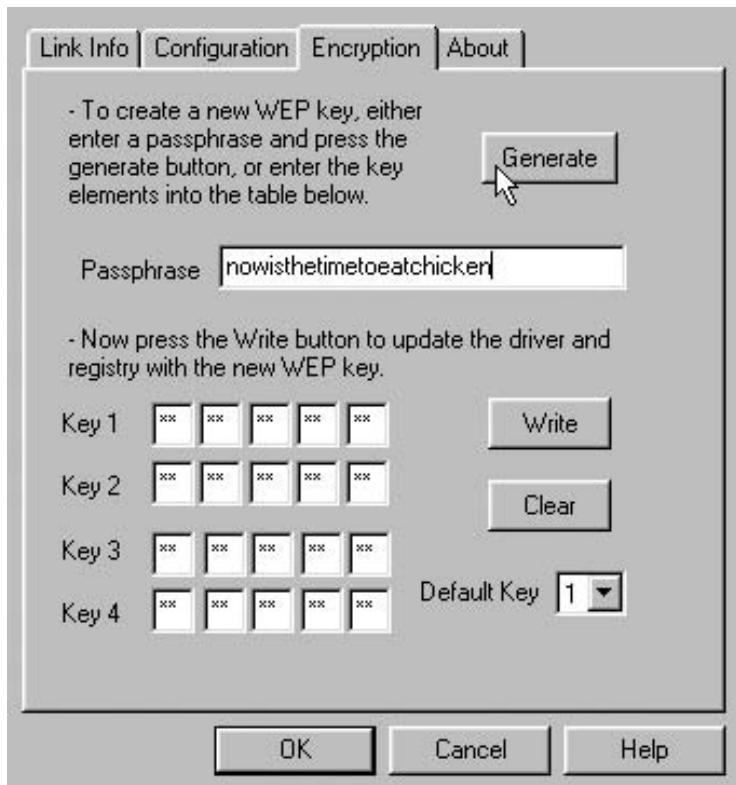


Figure 2.15 WEP enables up to four encryption keys to be defined, of which only one can be used at a time.

2.2.3 Deficiencies

The IEEE 802.11 wireless LAN standard has a number of security deficiencies. We will now become acquainted with a few of those limitations, leaving it for future chapters to determine how to overcome them.

2.2.3.1 IV Length

The length of the IV is 24 bits. This means that the maximum number of IVs that can occur as seeds for the pseudo-random number generator prior to an IV repeating is 2^{24} , or 8,388,608. If the average frame length is 1000 bytes, this means that at a data rate of 11 Mbps one frame is transmitted in;

$$\frac{1000 \text{ bytes} \times 8 \text{ bits/byte}}{11 \text{ Mbps}}$$

or 727.2×10^{-6} s.

Thus, the time required to transmit 8,388,608 one thousand byte frames one after the other becomes:

$$8,388,608 \times 727.2 \times 10^{-6} = 6100 \text{ s}$$

This means that approximately every 102 minutes an IV would have to be reused. Even if a wireless LAN only transports traffic one third of the time, this would result in an IV repeating approximately every five hours. If a third party was monitoring communications they can easily record each IV as it is transmitted in the clear. When two IVs repeat they then know that the encrypted text was created using the same key. This means that without knowledge of the key used to create the pseudo-random sequence of binary 1s and 0s used to encrypt data, you can decrypt the ciphertext through the process of frequency analysis. For example, suppose you monitored communications over a period of time and recorded the encrypted portion of frames that occurred using the same IV. Let's assume you used software to obtain a frequency count of the occurrence of each character and noted that N had the most occurrences, followed by Z . Because e and t are the two most frequently occurring characters in the English language it would probably be safe to assume that the character N represents the plaintext character e while the Z represents the plaintext character t . As you continue with the frequency analysis it becomes possible to decrypt encrypted text without having knowledge of the actual key used.

A second limitation of WEP is the fact that by default on most hardware products it is disabled. This means that it is quite common for network

managers, LAN administrators and other users to take IEEE 802.11 products out of a box and set them up without enabling encryption. In fact, as we will note later in this book, the default of no encryption accounts for the vast majority of articles concerning wireless LAN security problems.

Another commonly mentioned vulnerability associated with the use of WEP actually relates to the composition of data in certain fields transported by IEEE 802.11 frames. For example, IP headers have many known field values, such as '4' in the Version field. Thus, it becomes possible to passively monitor frames and construct a database of IVs and frames that enable the WEP key in use to be determined. Referred to as a key recovery attack, this attack, as well as methods to prevent it, will be described in subsequent chapters.

2.2.3.2 SSID

As noted earlier in this chapter, the SSID is used as an elementary password during the association process. Unfortunately the SSID is transmitted in the clear, which means it is a relatively easy process to monitor traffic to include beacons and join a network. In addition to monitoring network traffic, most hardware vendors ship products with a default SSID whose composition is relatively easy to determine. If this was not bad enough, you can configure a station with either a blank SSID or use the keyword 'any' as a mechanism to connect to an access point whose SSID is unknown. As we probe deeper into security issues we will note several examples of the use of the SSID to associate a station with an access point.

2.2.3.3 Unintended Frame

The last security related problem we will discuss in this chapter concerns the use of unintended frames. For example, transmitting a disassociation frame causes the recipient to honor the request. With a bit of effort a third party can monitor traffic and transmit disassociation requests to stations accessing an access point. By continuously broadcasting disassociation requests the third party in effect can jam wireless LAN communications.

chapter three

Understanding Wireless Signals

Any book covering wireless LAN security would be remiss if it did not provide an overview of wireless signals. By understanding wireless signals you can use readily available utility programs, bundled with many wireless LAN client stations, to determine the signal strength of access points at different locations within and outside of a building. This action can assist you in locating vulnerable areas, such as adjacent floors or parking lots where a third party could literally hide within plain sight while they record your network transmission for future analysis.

In this chapter we look at the wireless RF spectrum, first observing the locations in the spectrum that are used by wireless LANs. Once we obtain an appreciation for the frequency spectrum used by wireless LANs we will examine how to obtain knowledge about different Radio Frequency (RF) signal strength indicators and the use of general purpose and specialized antennas. In doing so we will note that differences in antenna sensitivity can enable one station to receive signals at a distance of several miles from an access point, while another station may have difficulty receiving signals from the same access point at a distance of several hundred feet. In this chapter we will also discuss the use of shielding and access point placement within a building to minimize RF signal leakage to other floors and also to outside the building. Because you cannot intercept a signal you cannot hear, one low-tech solution to minimize the risk of wireless LAN signal interception is the placement of stations and access points within a building and the use of shielding to minimize RF energy that leaves a building or a floor within a building. By considering both, you should be able to minimize the ability of an unauthorized third party to monitor your wireless LAN transmission.

As we discuss signal strength we will note how it is measured in decibels. We will also examine the use of several utility programs, bundled with various wireless LAN products, that can be used to measure signal strength within and outside of a building.

3.1 The wireless RF spectrum and basic measurements

The ability of different devices to transmit at one or more frequencies is commonly regulated in most countries. The primary reason for such regulation is to prevent communications interference. After all, you wouldn't want a person using a cell phone to interfere with ground control at the local airport guiding a Boeing 747 jet in its final landing approach.

While most countries regulate the use of RF, on a global basis it is important that the regulations of one country do not have a serious impact upon the use of equipment in another country. To facilitate the use of communications on a global basis the International Telecommunications Union (ITU) defines the general use of frequencies via treaties. ITU treaties permit countries to allocate domestic use of the frequency spectrum differently from international allocation, as long as the domestic allocation does not conflict with neighboring country frequency spectrum allocation. Thus, you can expect some differences in the use of frequency allocated for wireless LANs as you move between certain countries. In this section we will primarily focus upon the general location of wireless LAN communications within the overall frequency spectrum. Because our objective is to understand wireless signals and their affect upon security, we can satisfy this goal by noting the effect of transmission in the Gigahertz (GHz) range without having to examine transmission occurring at the precise frequencies within a channel allocated for wireless LANs. To obtain an appreciation of how wireless LANs use the RF spectrum let's first review the basics of radio frequency communications commencing with frequency.

3.1.1 Frequency

The term frequency is used to note the number of periodic oscillations or waves that occur per second. Figure 3.1 illustrates two sine waves oscillating at different frequencies. At the top of Figure 3.1, a sine wave operating at one cycle per second (cps) is shown. In the lower portion of Figure 3.1 the same sine wave is shown after its oscillating rate is doubled to 2 cps. Note that the term cycles per second was replaced by the term Hertz (Hz) in honor of the German physicist.

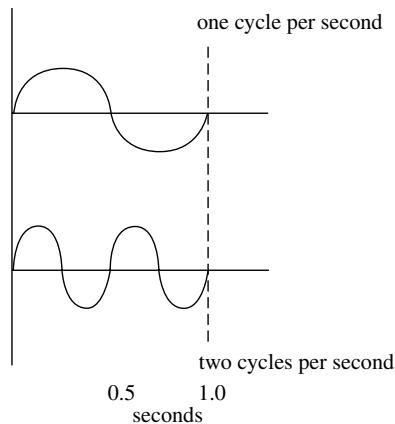


Figure 3.1 Oscillating sine waves at different frequencies.

In examining Figure 3.1 you will note that the time required for one cycle is halved when the frequency is doubled. In fact, we can mathematically describe the relationship between the period or duration (T) of a cycle and its frequency (f) as follows:

$$T = 1/f$$

We can also express the frequency in terms of the period of a signal as indicated below:

$$f = \frac{1}{T}$$

3.1.2 Period and wavelength

The period of a signal is also known as its wavelength and is denoted by the Greek letter lambda (λ). As previously indicated, the period or wavelength is the reciprocal of the frequency of a signal. The wavelength of a signal can be obtained by dividing the speed of light (approximately 3×10^8 m/s) by the frequency of a signal in Hertz. That is:

$$\lambda(m) = \frac{3 \times 10^8}{f(\text{Hz})}$$

You can easily adjust the numerator and denominator of the preceding equation to determine the wavelength based upon frequency expressed in terms of kHz, MHz and GHz. For example, to compute wavelength in terms of

kHz of a signal, the equation becomes:

$$\lambda(m) = \frac{3 \times 10^5}{f(\text{kHz})}$$

Similarly, to compute wavelength when the frequency of a signal is expressed in terms of MHz and GHz, the equations become:

$$\lambda(m) = \frac{300}{f(\text{MHz})}$$

$$\lambda(m) = \frac{0.3}{f(\text{GHz})}$$

As we will note later, the wavelength of a signal is an important criteria in antenna design. As antennas are commonly fabricated to match a quarter, half or full wave of a signal, the frequency of a signal has a direct bearing on the length of an antenna. This is because the wavelength is inversely proportional to the frequency of a signal. Thus, as the frequency increases, the wavelength decreases. This means that wireless LANs which operate in the GHz band will require a smaller antenna than an FM radio or television set that operates in MHz bands.

3.1.3 Bandwidth

Since we previously discussed frequency, a related term that warrants attention is bandwidth. Bandwidth represents a measure of the width of a range of frequencies and not the frequencies themselves. For example, if the lowest frequency that can be used within a band of frequencies is f_1 and the highest is f_2 , then the available bandwidth is $f_2 - f_1$.

One of the basic foundations of communications is the fact that data transmission operating rates are proportional to bandwidth. That is, the more bandwidth that is available the higher the potential operating rate. As we will shortly note, wireless LANs operate in the 2.4 GHz and 5.0 GHz frequency bands, with the latter providing more bandwidth, which enables higher operating rates to be achieved.

3.1.4 The frequency spectrum

The range of frequencies at which different types of communications can occur is referred to as the frequency spectrum. Included in the frequency spectrum, which ranges from 1 Hz to approximately 10^{23} Hz, are a wide range

of communications applications to include AM and FM radio, different types of mobile and cellular telephone operations, paging systems and various types of satellite communications and wireless LANs.

Table 3.1 lists a number of communications applications and the frequency where they operate. In examining the entries in Table 3.1 note that the prefixes (K) for kilo, (M) for mega and (G) for giga are used to denote thousand, million and billion of hertz, respectively. Because the period or wavelength of a signal is inversely proportional to its frequency, communications at low frequencies require longer antennas than communications occurring at high frequencies. This explains why submarines that communicate underwater using a very low frequency let out a spool of wire as an antenna that can stretch in length for hundreds to thousands of yards. This also explains why cellular telephones that operate at relatively high frequencies and have a short period or wavelength can use miniature antennas.

The two wireless LAN operating frequencies used by IEEE standardized products shown in Table 3.1 correspond to two Industrial, Scientific and Medical (ISM) bands that permit equipment to operate without license. Thus,

TABLE 3.1 Some wireless applications and the frequency bands they use

Application	Frequency
AM Radio	535–1635 KHz
Analog Cordless Telephone	44–49 MHz
Television	54–88 MHz
FM Radio	88–108 MHz
Television	174–216 MHz
Television	470–806 MHz
Wireless Data (to be licensed)	700 MHz
RF Wireless Modem	800 MHz
Cellular	806–890 MHz
Digital Cordless	900 MHz
Industrial, Scientific & Medical	902–928 MHz
Nationwide Paging	929–932 MHz
Satellite Telephone Uplink	1610–1626.5 MHz
Personal Communications	1850–1990 MHz
Wireless LANs (802.11, 801.11b)	2.4–2.4835 GHz
Satellite Telephone Downlinks	2.4835–2500 MHz
Wireless LANs (802.11a)	5.15–5.35, 5.725–5.85 GHz
Large Dish Satellite TV	4–6 GHz
Small Dish Satellite TV	11.7–12.7 GHz
Wireless Cable TV	28–29 GHz

another popular term for the frequency bands where wireless LANs operate is unlicensed frequency bands.

A third unlicensed ISM band where wireless LANs can operate is the 902–928 MHz band. Because the bandwidth is only 26 MHz in that band (the other ISM bands have 83.5 MHz, 200 MHz and 125 MHz of bandwidth) the 902–928 MHz band was not used by IEEE 802.11 compliant LANs. Due to this our primary focus concerning wireless signals will be oriented towards the 2.4 GHz and 5.0 GHz frequency bands. Although unlicensed, equipment must conform to certain regulations based upon the country where products will operate. For example, in the United States the Federal Communications Commission (FCC) regulates the frequency range within the ISM bands that equipment can operate, the channel usage for Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS) as well as the power of the RF signal permitted.

3.1.5 Power measurements

Wireless transmission is similar to its wired cousin in that various impediments cause a loss of power as a signal flows over the medium. Power measurements date to the development of the telephone and provide a mechanism to define the relationship between the received power of a signal and its original power. In this section we will examine the use of three common power measurements – the bel, decibel and decibel milliwatt.

3.1.5.1 Bel

The first measurement developed to provide a relationship between transmitted and received power was the bel (B), named in honor of the inventor of the telephone, Alexander Graham Bell.

The bel recognizes the fact that humans hear logarithms. A sound that is ten times louder than another sound appears to be twice as loud to the human ear. Due to this, the bel uses logarithms to the base 10 to express the ratio of power transmitted to power received. The resulting gain or loss is given by the following formula:

$$B = \log_{10} \frac{P_O}{P_I}$$

where B represents the power ratio in bels, P_O is the output or received power, and P_I is the input or transmitted power. As a refresher for those of us that are rusty concerning the use of logarithms, note that the logarithm to the base 10 (\log_{10}) of a number is equivalent to how many times 10 is raised to a power to

equal the number. For example, $\log_{10} 100$ is 2 since 10^2 is 100, while $\log_{10} 1000$ is 3, since 10^3 is 1000.

Because signals attenuate as they flow through a medium, output or received power is normally less than input or transmitted power. This means that the denominator in the preceding equation will normally be larger than the numerator. To simplify computations we need to note another property of logarithms, which states that the log of a fraction is equal to minus the log of the inverse of the fraction, which is mathematically expressed as follows:

$$\log_{10} \frac{1}{X} = -\log_{10} X$$

As an example of the use of the bel for the computation of the ratio of power received to power transmitted, assume the received power is one-tenth the transmitted power. Then:

$$B = \log_{10} \frac{1}{10}$$

Because $\log_{10} 1/X = -\log_{10} X$ we obtain:

$$B = -\log_{10} 10 = -1$$

Since a negative value was obtained, this indicates that a power loss occurred, whereas a positive value would indicate a power gain. Although the bel was used for many years, industry required a more precise power measurement. This need resulted in the adoption of the decibel (dB) as the preferred power measurement.

3.1.5.2 Decibel

The decibel (dB) is a more precise measurement of the gain or loss of a signal. The dB represents one-tenth of a bel and is computed as follows:

$$dB = 10 \log_{10} \frac{P_O}{P_I}$$

where dB represents the power ratio in decibels, P_O is the output or received power and P_I is the input or transmitted power. Using the preceding example, where the received power is one-tenth the transmitted power, the power ratio in decibels becomes:

$$dB = 10 \log_{10} \frac{1}{10}$$

Because $\log_{10} 1/X = -\log_{10} X$, we obtain:

$$\text{dB} = -10 \log_{10} 10 = -10$$

Today the dB represents the preferred measurement for computing power measurements. As noted from the preceding computations, a 10 dB gain or loss corresponds to a 10-fold increase in the level of a signal. Similarly, a 20 dB gain or loss corresponds to a hundred-fold increase or decrease. Thus, the use of the dB permits large variations in signal levels to be handled with small digits due to use of a log scale.

3.1.5.3 Decibel Above 1 mW

In our prior discussion of the bel and decibel we noted that they represent a ratio or comparison between two power values, such as input and output power. Because it is often necessary to compare several systems to one another, a uniform method of measuring signal power is needed. That uniform method results in the use of a 1 mW input signal being used as a standard for measuring the strength of an output or received signal. To ensure that a tester does not forget that the resulting power measurement occurred with respect to a 1 mW input signal, the term decibel-milliwatt (dBm) is used. Here the computation of the power level in dBm becomes:

$$\text{dBm} = \log_{10} \frac{P_o}{1 \text{ mW}}$$

Although the term decibel-milliwatt is used in most literature, dBm actually references the value of the output or received signal above 1 mW. Thus, 10 dBm represents a signal 10 dB above OR bigger than 1 mW, whereas 20 dBm represents a signal 20 dB above 1 mW, and so on. Because a 30 dBm signal is 30 dB or 1000 times larger than a 1 mW signal, this means that 30 dBm is equal to 1 W. Using the relationship previously described results in the construction of the watts to dBm table shown in Table 3.2.

TABLE 3.2 Relationship of Watts and dBm

Power in Watts	Power in dBm
0.1 mW	-10 dBm
1.0 mW	0 dBm
1.0 W	30 dBm
1.0 KW	60 dBm

We can express the relationships shown in Table 3.2 mathematically. To convert from dBm to watts or mW, we would use one of the two following equations:

$$W = 10^{((\text{dBm}-30)/10)}$$

$$\text{mW} = 10^{(\text{dBm}/10)}$$

If we know the signal strength in milliwatts we can convert to dBm using the following relationship:

$$\text{dBm} = 10 \log_{10} [\text{milliwatts}] + 30$$

3.1.6 Power level

Another key relationship shown in Table 3.2 that warrants attention is the fact that 1 mW is equivalent to 0 dBm. To ensure we understand this relationship let's assume the output and input power are both 1 mW. Then, the power level in dBm becomes:

$$\text{dBm} = 10 \log_{10} \frac{1 \text{ mW}}{1 \text{ mW}} = 10 \log_{10} 1 = 0$$

Thus, a signal strength or power level of 0 dBm represents 1 mW of power. In a wireless LAN environment you can examine the specifications of different equipment to note two key metrics. Those metrics concern the output power and antenna sensitivity, the latter commonly referred to as RX (receiver) sensitivity. Both output power and receiver sensitivity are expressed in mW and dBm. While there are no regulations concerning antenna sensitivity, the FCC in the United States (and other organizations in different countries responsible for regulating communications) place limits on the signal strength of different applications and antenna gain, the latter is a term we will discuss when we examine antenna operations later in this chapter.

3.1.7 Signal-to-noise ratio

In all communications systems there is a degree of noise caused by the movement of electrons, power line induction and other disturbances. There are two basic types or categories of noise that can adversely effect communications. One type of noise is called thermal or white noise and represents a near uniform distribution of energy over the frequency spectrum. A second type or category of noise is referred to as impulse noise. Impulse noise represents noise that occurs at random times and at random frequencies. Sources of impulse noise include electrical machinery turning on and sun spots.

When designing a communications system it is obviously important to ensure that the signal can be heard by the receiver. Because thermal noise represents a near uniform distribution of energy over the frequency spectrum it also represents the lower level of sensitivity of a receiver. That is, a receiver must be able to hear a signal above the level of noise to be able to discriminate the signal from the noise. Similarly, a transmitter must generate a signal above the level of noise for the receiver to be able to hear it.

One common method used to categorize the quality of a transmission system is obtained through the use of the signal-to-noise (S/N) ratio. The S/N ratio is measured in decibels and is defined as the ratio of the signal power (S) divided by the noise (N) power on a transmission medium. The S/N level should always be greater than 1 to enable a receiver to discriminate the signal from background noise. While a high S/N ratio is desirable, there are limits on the signal strength transmitters can generate. In the United States the FCC regulates the amount of power that can be transmitted. As we will note later, the maximum power level that wireless LANs can operate at are based upon the frequency at which they operate and the gain of the antenna used.

Table 3.3 provides a summary of the relationship between decibels and the power or S/N ratio. In examining the entries in the table there are several that warrant attention. First, note that a decibel reading of 0 means that power output equals power input and there is no gain or loss. When computing the S/N ratio, this means that the signal power and noise power are equal. A second dB value to note is 3, as this represents a power or S/N ratio of 2 : 1. Thus, a 3 dB value indicates that the signal power is twice that of the noise power (when computing the S/N ratio) or the output power is twice the input power (when computing the power measurement). Because the output or received power is normally less than the transmitted power, a more typical power measurement would be -3 dB which would indicate the received power was one half of the transmitted power.

If you look at the decibel values that are multiples of 10 you will notice that they correspond to increments of power or S/N ratios that increase by a power of 10, commencing at 10. That is, a dB value of 10 corresponds to a power or S/N ratio of 10 while a dB value of 20 corresponds to a power or S/N ratio of 100, and so on.

As in our prior discussion, when the dB measurement is preceded with a negative sign, it indicates that the received power is less than the transmitted power. Thus, a dB of -10 indicates that one tenth of the transmitted power was received while a -20 dB reading indicates one hundredth of the transmitted power was received and so on. Negative dB readings are important when

TABLE 3.3 Relationship between decibels and power measurements

Decibels	Power or S/N Ratio
0	1.0 : 1
1	1.2 : 1
2	1.6 : 1
3	2.0 : 1
4	2.5 : 1
5	3.2 : 1
6	4.0 : 1
7	5.0 : 1
8	6.4 : 1
9	8.0 : 1
10	10.0 : 1
13	20.0 : 1
16	40.0 : 1
19	80.0 : 1
20	100.0 : 1
23	200.0 : 1
26	400.0 : 1
29	800.0 : 1
30	1000.0 : 1
33	2000.0 : 1
36	4000.0 : 1
39	8000.0 : 1
40	10000.0 : 1
50	100000.0 : 1

discussing receiver sensitivity as they indicate the percentage of transmitted signal power an antenna can receive.

Now that we have an appreciation for the location in the frequency spectrum where wireless LANs operate and also of some basic signal measurements, we can use this information to understand how antennas operate. In the next section we will examine how antennas radiate RF signals and their basic characteristics, and how they can be used to pick up weak and obscure signals from certain locations.

3.2 Antenna basics

The antenna represents an essential part of an RF communications system. In this section we will look at basic types or categories of antennas and

metrics that define how well an antenna picks up or transmits a radio signal.

3.2.1 Basic operation

An antenna represents a transmission line that converts electrical energy in the form of voltage and current into electromagnetic energy in the form of RF waves. The length of the antenna is inversely proportional to the frequency of transmission. Thus, as previously noted, as we move up the frequency spectrum from radio to television to cell phone and wireless LANs, the antennas used for each method of RF transmission decreases in length.

An antenna transmits electromagnetic waves that propagate in all directions away from the transmission line. The actual process by which antennas operate were described mathematically by Marwell in 1865. Without going into detail, we can state that RF waves are generated in response to electrical current traveling through a conductor, changing its velocity or direction. This enables antennas to be fabricated in many shapes, such as long rods, curved, and shaped in a T or F. Such variations in antenna shapes are designed to vary the flow of current, which functions as a mechanism to induce electromagnetic energy.

In an ideal situation, selecting the length of an antenna as an integral multiple of the frequency of oscillations maximizes the radiation or RF waves emanating from the antenna. One of the most efficient antennas is the dipole, which is fabricated by bending a two-wire transmission line into the shape of the letter 'T', where the horizontal portion of the T represents the radiating portion of the antenna. Here the length of the horizontal portion of the 'T' shaped antenna is the wavelength (λ) of the signal. However, this design results in half of the antenna being above and half below the transmission device it is connected with. Because this is not an attractive design for equipment that must reside on a desk or be carried in a person's hand, the monopole antenna was developed. The monopole antenna consists of half the length of the dipole ($\lambda/2$) and is commonly implemented using a quarter wavelength ($\lambda/4$). Monopole antennas are commonly used in cellular phones and in wireless LANs, especially in access points. For most client stations an embedded or internal antenna is fabricated within the plastic portion of a PC Card that protrudes from the card slot in a notebook. Some common types of embedded antennas include microstrip lines fabricated by etching a copper strip onto a circuit board and a Planar Inverted 'F' Antenna (PIFA) that resembles the letter 'F' lying on its side. Unlike the dipole, the microstrip and PIFA have a shorter range due to their embedded fabrication and lack of height.

3.2.2 Categories

There are two basic types or categories of antennas, unidirectional and omni-directional. A unidirectional antenna radiates in one direction while an omni-directional antenna radiates signals in many directions. Antennas can radiate as well as receive information in the horizontal and vertical plane. The 3-dimensional (3D) radiation pattern is represented by two perpendicular planes referred to as azimuth elevation. The azimuth represents horizontal radiated power, while the elevation represents vertical radiated power. The horizontal and vertical patterns of radiated power are commonly noted in diagrams with respect to 360 degree circles. Figure 3.2 illustrates an example of the radiation power of a broadband wireless antenna developed to operate in the 2.4 GHz frequency band. Note the concentric circles represent power levels in dB that are very weak at the center and increase as each circle expands. Thus, the antenna pattern indicates both the direction and strength of the radiated signal.

3.2.3 Antenna gain

A measure of how well an antenna can transmit or receive a radio signal is referred to as the antenna gain. Antenna gain is measured in terms of decibel isotropic (dBi). The dBi represents a unit of measurement denoting how much better an antenna is in comparison to an isotropic radiator, with the latter representing a theoretical antenna that transmits signals equally in all directions in the horizontal and vertical plane. An antenna that functions as an isotropic radiator has a 0 dBi gain and serves as a point of reference. The higher the dBi the higher the gain. For example, a 4 dBi antenna gain results in the reception of a better signal than a 2 dBi antenna.

Because dBi represents a log scale from Table 3.3, a 3 dBi value represents an antenna twice as good as a 0 dBi antenna. Similarly, an antenna with a

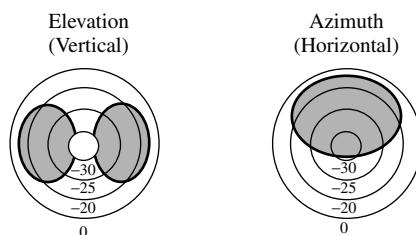


Figure 3.2 An example of broadband wireless antenna patterns (scale in dB).

20 dBi value can be considered to be one hundred times as good as a 0 dBi antenna. In the real world there are many factors that govern the antenna gain beyond the type of antenna. Other factors include the antenna placement and its orientation.

A second measurement used with antennas to note their gain is decibel dipole (dBd). The dBd represents a measurement that indicates how much better an antenna performs in comparison to a dipole antenna. When used as a gain reference, a ‘lossless’ half-wave dipole has a power gain of 0 dBd. The gain of microwave antennas operating above 1 GHz is generally given in dBi. A dipole antenna has 2.15 dB gain over a 0 dBi isotropic antenna. Thus, if an antenna gain is given in dBd you can add 2.15 to it to obtain its dBi rating. For example, if an omni-directional antenna has a 4.5 dBd gain, it would have a $4.5 + 2.15$ or 6.65 dBi gain.

3.2.4 Directionality and EIRP

Antennas can obtain more gain by concentrating their radiated energy in a specific direction. For example, an omni-directional antenna attempts to concentrate its energy into the horizontal plane in a 360-degree radius since transmitting RF energy vertically is usually not beneficial. A unidirectional antenna will concentrate its power in a narrow beam, with the term ‘beam width’ used to reference the angular width in degrees between the half power points (3 dB down from maximum) of the major lobe in either the elevation or azimuth radiation pattern.

The Effective Isotropic Radiated Power (EIRP) represents the effective power in the main lobe of a transmitter antenna relative to an isotropic radiator that has a 0 dB gain. EIRP is equal to the sum of the antenna gain in dBi and the power in dBm injected into the antenna. For example, assume you inject a 15 dBm signal into an antenna that has a 12 dBi gain. Then, the EIRP becomes:

$$12 \text{ dBi} + 15 \text{ dBm} = 27 \text{ dBm}$$

Note that 27 dBm represents a signal 500 times above 1 mW. Thus, the effect obtained from injecting a 15 dBm signal into an antenna that has a 12 dBi gain is to radiate 500 mW of power.

3.2.5 Power levels

In the United States the FCC places limits on the transmit power levels of wireless LANs. For transmission in the 2.4 GHz frequency band, transmit power must be at or below 100 mW. Because the FCC regulates output

power, which represents the sum of the transmit power and antenna gain, power requirements are commonly expressed in terms of EIRP. In the United States the maximum output power for wireless LANs operating in the 2.4 GHz band is restricted to 36 dBm. From Table 3.3, this is equivalent to 4000 times 1 mW or 4 watts. In some literature you may view different values expressed in mW. Such values reflect the maximum transmit power which is limited to 50 mW for devices operating in the first 100 MHz of the wireless LAN 5 GHz band (5.15–5.25 GHz), 250 mW for devices operating in the second 100 MHz (5.25–5.35 GHz) and 1 W for devices that operate from 5.725–5.825 GHz, which is the band reserved for outdoor applications. Transmission in the 5 GHz band can occur in three distinct sub-bands, each having a different amount of permissible output power as indicated in Table 3.4.

In examining the entries in Table 3.4 note that the 5.725–5.825 GHz band is for outdoor use, while the two lower bands are for indoor use. Also note that the maximum output power is expressed in terms of using an antenna that has a gain up to 6 dBi.

You can use Table 3.4 to determine the maximum signal level that can be injected into an antenna with 6 dBi gain. For example, in the 5.15 to 5.25 GHz band the maximum output power is 40 mW, which is equivalent to a 16 dBm signal. This means a wireless LAN access point or station adapter's signal must be at or below 10 dBm when injected into a 6 dBi antenna. In actuality, most antennas used with wireless LANs have a gain well below 6 dBi. For example, a PIFA antenna used in PC Cards has a peak gain of approximately 3.9 dBi, while a 1/2 wave dipole antenna used with many access points has a peak gain of approximately 3.4 dBi.

3.2.6 Propagation loss

As a signal flows through free space it loses strength. The term Free Space Loss (FSL) is used to denote the loss that occurs to an RF signal. At an operating

TABLE 3.4 Maximum wireless LAN transmit power levels in the 5 GHz band

Frequency Band (GHz)	Maximum Output Power with up to 6 dBi Antenna Gain (mW/dBm)
5.15–5.25	40/16
5.25–5.35	200/23
5.725–5.825	800/29

rate of 2.4 GHz the formula for computing free space loss is:

$$\text{FSL} = 104.2 + 20 \log D$$

where D is the distance in miles.

For example, the free space loss at a distance of 5 miles is 118 dB. As a general rule of thumb, each time the distance between a transmitter and receiver is either doubled or halved, the signal level is increased or decreased by 6 dB.

3.2.7 Increasing antenna gain

As noted earlier, gain represents an important characteristic of an antenna. Simply stated, the higher the gain the greater the transmission distance when comparing antennas with the same beam width. Similarly, the antenna gain pattern reflects the ability of an antenna to pull a signal out of the air. Thus, it is important to note how antenna gain can be increased. You can increase antenna gain either by increasing the size of the antenna or its radiation area, the latter is referred to as its aperture. One common method used to increase antenna gain is to arrange a number of half-wave radiators into an array. In doing so the radiation becomes additive such that the gain of the array exceeds that of a single radiator. Both vertical and horizontal antenna arrays are used to increase antenna gain. When stacked vertically the antenna array will provide an omni-directional signal. When stacked horizontally the antenna array will provide a directional signal. Figure 3.3 compares the elevation and azimuth

	Aperture of Dipoles	Elevation Pattern	Azimuth Pattern
Single Antenna	①	∞	○
Vertically Stacked Array	① ① ① ①	∞	○
Horizontally Stacked Array	① ①	∞	∞

Figure 3.3 Comparing the elevation and azimuth patterns of a single dipole to vertically and horizontally stacked dipole arrays.

pattern of a single dipole antenna to vertical and horizontal dipole arrays. In examining the elevation and azimuth patterns shown in Figure 3.3, note that when dipoles are stacked vertically in line the gain is obtained from a decreased vertical aperture. In comparison, when spaced horizontally the gain is obtained from a decreased horizontal aperture.

3.2.8 Power limits

Although you can consider the use of an antenna array there are limits on the amount of power you can transmit. For example, as previously noted, FCC regulations in the United States restrict transmission to 36 dBm (4 watts) EIRP in the 2.4 GHz band. Because transmitter power and antenna gain are cumulative you need to consider both to stay within the legal limits if you are using a separate access point and antenna. Otherwise, the manufacturer is responsible for ensuring that the radiated power is within the legal limits. For example, if you use a 6 dBi gain antenna the maximum power that can be injected into the antenna is 30 dBm (1 W), resulting in 36 dBm of EIRP. Table 3.5 provides a summary of the relationship of power injected into an antenna, antenna gain in dBi, and EIRP in dBm. As indicated earlier, the maximum power of 36 dBm is equivalent to an EIRP of 4 watts.

Now that we have an appreciation of the basic parameters associated with antenna operation, let's look at their effect upon wireless LAN security.

As previously noted, wireless LANs operate in three bands set aside for unlicensed Industrial, Scientific and Medical (ISM) use. Those ISM bands are at 902–928 MHz, 2.4–2.4835 GHz, and three sub-bands in the 5 GHz band. Of those three bands, IEEE 802.11 wireless LANs operate in the two higher bands. While the FCC in the United States and different agencies in other

TABLE 3.5 Relationship between power into an antenna and antenna gain to remain within legal limits in the 2.4 GHz band

Power at Antenna (dBm/Watts)	Antenna Gain (dBi)	EIRP (dBm)
30 dBm (1 W)	6	36
27 dBm (500 mW)	9	36
24 dBm (250 mW)	12	36
21 dBm (125 mW)	15	36
18 dBm (62.5 mW)	18	36
15 dBm (31.25 mW)	21	36
12 dBm (15.625 mW)	24	36

countries regulate the power wireless LANs can use, there are no regulations that prohibit a person from constructing a very sensitive antenna that is used passively. Thus, in examining the role of antennas, let's first turn our attention to their sensitivity antenna as it governs its ability to pick up a signal.

3.2.9 Receiver sensitivity

The sensitivity of an antenna has a considerable bearing on its ability to receive a signal. In the wonderful world of wireless LANs, antenna gain increases the sensitivity of the antenna. For example, if an antenna transmitting a signal has a 10 dBi gain and the receiver has a similar gain, the net effect of two 10 dBi antennas is to increase overall communication by a factor of 100. By using a higher gain antenna you make it both more directional and more sensitive.

Although the FCC does not place limits on receiver sensitivity, IEEE standards denote receiver performance requirements. For operations in the 2.4 GHz frequency band sensitivity is defined as the minimum signal level required for an error rate of three percent for data units of 400 bytes. For that error level, receiver sensitivity shall be less than or equal to -80 dBm. For operation in the 5 GHz frequency band, receiver sensitivity levels are based upon an error rate less than 10 percent of a data unit of 1000 bytes for each of eight distinct operating rates. Table 3.6 lists IEEE 802.11a receiver sensitivity levels based upon LAN operating rates.

To obtain an appreciation of receiver sensitivity remember that dBm represents a log to the base 10 scale with respect to a 1 mW signal. The negative sign in front of each minimum sensitivity level indicates that the received power is less than the 1 mW reference signal. Because 60 dB is equivalent to a ratio of a million to 1, -60 dBm sensitivity indicates a receiver is capable of receiving one millionth of the transmitted signal. Similarly, -70 dBm receiver sensitivity level indicates the receiver can pick up one ten-millionth of a

TABLE 3.6 IEEE 802.11a receiver sensitivity

Data Rate (Mbps)	Minimum Sensitivity (dBm)
6	-82
9	-81
12	-79
18	-77
24	-74
36	-70
48	-66
54	-65

signal while a -80 dBm sensitivity level indicates the ability to pick up one hundred millionth of a signal.

3.2.10 Reducing emitted radiation

Earlier in this chapter we noted that a signal which cannot be received cannot be intercepted. In this section we will examine two methods that can be used to reduce the level of RF energy that flows over the air. One method involves the use of directional antennas, while a second method involves the use of shielding.

3.2.10.1 Using Directional Antennas

If you locate an access point in the center of a floor in a multistorey building, a majority of RF energy will radiate outward from the antenna along the length of the floor. A portion of RF energy will also flow both upward and downward along the antenna axis, resulting in a portion of the signal being transmitted to floors above and below where the access point is located.

You can reduce the amount of radiated energy flowing to other floors by either using a different type of antenna or through the use of shielding. Concerning the use of a different antenna, when dipoles are stacked vertically their radiation is in phase, which results in RF energy being concentrated along the axis of the dipoles in the array. One type of antenna you can consider using whose fabrication is based upon an antenna array is a slotted waveguide. This type of antenna has a relatively narrow range of operating frequencies and in many respects is similar to a dipole array.

A slotted waveguide uses a low loss transmission line (the waveguide) to send signals to a number of small antennas referred to as slots. Signals flow along the waveguide, which traverses the slots. Each slot permits a portion of the signal energy to be radiated. The slots are positioned in a linear array pattern, which results in the sum of radiated energy providing a high power gain over a small range of angles close to the horizon. The result is an extremely directional antenna whose energy primarily flows along the horizontal plane.

A typical slotted waveguide antenna can be expected to have a gain between 15 and 17 dBi that varies slightly over the range of frequencies it supports. Because energy primarily flows in the horizontal plane, the use of a slotted waveguide antenna results in a significantly weaker signal that will be received on the floors above and below the floor where an access point is located.

Although you can consider using several types of directional antennas to minimize RF leakage to other floors, such antennas may transmit a stronger signal in the horizontal plane. Thus, you need to consider the horizontal

distance by which an RF signal can flow. However, before we discuss horizontal distance, let's briefly discuss the use of shielding as a mechanism to control RF signal leakage.

3.2.10.2 Shielding

If you use a directional antenna some energy will flow to areas where they could be intercepted by an unauthorized third party. To minimize the potential of RF energy flowing to different floors you can consider placing shielding above and below the location of your access points. Although you could also place shielding above and below your organization's wireless client stations, from a practical standpoint it is much more difficult to do so since many stations are mobile. Concerning shielding, this author determined that old fashioned 'tin foil,' which is now produced as aluminum foil and costs a few dollars for a 50 yard roll, can be effectively used when a length of foil is doubled. By positioning a doubled length of foil above and below an access point you can minimize the leakage of the strongest portion of the signal to other floors. Because it is important to be able to observe the strength of RF signals we will describe the use of tools bundled with wireless LAN hardware in concluding this chapter.

3.2.11 Horizontal transmission distance

Ignoring obstructions in the path of a signal, its strength is inversely proportional to the distance squared. This means that when the transmission distance is doubled, the strength of the received signal becomes one quarter of the original signal strength. Two additional factors that need to be considered concerning the ability of both authorized and nonauthorized people being able to receive RF signals, are the operating rate of the signal and its frequency. Concerning the operating rate of an RF signal, as the baud or signal rate increases the duration between signal changes decreases. This means that it becomes harder to receive a signal at a given distance as the baud rate increases. Because a higher data transmission rate involves packing more bits into each signal change, we can also note that as the data rate increases it becomes harder to receive a signal at a given distance.

Table 3.7 lists the transmission distances for a Linksys 802.11b access point for indoor and outdoor operations. Note that the transmission distance is proportional to the operating rate, with a higher operating rate having a lower transmission distance. This means if you are using equipment that permits you to fix the data rate of client stations and access points you can minimize transmission distances by setting the data rate to a higher setting. Also note

TABLE 3.7 Linksys access point transmission distances

Data Rate (Mbps)	Outdoors	Indoors
11	50 M (164 ft)	250 M (820 ft)
5.5	80 M (262 ft)	350 M (1148 ft)
2	120 M (393 ft)	400 M (1312 ft)
1	150 M (492 ft)	500 M (1640 ft)

that the transmission distances contained in Table 3.7 are based upon the sensitivity of antennas used by Linksys. Linksys, like other wireless LAN equipment vendors, fabricates a built-in antenna in their PC Cards. Because it is rather difficult to fabricate an antenna onto the small circuit board inside the plastic cover that represents the edge of the PC Card which protrudes from a laptop or notebook computer, the effective gain of such antennas are relatively low. The gain of an antenna embedded into a PC Card is less than 0 dBi (typically -4 dBi) and is very directional. This means that a majority of the leakage of RF signals onto other floors and to the outside of a building result from the access point and not from wireless stations using PC Cards. Thus, unless you use PC Cards that have a socket for an external antenna and use a stand-alone antenna with the card, you can concentrate your shielding effort upon the antennas connected to access points.

A third factor that adversely effects transmission distance is frequency. If you had the good fortune to take a physics class you probably remember reading that high frequencies attenuate more rapidly than low frequencies. We can apply this property of physics to wireless LANs and note that the radius of unobstructed transmission in the 5 GHz frequency band is approximately half that of wireless LANs which operate in the 2.4 GHz band. This explains why IEEE 802.11a networks that operate in the 5 GHz frequency band require more access points to provide coverage over a given geographic area than IEEE 802.11 or 802.11b networks which operate in the 2.4 GHz frequency band. This also explains why RF signal leakage may not be as much of a problem when operating at 5 GHz as when operating in the 2.4 GHz frequency band.

3.2.12 Equipment positioning

One technique you can consider to minimize RF leakage to undesirable areas concerns the positioning of equipment in conjunction with a small amount of shielding. Because access point antennas typically have a higher gain than the antennas used by workstations, we will focus upon the former.

Because signal strength is highest when a signal begins its radiation from an antenna, shielding is most effective when placed near the antenna. Thus carefully positioning and shielding the antennas of an access point may prevent RF leakage to locations where an unauthorized third party could receive and monitor your organization's transmission.

Because parking lots and open areas represent locations where unauthorized monitoring commonly occurs, you should consider positioning and shielding access points to minimize RF radiation towards those areas. To determine the level of RF radiation, and if your wireless LAN signals can be observed, you can use one of the utility programs that are commonly bundled with wireless hardware, so let's conclude this chapter by examining their use.

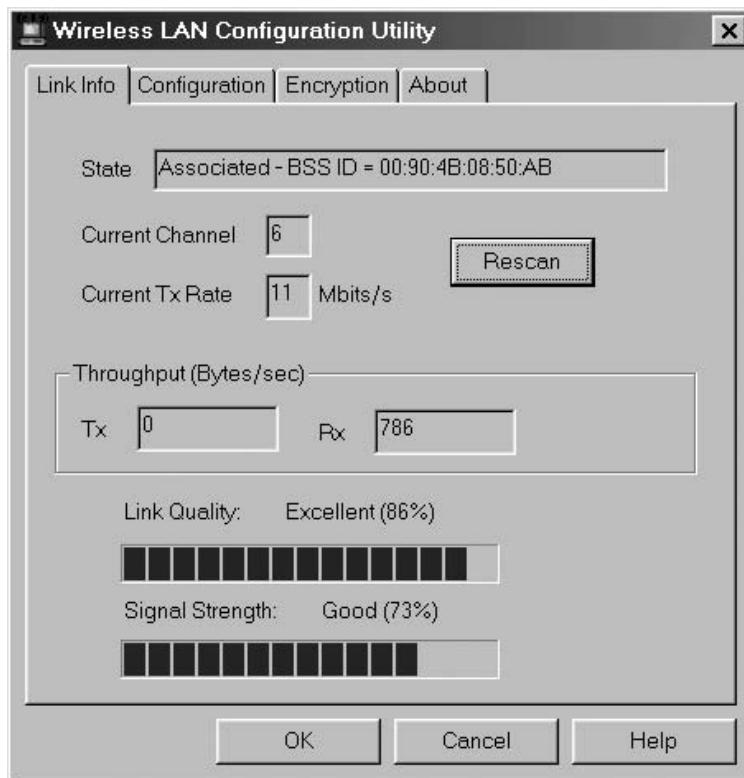


Figure 3.4 You can use the wireless LAN utility program bundled with many hardware products to determine the general level of signal strength within and outside of a building.

3.2.13 Using monitoring equipment

Figure 3.4 illustrates the use of the wireless LAN configuration utility program bundled with SMC Networks wireless LAN adapter cards to determine the link quality and signal strength of an access point. By operating this program on a notebook and moving about the office and outside the building you can determine the signal strength that a third party would receive. However, when doing so it is important to realize that PC Card type antennas typically have a 0 dBi gain. Thus, even a poor level of observed signal strength could be enough for a third party equipped with a very sensitive antenna to monitor your organization's communications. This means that when using a utility program which provides a general level of signal strength, the signal level shown may not be sufficient to determine if the RF signal can be received and understood by a third party. Thus, you may wish to consider using a client station that can accept the insertion of a more sensitive antenna into the wireless PC Card installed in your notebook.

To obtain a higher level of information concerning RF signal strength you can also consider using a utility program which provides a signal level in terms of dBm. One example of this type of program is the Orinoco Client Manager Link Test, shown in Figure 3.5. Note that the use of the link test

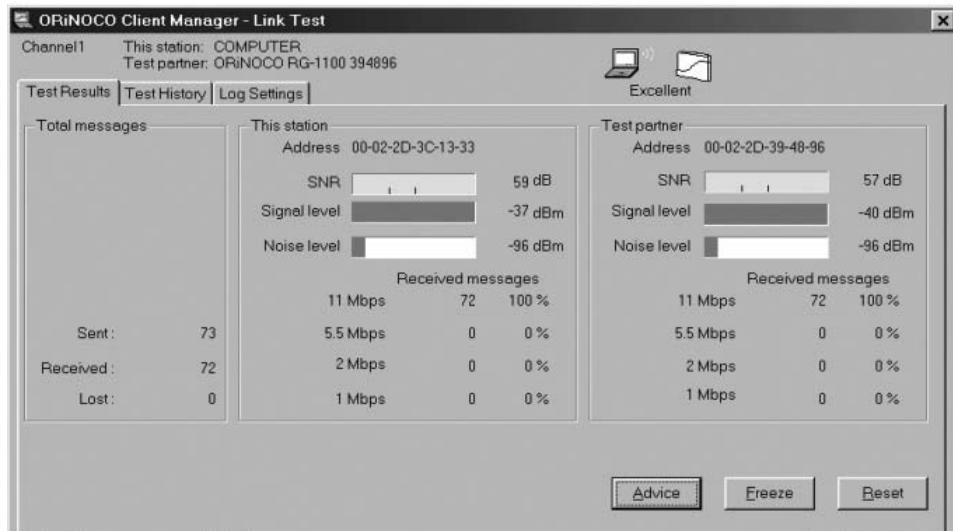


Figure 3.5 The Orinoco Client Manager Link Test displays the signal level and noise level for the station and its test partner in dBm.

results in the display of the signal level for the station and its test partner, which was an Orinoco residential gateway. Because the noise level is shown as -96 dBm , if you move your notebook or laptop outside the building and find that the signal level approaches that metric, it will be near impossible for a third party to monitor your organization's wireless LAN activity. This, as we noted earlier, results from the need to have the signal level above the noise level for a receiver to be able to discriminate the signal from the noise.

chapter four

Understanding WEP

The basic security mechanism used by IEEE 802.11 wireless LANs is referred to as Wired Equivalent Privacy (WEP). Unless you avoided reading technical magazines, newspapers and watching television over the past year, you very likely noted many media related articles which discussed WEP vulnerability. Unfortunately, many of the so-called ‘success stories,’ which described how easy it was for a third party to monitor and understand wireless transmission, were a bit deceptive. As we will note, a key WEP related problem is that by default on most products it is disabled. This means it is relatively easy for an unauthorized third party to determine what is being transmitted over the air if they can hear the wireless signal.

In this chapter we will look at WEP and obtain an understanding of its weaknesses. In doing so we will commence our examination of WEP with a quick review of the general manner in which this security mechanism operates. Once this is accomplished, we will examine the default settings of several hardware products to obtain an appreciation of why most default settings are dangerous. To illustrate the danger of most default settings we will examine the use of a program that can locate ‘hot zones’ where wireless LAN activity is occurring. We will then use another program to monitor and decode over-the-air transmissions. After we note how easy it is to locate and read IEEE wireless LAN traffic which is not encrypted, we will probe deeper into WEP. Because WEP uses the RC4 algorithm to encrypt plaintext and decrypt cipher text, we will discuss how that algorithm operates. We will also review the findings of several papers which note the vulnerability of the structure of WEP and the use of the RC4 algorithm which illustrates why WEP can be easily broken. From information presented in this chapter we will obtain an appreciation of how WEP operates, why it is not secure, and how it can be improved.

4.1 The WEP frame body

Because the best way to obtain an appreciation of WEP is through an examination of its frame body, we will briefly review its composition. Figure 4.1 illustrates how the encrypted frame body is constructed by the WEP encipherment process.

4.1.1 The IV

As a review of previously presented material, the Initialization Vector (IV) is 4 bytes in length, of which 3 bytes (24 bits) are used as a seed with the secret key to generate the WEP pseudo-random number sequence. The fourth byte has two subfields. The first subfield of 6 bits is not used and represents pad bits. The second subfield, which is 2 bits in length, is used to select one of four possible secret key values for use in decrypting the frame body. This field is known as the Key ID field.

In examining Figure 4.1 note that the portion of the IV that is used as a mechanism to seed the pseudo-random number generator is transmitted in the clear. Also note that it is 24 bits in length. As we shall see later in this chapter, the relatively small length of the IV means it will repeat fairly often, a condition referred to as an IV collision. Because a repeated IV generates the same pseudo-random number sequence, it becomes possible for a third party to passively monitor transmission, capture repeating IVs and encrypted packets and perform a statistical analysis of captured encrypted packets. This

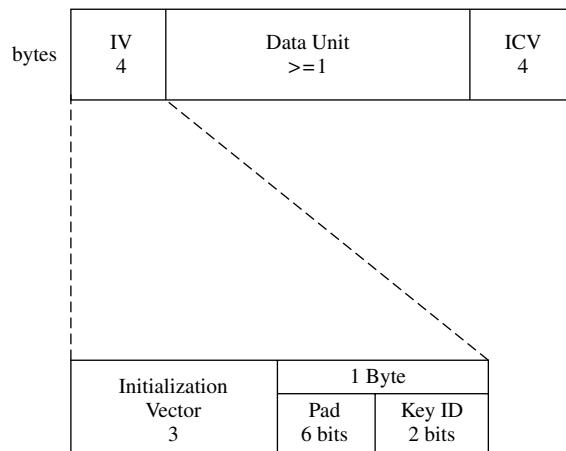


Figure 4.1 The WEP frame body.

is but one of several techniques that we will discuss in this chapter which can be used by unauthorized people to understand encrypted wireless LAN traffic.

4.1.2 The ICV

When WEP encryption is enabled the data portion of the data unit and the Integrity Check Vector (ICV) are encrypted. The WEP ICV is a 4 byte (32 bit) field, which contains a CRC-32 computed over the data field. The algorithm used for actual encryption is the RC4 algorithm, which we will discuss later in this chapter.

The purpose of the ICV is to assure the integrity of the packet that was transmitted. That is, if a bit error occurred, the computation of the ICV at the receiver over received data would not match the transmitted ICV. While ICVs in the form of CRCs have been used for decades, they do not prevent a man in the middle attack. That is, because the CRC-32 is linear it is possible for a third party to intercept packets, flip bits in the data field and the ICV and retransmit the packet with the receiver none the wiser. Although perhaps farfetched, this represents another type of attack we will discuss in this chapter.

4.1.3 The naked default

As briefly mentioned earlier, by default most vendors disable WEP, leaving it for the end-user to enable security. During the past year this author worked with products from seven different vendors. Six of those products by default set WEP to a disabled status, while one product forced users accessing its gateway with a client station to enable WEP. While this author's observations do not represent a full survey of all products, it does match what has been reported in many trade publications.

To obtain an appreciation of the reason why it is easy to accept default settings, let's examine a series of screen images associated with the setup of the Agere System's Orinoco wireless LAN client. Although this author is using the Orinoco client, similar results can be obtained through the use of other vendor products.

Figure 4.2 illustrates the first screen in a series of screen displays that can be generated when a person either initially configures an Orinoco wireless LAN client or wishes to change an existing configuration. Similar to other products, you can configure up to four profiles, with a default profile shown providing access from the client to an access point. Other options include peer-to-peer networking and access to an Orinoco Residential Gateway.

If you simply accept the default setting on the initial configuration screen you will be communicating in the clear. Since the proof of the pudding is in

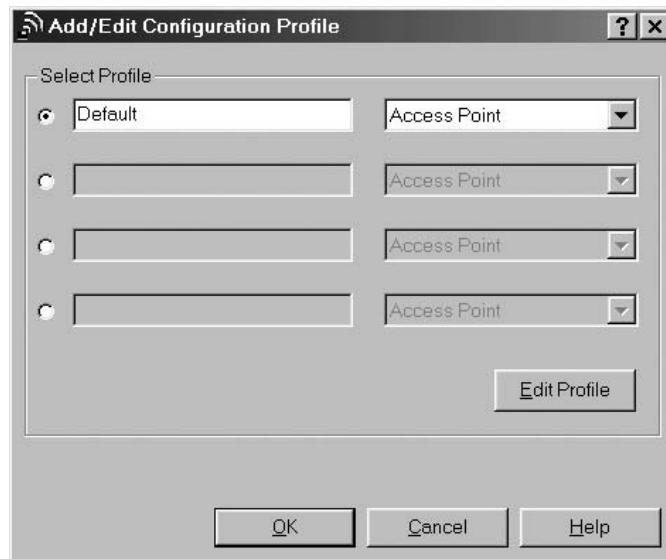


Figure 4.2 The initial Agere Systems Orinoco wireless LAN client configuration screen permits up to four profiles to be defined.

the eating, let's click on the button labeled 'Edit Profile' instead of the OK button and view how you can use the Agere Systems client manager software to set up its various options.

Selecting the Edit Profile button in Figure 4.2 results in the display of an Edit Configuration screen that has four tabs. Figure 4.3 illustrates the Edit Configuration screen with the Basic tab in the foreground. The Basic tab permits a user to enter a network name associated with an access point. By default the network name is blank, which in actuality represents one of two settings that enables a user's wireless LAN client to complete the association process with an access point without having to know the name assigned to the AP. The other setting is the network name of 'any' which enables a client wireless LAN to connect to an access point without prior knowledge of the network name assigned to the AP. As we will note in Chapter 5, these two settings make the use of the network name as a password very insecure.

Because the key focus of our concern is on the WEP, let's click on the tab labeled 'Encryption' to observe the default setting associated with the Agere Systems wireless LAN client station. Figure 4.4 illustrates the positioning of the Encryption tab to the front of the Edit Configuration dialog box. In examining Figure 4.4 note the box to the left of the label 'Enable Data

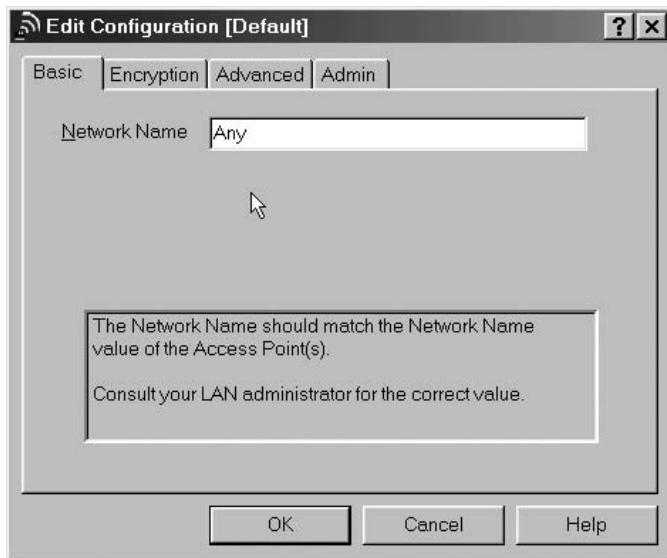


Figure 4.3 Configuring a blank or the network name of ‘any’ permits a client station to associate with an access point without having to know the name assigned to the AP.



Figure 4.4 The Orinoco Encryption tab permits up to four keys to be configured for use. If not edited, the default of no encryption is used.

Security,' which is shown as not selected. This is the default setting, which results in a station literally being naked, as its transmission is not encrypted. To select WEP encryption you would have to select the previously mentioned box that would then enable you to select one or more keys for configuration and enter values for each key. As previously noted when we reviewed the IV shown in Figure 4.1, the IV contains a 2 bit Key ID subfield which enables up to four keys to be defined. Thus, once you select the box to the left of the 'Enable Data Security' label you obtain the capability to define values for up to four WEP keys. In doing so you can either enter alphanumeric or hexadecimal characters. In comparison, some vendors permit a passphrase to be used, a technique we will examine later in this book.

Based upon our examination of the default security settings for Agere Orinoco hardware, we need to note two important items. First, the network name offers no protection since it can be overridden by the use of a blank or the keyword 'any'. Secondly, Agere is similar to many other vendors in that its default security setting results in encryption being disabled.

4.1.4 WEP key limitations

Under the IEEE 802.11 standard it is left to the implementer to determine how often to change the secret WEP key. Due to this, most WEP keys have a relatively long life, which can range from weeks to months or years, depending upon the operating procedure of the organization implementing and operating the wireless LAN.

Two additional WEP key limitations are the key length and the fact that initially no hardware manufacturers supported dynamic keys. Concerning key length, the 40 bit key represents a weak key that is used it was exportable under U.S. Government export laws then in place when the IEEE 802.11 standard was developed. Concerning the ability for keys to be dynamically changed, initial versions of wireless LAN hardware only supported static keys that had to be changed manually. This lack of dynamic key support almost ensures keys are rarely changed, which provides an unauthorized third party with the ability to capture IV collisions and the encrypted packets for a frequency analysis that only works if the same key is used.

Now that we have an appreciation of why the default settings of most wireless LAN products literally leave us naked, let's turn our attention to how easy it is for people to locate and observe wireless LAN activity. In doing so we will briefly examine the use of two readily available programs, one available as shareware while the second represents a commercial program.

4.2 Locating and observing wireless LAN traffic

In this section we look at the use of two programs that can be used to locate and monitor wireless LAN traffic. The first program we will examine is the Network Stumbler authored by Marius Milner (mariusm@pacbell.net) which literally sniffs the air looking for wireless LAN activity. The second program is AiroPeek, a commercial program from WildPackets of Walnut Creek, CA that provides a sophisticated network monitoring and traffic decoding capability.

4.2.1 Network stumbler

Network Stumbler, as its name implies, provides a user with the ability to stumble upon wireless LANs. The version used by this author was restricted to working with network interface cards that use the Hermes chipset, such as the Agere Orinoco, Dell True Mobile 1150 Series, Toshiba Wireless LAN card, Compaq WL110 and a few additional network cards.

4.2.1.1 Operation

Network Stumbler generates broadcast probes approximately once per second, reporting the responses received. If the program connects to a BSS network it will attempt to obtain the name of the access point. In comparison, if the program connects to an IBSS network it will attempt to obtain the names of all locally visible peers.

The version of Network Stumbler used by this author works actively instead of passively listening for beacon frames. Figure 4.5 illustrates the initial screen display of Network Stumbler, which within a brief period of time was able to locate an access point operating in this author's home. The program was operating on a Compaq Presario notebook equipped with an Agere Orinoco wireless LAN card positioned approximately 300 feet from this author's home. This explains how easy it is for someone to drive around office buildings or a residential area and locate wireless LAN access points.

4.2.1.2 Features

In addition to being able to note the presence of access points, Network Stumbler has several other features that warrant observation. First, Network Stumbler includes several built-in filters which enable the program user to selectively view access points with encryption off, encryption on, or those that are part of an ESS or IBSS. The left portion of Figure 4.6 illustrates the selection of the filter 'Encryption Off', which results in the display of those

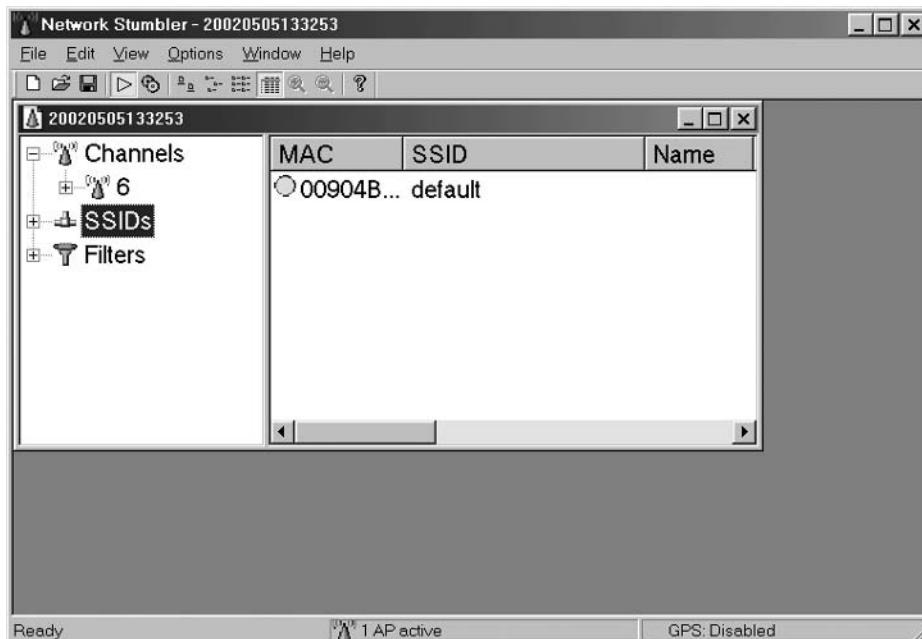


Figure 4.5 Using Network Stumbler to locate an access point operating on channel 6.

access points set in that manner. By moving the highlighted bar down over other filters you can display access points that meet the criteria of those filters.

A second series of features supported by the Network Stumbler program that warrant discussion can be viewed from the Options menu, which is shown pulled down at the top of Figure 4.6. Note the first entry (GPS) in the drop down menu, which is a bit obscured by the cursor arrow. This allows the program to interface Global Positioning System data to denote the locations of access points that are found.

Through the use of Network Stumbler and similar programs it becomes relatively easy to locate wireless LAN networks. In addition, through the use of the program's filtering capability you can locate unprotected networks that are not using encryption.

In discussing the use of Network Stumbler we note that it represents an active mechanism as the program transmits probe frames and records responses. You can also passively monitor for the presence of wireless LANs. To illustrate how easy this action is, this author will use AiroPeek, a product of WildPackets that is normally used to monitor, test and troubleshoot wireless LANs.

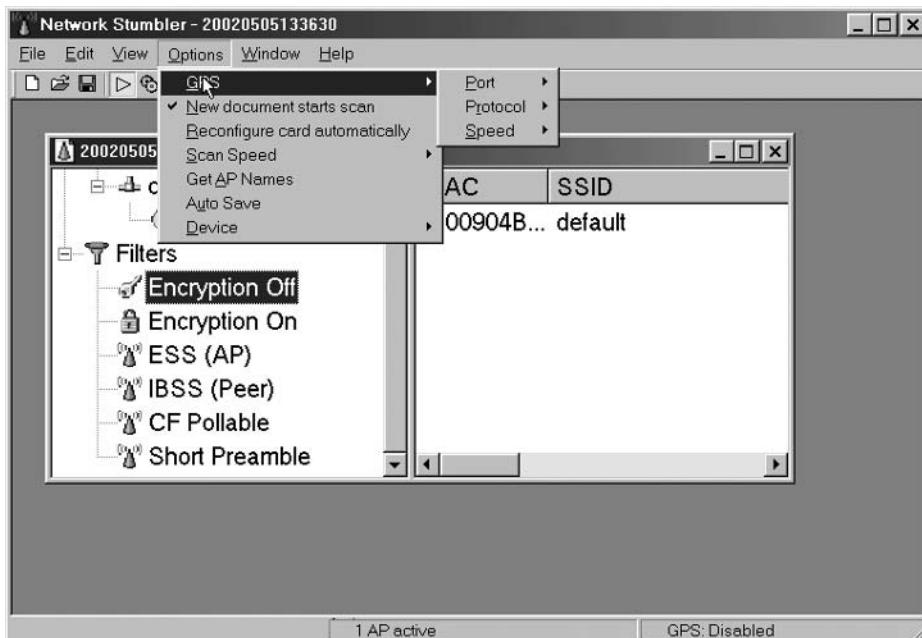


Figure 4.6 Through the use of Network Stumbler filters you can drill-in on access points operating without encryption.

4.2.2 Monitoring with AiroPeek

Figure 4.7 illustrates the use of AiroPeek to monitor beacon broadcasts generated by an access point installed in this author's home. At the time the screen capture occurred 52 packets were received and recorded by the notebook operating the program, of which the first 14 are shown in the upper window in the screen display.

4.2.2.1 Program Features

Below the window displaying the first 14 packets that were captured you will note a series of tabs commencing with 'packets' shown highlighted, followed by 'nodes' and so on. Once you capture packets, the program provides you with the ability to analyze the captured data by clicking on a particular tab or selecting an entry from the statistics menu. Because the focus of this book is upon wireless LAN security and this chapter in particular is concerned with WEP, we will use AiroPeek to illustrate the ease of locating and decoding wireless LAN traffic and not investigate its other features.

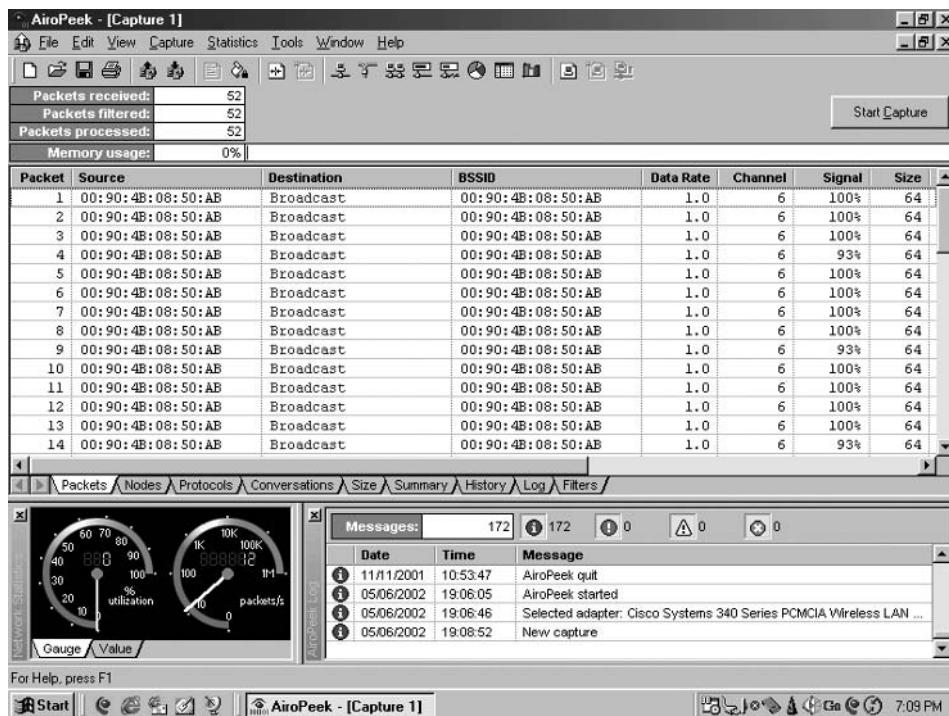


Figure 4.7 Using WildPackets AiroPeek to monitor broadcast frames generated by an access point.

4.2.2.2 Monitoring Network Traffic

Returning to our analysis of captured packets shown in Figure 4.7, if you examine the source and BSSID column entries you will note they are similar for all packets. This resulted from the fact that the access point used by the author uses its MAC address as the Basic Service Set ID or network name. Because no client stations were active, AiroPeek simply recorded broadcasts generated by the access point. Continuing our examination of the entries in the upper window portion of the display in Figure 4.7, note the data rate for each broadcast is shown as 1.0 Mbps. Even though the beacon frames were broadcast by an IEEE 802.11b compatible access point, all broadcasts commence at a data rate of 1 Mbps. This indicates that beacon frames can be observed and monitored at relatively long distances since the transmission distance is inversely proportional to the operating rate of an access point. This also means an unauthorized third party can first note the presence of

wireless LANs from a distance and then close the distance to monitor and record network activity occurring at higher data rates.

4.2.2.3 Packet Decoding

One of the features of AiroPeek that goes beyond Network Stumbler is a packet decoding capability. To decode a packet you can simply double-click on one of the packets shown in the window at the top portion of Figure 4.7. Figure 4.8 illustrates the packet decode when packet 3 was selected from Figure 4.7. Note that the decode is shown in the upper window. Concerning the packet decode, the first seven entries (flags through signal level) represent preliminary information about the packet and are not actually part of the packet. The actual packet decoding begins below the entry 802.11 MAC Header with the version subfield shown having a value of 0. This is followed by the program showing that the type of frame is a management frame while

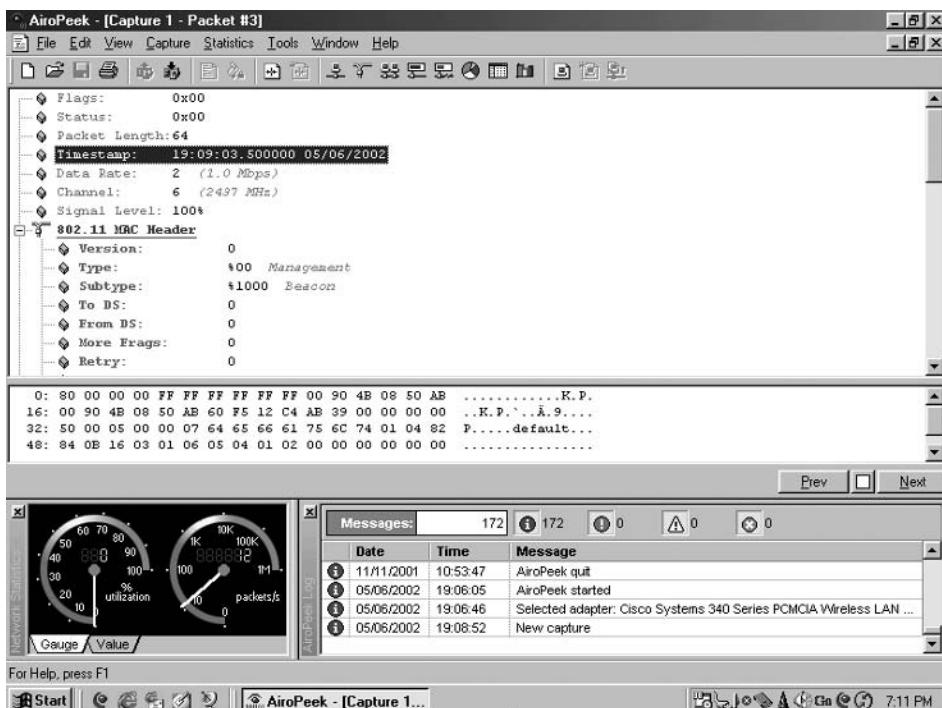


Figure 4.8 The initial portion of the decoding of packet 3 using WildPackets AiroPeek.

its subtype is a beacon. Since this beacon flows directly from an access point, the ToDS and FromDS fields as well as the More Frags fields are each set to a value of 0.

To view additional information about the packet that was decoded requires you to scroll down the window. Figure 4.9 illustrates a display of a continuation of the packet decode previously shown in Figure 4.8. If you examine the fourth entry from the top you will note that the setting for WEP is 0, which indicates that the access point broadcasting beacons has security disabled. The remainder of the decode provides additional information about the beacon frame that indicates how easy it is to record over the air transmissions with a laptop or notebook operating this commercially available program. Thus, it is important to note that it is a relatively simple process for an unauthorized third party to locate wireless LANs. Because the focus of this chapter is upon WEP, we will leave it for subsequent chapters to examine how wireless LAN traffic can be decoded and passwords and other valuable information

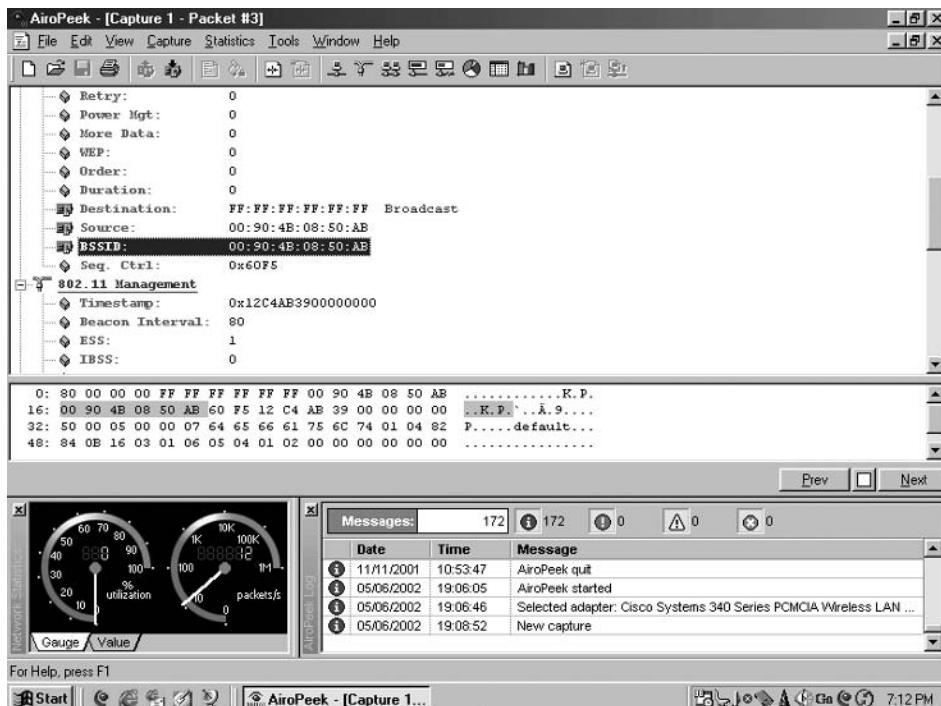


Figure 4.9 Continuing an examination of the decode of a previously captured broadcast beacon frame using WildPackets AiroPeek.

gathered by unauthorized people. Instead, let's continue our examination of WEP by focusing upon the symmetric stream cipher algorithm used by WEP, RC4.

4.3 RC4

RC4 represents a symmetric stream cipher algorithm developed by Ronald Rivest in 1987. Rivest is one of the three founders of RSA Data Security and details of the RC4 algorithm remained secret until 1994 when information about the algorithm was posted on the Internet. The 'RC' according to legend stands for 'Ron's Code' and RC4 was the fourth in a series of stream ciphers he developed.

Through the use of the Internet RC4 was posted to the Cypherpunks mailing list. Thereafter, it rapidly spread to ftp sites and Web servers. Although RSA Data Security attempted to claim it was still a trade secret, its publication and dissemination was counter-productive. Since its 1994 posting RC4 has been distributed at conferences, coded using numerous computer languages, and is readily available from many Internet sites.

4.3.1 Overview

RC4 is a variable key length stream cipher with byte-oriented operations. As a refresher, a stream cipher uses a key to generate an infinite pseudo-random number sequence. RC4 supports the use of a variable length key from 1 to 256 bytes in length, which is used to initialize a 256 byte state table formed from an 8 by 8 S-box: $S_0, S_1 \dots S_{255}$. The state table (S box) is then used to generate pseudo-random bytes, which form a pseudo-random byte stream. That byte stream is then XORed with the plaintext to generate ciphertext.

The length of the RC4 key is often limited to 40 bits due to U.S. Government export restrictions in place when the cipher algorithm was developed. The initial WEP key, as well as the exportable version of Netscape's Secure Socket Layer (SSL), use the 40 bit version of RC4, referred to as RC4-40. The 40 bit RC4 key used in the exportable version of Netscape's SSL was broken by several independent groups during 1996. At that time breaking the key required approximately 8 days; however, advances in processing power have significantly reduced the time necessary to break the algorithm. In spite of the above, the RC4 algorithm is used in many commercial products including Lotus Notes and Oracle Secure SQL. Part of its popularity results from the fact that encryption is relatively fast and the algorithm is easy to implement.

4.3.2 Operation

The RC4 algorithm uses 256 bytes of memory to form an array referred to as an S box ranging from the element $S[0]$ through element $S[255]$. RC4 operates in two phases, referred to as key setup and ciphering. During the key setup process the encryption key is used to generate an encrypting variable using the S box array, a key array and n mixing operations, where n references the length of the encryption key. Mixing operations include the swapping of bytes and modulo operations.

The initialization of the S box occurs by setting each of its 256 entries from a value of 0 to 255, in order, using the following pseudo code:

```
for i = 0 to 255;
    S[i] = i
endfor;
```

Once the S box is initialized you need to fill a second array with the key. This array is also a 256 element array. Because the key length can be smaller than the number of elements in the key array, you would repeat the key as necessary to fill the array $K_0, K_1 \dots K_{255}$. For example, assume the key is hex 391AC3OCBA or 5 bytes representing an exportable 40 bit key. K_0 would then be set to 39, K_1 to 1A, K_2 to C3, K_3 to OC and K_4 to BA. Then, the key would be reused to fill the K array, with K_5 set to 39, K_6 set to 1A and so on.

Once the S box and K arrays are initialized you need to obtain a starting position. In doing so you would use the following pseudo code:

```
j = 0;
for i = 0 to 255;
    j = (j + S[i] + K [i Mod Key length]) Mod 256
    swap S[i], S[j]
endfor;
```

Note that the preceding code generates encrypting variables using the S and K arrays and then shuffles or mixes S array bytes. The use of the i counter ensures that every element changes while the use of the j counter results in elements changing randomly. Once an encrypting variable is produced, it is XORed with a plaintext character to create an encrypted character. From the preceding code you can also note that no two passwords will mix in the same way, since the current operation is related to all previous swap operations.

4.3.3 Illustrative example

To illustrate the key setup process, let's use a 4 bit key for simplification and observe the operation of a 4 byte S box array consisting of the elements S_0 through S_3 . Initializing the S box results in the values 0, 1, 2 and 3 assigned to S_0 , S_1 , S_2 , and S_3 , respectively. Next, let's assume we used a 4 byte key array. We would then need to compare the key length to the number of elements in the key array and repeat the key to fill the K array. For example, if we used the key 15, we would repeat it obtaining 1515 to set the 4 elements in our abbreviated K array. Thus, we would now have the following values initialized for the S and K arrays.

$$\begin{array}{ll} S[0] = 0 & K[0] = 1 \\ S[1] = 1 & K[1] = 5 \\ S[2] = 2 & K[2] = 1 \\ S[3] = 3 & K[3] = 5 \end{array}$$

The mixing operations associated with our abbreviated example become iterations of the formula $(j + S_i + K_i) \text{ Mod } 4$, followed by swapping S_i with S_j . For the first iteration we obtain:

For $i = 0$

$$j = (0 + 0 + 1) \text{ Mod } 4 = 1$$

Swapping S_0 and S_1 we obtain:

$$\begin{array}{l} S[0] = 1 \\ S[1] = 0 \\ S[2] = 2 \\ S[3] = 3 \end{array}$$

For the second iteration we obtain:

For $i = 1$

$$j = (1 + 0 + 5) \text{ Mod } 4 = 2$$

Swapping S_1 and S_0 we obtain:

$$\begin{array}{l} S[0] = 0 \\ S[1] = 1 \end{array}$$

$$S[2] = 2$$

$$S[3] = 3$$

For the third iteration we obtain:

For $i = 2$

$$j = (2 + 2 + 1) \text{ Mod } 4 = 1$$

Swapping S_2 and S_3 we obtain:

$$S[0] = 0$$

$$S[1] = 1$$

$$S[2] = 3$$

$$S[3] = 2$$

For the fourth iteration we obtain:

For $i = 3$

$$j = (1 + 2 + 5) \text{ Mod } 4 = 0$$

Swapping S_3 and S_2 we now obtain:

$$S[0] = 0$$

$$S[1] = 1$$

$$S[2] = 2$$

$$S[3] = 3$$

To obtain a random byte for encryption we would first reinitialize i and j to 0. Then, we would set i equal to $(i + 1)$ and set j equal to $(j + S_i)$ Mod 4. We would then swap S_i and S_j and set K equal to $(S_i + S_j)$ Mod 4 to obtain the random byte for encryption. Following the above steps we obtain:

$$i = (i + 1) \text{ Mod } 4 \text{ or}$$

$$i = (0 + 1) \text{ Mod } 4 = 1$$

Then,

$$j = (j + S[i]) \text{ Mod } 4 \text{ or}$$

$$j = (0 + 1) \text{ Mod } 4 = 1$$

Swapping S_1 and S_2 we obtain:

$$S[0] = 1$$

$$S[1] = 0$$

$$S[2] = 2$$

$$S[3] = 3$$

To determine the random byte for encryption K , we need to compute $(S[i] + S[0]) \text{ Mod } 4$. Doing so we obtain:

$$K = (S[i] + S[0]) \text{ Mod } 4$$

$$K = (0 + 1) \text{ Mod } 4 = 1$$

Then, a binary vale of 1 (00000001), which represents the encrypting byte, is XORed with the plaintext to create a ciphertext or encrypted byte. For example, assume the plaintext byte was uppercase A which has the binary value 01000001. Then, the XOR operation and resulting encrypted character is generated as:

Plaintext byte	01000001
Encrypting byte	00000001
<hr/>	<hr/>
XOR operation produces encrypted byte	01000000

The complete RC4 algorithm, used to generated pseudo-random bytes that are used to encrypt or decrypt data, is shown in pseudo-code in Figure 4.10.

```

for i = 0 to 255;
    S[i] = i
endfor;
j = 0;
for i = 0 to 255;
    j = (j + S[i]) to K [i Mod Key length] Mod 256
    swap S[i], S[j]
endfor;
i = 0;
j = 0;
Loop until entire message encrypted/decrypted
    i = (i + 1) Mod256
    j = (j + S[i]) Mod 256
    swap S[i], S[j]
    K = (S[i] = S[j]) Mod 256
    output XOR of K and next byte of input

```

Figure 4.10 RC4 Pseudo-code for generating encrypting and decrypting bytes.

4.3.4 Strengths and weaknesses

Like any encryption algorithm, RC4 has strengths and weaknesses. Its strengths include the random nature of S box changes, which makes it difficult to locate a value in its table. Through the use of a 256 byte internal key, an S box RC4 can be in $256! \times 256^2$ possible states, which represents quite a large number, making an attack on its table structure very difficult. Another strength is the fact that it uses a few simple loops and swapping of bytes, making it extremely fast.

Although RC4 has been used in many commercial cryptograph products, it has several weaknesses. First, a short key length means that the pseudo-random generator will repeat, which permits passive monitoring to gather data that can be statistically analyzed. Secondly, the RC4 algorithm has what is referred to as weak keys. A weak key is a key that results in generated bytes being strongly correlated with a few bytes from the key, which opens up intercepted data to analysis. According to several reports, one in every 256 keys can be considered to represent a weak key.

4.4 WEP weakness

Over the past few years a number of papers were published denoting significant weaknesses in WEP. In addition, several programs were developed and placed on the Internet that are available for use to recover WEP keys. In this section we will review the findings of some of those papers and the programs that can be used to recover WEP keys from simply passively recording encrypted communications. This information will provide us with the rationale for not depending upon conventional WEP as defined under the IEEE 802.11 standard and it's a and b extensions. When referring to WEP it should be noted that unless specified otherwise, weaknesses reference the 64 bit and 128 bit WEP keys, with the latter sometimes referred to as WEP II or WEP 2.0.

4.4.1 Unsafe at any size

One of the first people to identify some of the problems associated with WEP was Jesse R. Walker of Intel Corporation. In October 2000 Walker published a paper titled 'Unsafe at Any Key Size: An Analysis of WEP Encapsulation' as IEEE document 802.11-00/362. In his paper Mr. Walker pointed out that at the time the prevailing notion that WEP was insecure due to the use of a 40 bit key was not correct. Instead, WEP was insecure regardless of the length of the key used.

In Mr. Walker's paper he reviewed WEP and pointed out the weakness of a 24 bit IV. In addition to the length of the IV being of concern, his paper noted that the standard has no IV avoidance algorithm. This means that one node can reuse an IV already used by another node, which enhances the probability of IV collisions. After describing how an attacker could construct a table of key streams for each IV to compromise privacy, the paper focused upon the use of RC4. According to Mr. Walker, the deficiency of the WEP encapsulation design results from adapting RC4 to an environment for which it is poorly suited. This results from the fact that one in every 256 RC4 keys is 'weak' and makes it easier to crypto-analyze encrypted data.

While the problem with RC4 was mentioned by other people, the major focus of the Walker paper that appears to have been of key interest to security conscious people was his analysis of the IV. Walker pointed out that there is a 50 percent chance of an IV collision after only 4823 (2^{12}) frames, with the probability of a collision increasing to 99 percent after 12, 430 frames or in a few seconds of normal traffic at 11 Mbps. While the Walker paper made several recommendations for new WEP encapsulation to include a 128 bit IV, his recommendations were unfortunately not implemented at a point in time where there were a limited number of wireless LAN products on the market. However, his paper can be considered to represent a catalyst that resulted in additional research concerning the vulnerability of WEP. One subsequent paper that warrants discussion was published by researchers at the University of California at Berkeley.

4.4.2 The insecurity of 802.11

One of the first papers to be published that exposed a series of WEP weaknesses was titled 'Intercepting Mobile Communications: The Insecurity of 802.11' authored by Nikita Borisov, Ian Goldberg and David Wagner at the University of California, Berkeley. Published in January 2001 this paper analyzed WEP and determined that it was susceptible to both passive and active attacks.

4.4.2.1 Passive Monitoring

The first attack the paper discussed concerned passive monitoring of network traffic until an IV collision occurs. When this situation occurs an attacker can XOR two packets with the same IV to infer data about the contents of the two messages. The basis for the ability to infer information results from the fact that IP traffic is very predictable, since it commences with an IP header for which many fields have static values. If an insufficient amount of data is

obtained from two messages a passive attacker could simply record additional data until the IV repeats.

As a review of previously presented information, the IV is a 24 bit field which is transmitted in the cleartext part of the message and is used as a seed with the secret key to generate a pseudo-random number sequence. That sequence is XORed with the data to produce ciphertext that represents encrypted data.

You can determine the frequency or duration at which random generated IVs repeat via the use of the following formula:

$$\frac{\text{Avg Frame Length}}{\text{Avg Data Transfer Rate (Mbps)}} \times \frac{8 \text{ bits}}{\text{byte}} \times 2^{24} \text{ IV combinations}$$

If we assume an average frame length of 1500 bytes and a data transfer rate of 11 Mbps, we obtain an IV repetition duration of:

$$\frac{1500 \text{ bytes} \times 8 \text{ bits/byte} \times 16772216}{11000000} = 18302 \text{ sec}$$

The above is equivalent to 305 minutes or slightly more than five hours.

If the wireless LAN is used for a mixture of activities the average frame length will more than likely be under 1500 bytes. To illustrate the effect of a reduction in frame length upon the IV repetition time, let's assume an average frame length of 1000 bytes. Then, the repetition time would become $1000/1500$ or 2/3rds of the repetition rate when the average frame length is 1500 bytes or 3.38 hours. Thus, as the average frame length decreases the frequency of IV collisions increases. To make matters worse, the IEEE 802.11 standard specifies that changing the IV with the transmission of each packet is optional, which could result in contiguous collisions. In addition, some hardware vendors reset the IV to 0 each time a wireless LAN adapter is initialized, which can significantly increase collisions in a dynamic wireless LAN environment where people frequently join and leave the network.

To illustrate the vulnerability associated with capturing a sequence of packets with the same IV, consider monitoring four captured packets where the IV value was the same for each of the packets passively monitored. If these packets were transporting IP datagrams, the first field would be the 4 bit Version field, followed by a 4 bit header length field, an 8 bit Type of Service (TOS) field and so on. Because all clients are more than likely operating IPv4, the encryption for each version field based upon the use of the same IV will result in the same encrypted value. Thus, if you were a crypto-analyst you could begin to determine how the pseudo-random number generator operates

and note how it is used to encrypt data. In doing so it also becomes possible to perform a statistical analysis of encrypted traffic that can be used to decrypt the captured enciphered data. Thus, the repetition of IVs represents a weakness in 802.11 security which could be exploited.

While a repetition duration of hours might appear to deter an unauthorized third party from sitting in a van located in a Silicon Valley parking lot, that repetition duration assumes one client talking to an access point with IVs selected randomly so they repeat in a best case scenario. Based upon the previously mentioned paper authored by Walker, the probability of IV collisions is quite high. In fact, because there is no IV collision avoidance mechanism, it can be expected that the larger the number of stations the quicker the possibility of IV collisions occurring. This means that a third party passively monitoring a large wireless LAN can collect a sufficient amount of packets with IV collisions to permit an analysis that will cause an understanding of the data transmitted over the network. While the Berkeley paper did not investigate key recovery, another paper did focus on this topic and found how a short period of passive monitoring could be used to reconstruct the WEP key.

4.4.2.2 Traffic Injection

A second type of attack noted in the paper authored by Borisov and companions concerns the ability of a third party to inject new traffic once they obtain knowledge of the plaintext for a single encrypted message. An even more insidious attack results from the fact that the ICV field is implemented as a CRC-32 checksum, which is linear. This means it is possible to compute the bit difference between two CRCs based upon the difference of the messages they protect. This also means that flipping bit n in a message results in a deterministic set of bits in the CRC that need to be flipped to generate a correct checksum on a modified message. According to the paper published at Berkeley, this also means it is possible to flip bits in a message and adjust the CRC to a correct value. This in turn means an attacker could intercept, modify and retransmit packets without causing an error at the receiver.

4.4.2.3 Tricking an Access Point

Because most access points provide a connection to a wired infrastructure that in turn is connected to the Internet, the Berkeley paper came up with a novel scheme for an active attack. Under this scheme an attacker would guess the destination IP address in a packet and flip appropriate bits to set the address to a computer on the Internet he or she controls. The packet would be

decrypted by the access point and forwarded in plaintext to the Internet to the computer operated by the third party. Needless to say, the third party would be able to build a matrix of encrypted and decrypted packets that correspond to one another. Those packets could be used as a mechanism for attempting to determine the pseudo-random number generator and the key used to generate the sequence.

4.4.2.4 Dictionary Attack

A fourth attack method described in the Berkeley paper involves a third party monitoring the wireless LAN throughout an extended period of time. By recording the IVs and associated encrypted text into a table it becomes possible to construct a decryption table. That table would enable a third party with knowledge of the plaintext for some packets to compute the RC4 key stream generated by an IV. This key stream could then be used to decrypt other packets that have the same IV. Using this technique a third party could construct a table of IVs and corresponding key streams. According to the paper, the table would require approximately 15 GB of data and once constructed would enable every packet transmitted to be decrypted.

4.4.2.5 Summary

The paper written at Berkeley discusses four possible attacks based upon weaknesses associated with WEP. Those weaknesses fall into three areas. The first weakness is the fact that the IV is only 24 bits in length, which means it repeats on a fairly regular basis. A second weakness is the fact that the WEP key is static. Taken together, this means that it is a relatively simple process to monitor IVs, capture repeating IVs and their encrypted packets and perform a statistical analysis to determine the pseudo-random number generator.

As we will note later in this book, the first two weaknesses can be countered by dynamically changing the WEP key. The third vulnerable area concerns the ability of a ‘man in the middle’ to intercept, alter and retransmit a packet. This vulnerability results from the linear relationship of packet data and the ICV. Because the ICV is created by the use of a 32 bit CRC that has the linear relationship to the data, this vulnerability can only be overcome if the packet is tunneled within a wrapper, a technique that requires encryption to occur at layer 3.

Both the paper authored by Walker and the Berkeley paper can be considered as thought provoking, as they raised the issue of WEP vulnerability to new heights. However, it wasn’t until the publication of the paper titled

'Weaknesses in the Key Scheduling Algorithm of RC4' that information was published which provided the tools for attacking WEP. In the remainder of this chapter we will review this paper and then examine how the information contained in it was used to recover WEP keys via passive monitoring.

4.4.3 Exploiting RC4 weakness

After the above-mentioned paper was published at Berkeley several researchers published papers concerning the weakness of the IV. Other papers noted a problem in the algorithm some vendors use to generate WEP keys. While such documents provided a service in making people aware of the vulnerability of WEP, it wasn't until the publication of the paper titled 'Weakness in the Key Scheduling Algorithm of RC4' by Fluhrer, Mantin and Shamir in August 2001 that a blueprint for breaking WEP in the form of an attack on RC4 occurred. This paper noted that it was possible to passively capture approximately 4 million packets to recover the encryption key. At a data rate of 11 Mbps and an average packet length of 1 Kbytes, it would require approximately 3000 seconds or slightly under one hour to obtain a sufficient database to recover the WEP key.

A key (no pun intended) finding of the paper is the fact that the Key Scheduling Algorithm (KSA) used by RC4 has two significant weaknesses. First, the KSA results in a large class of weak keys in which a small portion of the secret key determines a large number of the initial permutations of the KSA output. Secondly, and related to the first weakness, the pseudo-random generation algorithm built into RC4 translates patterns in the initial permutation into patterns at the beginning of the output stream. Thus, the initial output of weak keys are disproportionately affected by a small number of key bits. Using this information the paper shows how a small number of key bits is sufficient to completely determine a large number of bits in the output stream. The paper also discusses how the concatenation of the IV to the secret key acts as a literal door in determining the secret key. This results from the fact that when the same secret key is used with different IVs, an attacker only needs to obtain the first word of RC4 output for each IV used to reconstruct the secret key. In doing so the attacker must guess the first word; however, because it is often easily guessed, especially when it represents an IP header, a minimum amount of effort can recover the secret key. While this paper can be considered as providing a roadmap for WEP key recovery, it did not actually recover any keys. The actual implementation of the findings of this paper occurred less than a month after its publication.

4.4.4 Breaking WEP

The proverbial ‘straw that broke the camel’s back’ concerning the security of WEP occurred in August 2001 at Rice University and AT&T Labs in Forham Park, NJ. Using information from the Fluhrer, Mantin and Shamir paper, Adam Stubblefield, John Ioannidis and Aviel Rubin implemented a method to recover the 128 bit key of an IEEE 802.11b LAN through a passive attack. In the paper appropriately titled ‘Using the Fluhrer, Mantin and Shamir Attack to Break WEP,’ the authors first presented an overview of the WEP protocol and explained how the attack proposed by Fluhrer, Mantin and Shamir would be applied to WEP. In doing so this new paper mounted its attack by searching for IVs that place the RC4 key setup algorithm into a condition which leaks information about the key.

According to this paper the authors first created a simulation of the RC4 attack. In doing so they noted that they were able to recover the full key once they obtained 256 probable resolved cases. Here the term ‘resolved’ referenced IVs that place the key setup algorithm into a state that leaks information about the key. Using a \$100 Linksys wireless LAN card and a Linux driver with a modified version of the Ethereal network monitoring program, they captured raw WEP encrypted packets that were then used to form a database for their attack. In performing the actual attack they noted that an 802.2 encapsulation header is prefixed to both ARP and IP traffic. Because the first plaintext byte is set to hex AA, which represents the designation of a subnetwork access protocol (SNAP) frame, this makes guessing a relatively simple event. In fact, if IPX was transported one would then use the pseudo-checksum value in the NetWare header which is hex FF instead of hex AA. Because IP and IPX are the predominant protocols in use, guessing the composition of a plaintext byte is a relatively simple process.

In the referenced paper two attack methods were discussed. The first method was an outline of how a so-call ‘naïve’ or basic attack on WEP could occur. Under this method for each packet a computer would compare the use of pseudo-random sequences generated by different keys to recover the guessed value. According to the paper they found that between 5,000,000 and 6,000,000 packets would be required to determine the secret key, instead of the 4,000,000 packets postulated in the Fluhrer, Mantin and Shamir paper.

To improve the basic attack, the authors of this paper investigated the use of a user memorable passphrase instead of a string of hex digits for the secret key creation. In doing so the authors were able to determine if each key byte that could be part of a passphrase corresponded to an ASCII letter, number or punctuation character. This considerably improved the WEP attack, reducing

the number of packets required to recover a 128 bit secret key to between 1,000,000 and 2,000,000 packets.

The Stubblefield, Ioannidis and Rubin paper contained coding for two WEP attacks that could be implemented to recover the secret key being used. Both attack methods involve the passive monitoring of a wireless LAN and require a database of either 5,000,000 to 6,000,000 or 1,000,000 to 2,000,000 packets to be captured. For either attack method to work, the WEP key must remain constant over the captured database and information at the beginning of the encrypted data within the captured packets must be able to be guessed.

Recognizing the fact that they can control the frequency of secret key changes, many wireless LAN equipment vendors tackled this security hole by introducing support for dynamic key exchanges. As we will note in subsequent chapters, the use of dynamically changing WEP keys potentially closes the weakness of WEP and represents one method that can be used to secure your wireless LAN. However, since vendors handle dynamic key exchange differently with some products permitting the user to set the frequency at which key changes occur, it is quite possible to incorrectly configure a product that will make your network vulnerable to passive monitoring.

In concluding this chapter we will briefly look at two Internet available programs that can be used to recover WEP keys. While they can be used by hackers it should be noted that you can use them to test the vulnerability of your existing wireless LANs. Thus, they represent a network vulnerability analysis tool that you may wish to consider using.

4.4.5 AirSnort

AirSnort represents one of two popular wireless LAN tools that can be used to recover encryption keys. Like the work performed by Stubblefield, Ioannidis and Rubin, AirSnort operates by passively monitoring transmissions to build a database of encrypted packets which are used to recover the secret key.

AirSnort is available for downloading at <http://airsnort.shmoo.com/> and its home page is shown in Figure 4.11. According to data on its home page, AirSnort requires approximately 5,000,000 to 10,000,000 encrypted packets to be captured prior to the program being able to recover the secret key used for encryption. The program runs under the Linux operating system and can only be used with certain vendor specific wireless LAN adapter cards that are listed on the referenced URL. A second URL that is worth considering is <http://www-be-secure.com/airsnort.html>, which is listed on the Web as AirSnort Home. A version 2.0 of the program, available at this site, appears to support more wireless LAN adapter cards than the

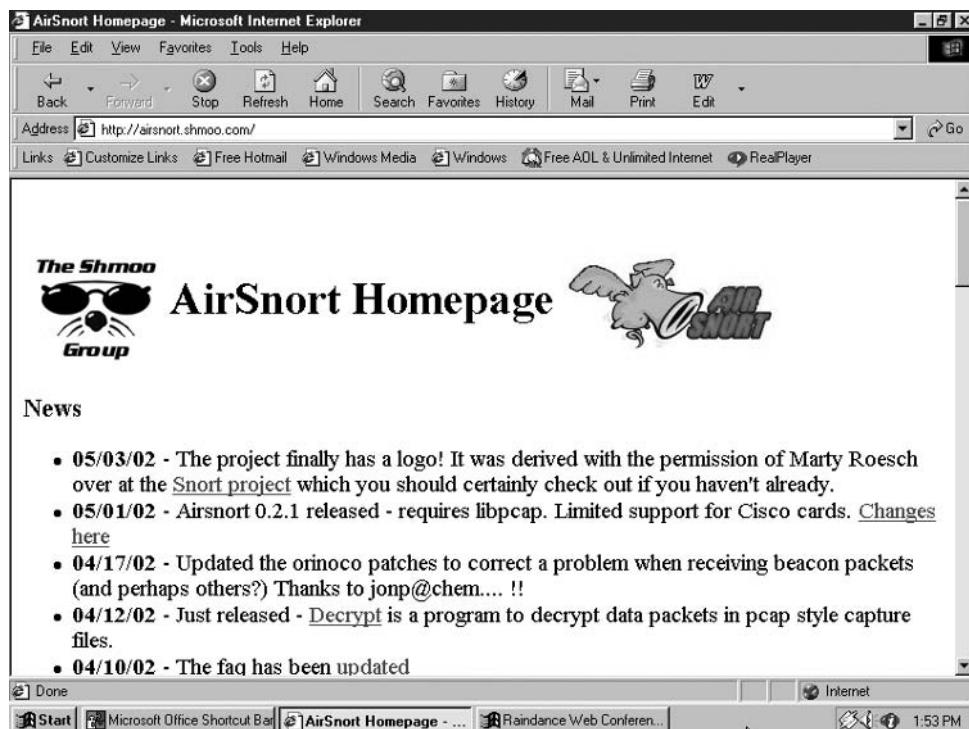


Figure 4.11 The AirSnort Homepage at <http://airsnort.shmoo.com/>.

AirSnort program available from the AirSnort Homepage previously shown in Figure 4.11.

4.4.6 WEPCrack

WEPCrack represents a second popular open source tool for recovering the secret key used in so-called secure 802.11 wireless LANs. WEPCrack was actually the first publicly available code for recovering secret keys, reaching the Web about a week prior to the release of AirSnort. WEPCrack can be obtained at <http://wepcrack.sourceforge.net> and consists of three Perl-based scripts. One script permits a simple emulation of IV/encrypted output and generator IV combinations that can be utilized to weaken the secret key used to encrypt traffic. The second script searches a database for IVs that match the pattern known to weaken secret keys and logs the first byte of encrypted output

and weak IVs into a log file. The third script uses collected data or data created by the first script to determine the secret key. According to information posted on the WEPCrack Web site, future enhancements of the program are expected to include a database of SSIDs and AP MACs for multiple IV collection and cracking, dynamic WEP determination, and a patch to the Ethereal program to enable the program to use a WEP key to decrypt WEP traffic.

chapter five

Security Risks and Countermeasures

Until now our examination of wireless LANs was primarily oriented towards obtaining an understanding of the technology and the rationale for their built-in security vulnerability in the form of WEP being weak. In this chapter we will look at the additional security risks associated with wireless LANs and potential countermeasures you can consider using to minimize such risks. While WEP represents a significant vulnerability, it is not the only risk a user of wireless LANs can face. Thus, the purpose of this chapter is to help you become acquainted with risks that go beyond the use of WEP.

Because listing and explaining security vulnerabilities by itself does not provide any indication of how to overcome existing limitations, we will also note countermeasures when appropriate. In doing so we will discuss techniques that can be used to overcome different wireless vulnerabilities and reference proprietary and standards based security methods that are more fully described in Chapters 6 and 7. Because the Service Set Identification (SSID) is considered by many to represent a password, it is a good starting point for discussing security risks.

5.1 The SSID

As discussed earlier, an IEEE 802.11 wireless LAN requires each client station to be configured to use the network name associated with the access point they wish to communicate with. The network name is more formally referred to as the Service Set Identification (SSID).

5.1.1 Overview

The SSID represents a unique identifier that is included in the header of wireless LAN packets when a client station attempts to join a Basic Service Set (BSS) via communicating with an access point that forms the service set. The actual role of the SSID is to provide wireless LAN commonality. That is, the SSID differentiates one wireless LAN from another, enabling a client station to connect to the appropriate access point that makes up the heart of a BSS. For example, assume two access points are located on the same floor in a building but support different groups of employees, such as accountants and engineers. Then, one SSID could be set to ‘accounting’ while the second could be set to ‘engineering’ to ensure employees use the applicable access point.

While each client station should be configured with the SSID of the particular access point that it wishes to communicate with, this is actually not always a necessity. As we will shortly note, there are three areas of concern that make the use of the SSID as a password meaningless, although it retains its value as a mechanism for clients accessing the correct access point when one is located in close proximity to another.

5.1.2 Overriding the SSID

There are two keywords you can use to easily override an SSID configured for use by an access point. First, you can configure a blank as the network name or SSID in your client station configuration. To illustrate the use of a blank SSID this author used a Cisco Aironet 340 series wireless LAN card to access an SMC Networks Barricade Broadband Wireless Router, the latter representing a combined router and access point. Figure 5.1 illustrates the display of the 340 series properties dialog box with the System Parameters tab in the foreground.

In examining the entries in the System Parameters tab, note that the client name shown as ‘MICRON’ represents the station name that would be displayed in the table of connected devices on a Cisco Access point. The use of station names instead of MAC addresses makes it easier to determine which devices are connected to a particular access point. Directly under the entry area for the client name are entry areas for up to three SSIDs. SSID2 and SSID3 are optional, and are for use if a person needs to roam between up to three distinct networks. As shown, entries for all three SSIDs are blank. If you examine the background of the display shown in Figure 5.1 you will note this author was accessing Yahoo Mail. This access was accomplished via the use of the Cisco 340 series wireless adapter card communicating with an SMC Networks Barricade broadband router, using a blank entry for the SSID when configuring

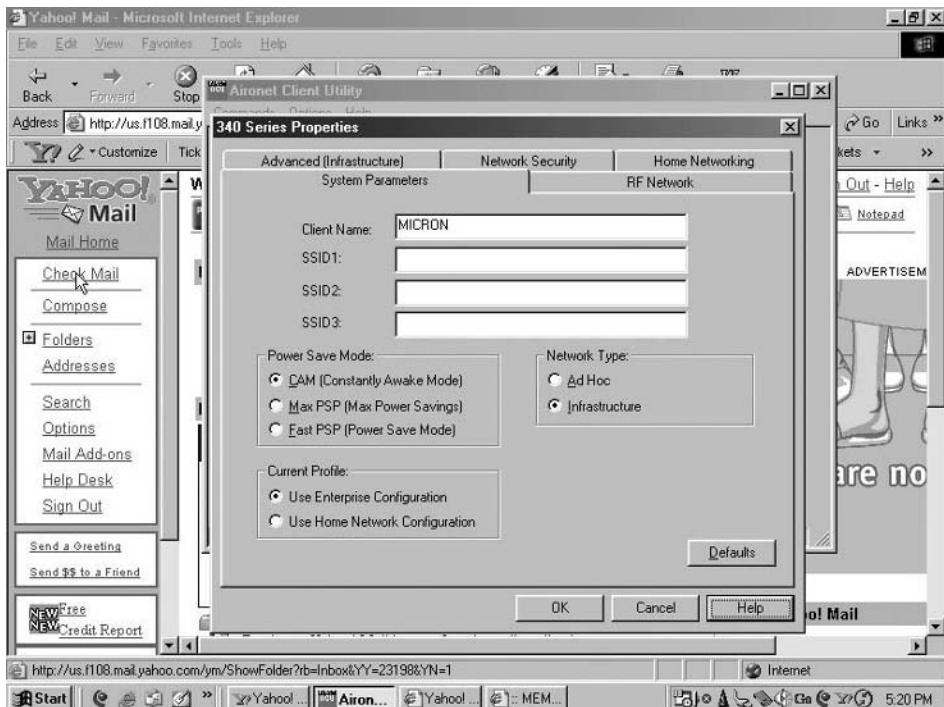


Figure 5.1 By leaving the SSID blank a Cisco 340 wireless LAN adapter is able to communicate with an access point with a configured network name.

the client station. Thus, Figure 5.1 illustrates the ease at which overriding an SSID can be accomplished.

As an alternative to the use of a blank SSID you can use the keyword 'any.' Either option results in the ability of the client station to communicate with an access point without requiring the client to be configured with a network name that matches the one used by the AP. The rationale for this override capability results from the need to obtain a mechanism for a client station to connect to a particular AP when the signals of two or more can be heard. This action provides a list of SSIDs on the client station, enabling the operator to select the applicable access point when more than one AP can be heard.

5.1.3 Obtaining the SSID

According to documentation read by this author, in addition to first hand configuration experience with some products, it is possible to configure many

access points to eliminate the SSID in beacon frames. While this action is supposed to enhance network security, there are two methods you can use (which can also be employed by an unauthorized third party) that can easily override a lack of prior knowledge of a network name or SSID. First, because the SSID flows in the clear, the client frames joining an AP can be monitored. Thus, removing the SSID in beacon frames does not eliminate the client side use of the network name. Secondly, most manufacturers of access points place their documentation on the Web. If you spend a few moments surfing different vendor sites you can easily make a list of default network names. You can then configure your client station with those names, observing if a particular network name provides the opening you require.

Even when an access point does not have a predefined default SSID other than a blank, it may have a ‘suggested’ value. For example, consider the Cisco AP Radio Identification Page partially illustrated in Figure 5.2. Cisco uses the keyword ‘tsunami’ in its publications on the Web to indicate an entry



Figure 5.2 From the Cisco Web site you can view access point documentation that indicates the use of tsunami as the Service Set ID (SSID).

for the SSID when configuring several of the vendor's access points. Because it is quite common for some network managers and LAN administrators to use values from vendor manuals, it is relatively easy to discover some Cisco access points configured to use tsunami as the SSID.

5.1.4 Countermeasures

There are several countermeasures we can place into effect to make the SSID more reliable as an elementary barrier to network access. However, prior to discussing those methods, it is important to remember that the SSID does not actually represent a password. Instead, its use is to enable client stations to associate with the correct access point when two or more APs are within radio frequency range. That said, let's take a look at several countermeasures.

While the SSID or network name is obviously an easy to defeat 'password,' you can make it more difficult for an unauthorized third party to access your network. To do so you can remove the SSID from beacon frames if your equipment supports its removal. In addition, where possible you should change the SSID from its default setting. While this is possible for most equipment, some access points appear to have been configured to always use the MAC address of the device as the network name. When this occurs, software will not allow the SSID to be changed.

Another countermeasure you can consider is similar to avoiding the use of default SSID values. This countermeasure involves avoiding 'suggested' SSID settings that appear in vendor literature. Although once again it is important to note that the SSID is not a password and its value can be monitored by considering one or more of the previously mentioned countermeasures, you can at least make it more difficult for an unauthorized third party to join your network.

5.2 Eavesdropping

The establishment of a wireless LAN within an office building or home results in walls providing a false sense of security. In this section we will examine the risk associated with eavesdropping and countermeasures we can consider to minimize this risk.

5.2.1 Overview

Although the transmission distance of wireless LANs is normally limited to hundreds of meters, this limitation is based upon the use of small antennas

built into PC Cards and other form factors used to create wireless network interface cards. When more sensitive antennas are used, it becomes possible to pick up the radio frequency transmission of wireless LANs at a considerable distance from their source. In fact, certain types of antennas with a very high level of directional sensitivity can be used to receive wireless LAN signals at distances of up to several miles. Because glass windows represent a poor shielding it is quite common for RF energy to literally 'leak' out of a building. This explains why, over the past few years, several articles appeared in *The New York Times*, *The Wall Street Journal* and other publications about the exploits of people who were able to monitor the transmission of in-building wireless LANs from parking lots located outside the buildings.

5.2.2 Threats

From previous chapters we noted there are several programs that can be obtained from the Internet which can reconstruct the WEP key in use if a sufficient number of frames are captured. For example, we discussed the use of AirSnort and Network Stumbler, two programs that can be employed to reconstruct WEP keys using a database of several million passively monitored and captured frames. It is also possible that an Internet search will very likely result in the location of additional programs that have a similar capability.

In addition to the use of software programs, we also noted that simply capturing several frames with the same Initialization Vector (IV) can enable a frequency analysis to be performed that could result in the contents of an encrypted frame to be decrypted. Because such attacks require the wireless LAN signal to be captured, several countermeasures worth noting are based upon obscuring the RF signals of the wireless LAN.

5.2.3 Countermeasures

Working upon the premise that one cannot decrypt a signal one cannot hear, a valuable countermeasure to eavesdropping that you can utilize is to obscure or hide RF signals from unauthorized third parties. To do so you can consider antenna positioning and the use of shielding. In Chapter 3 we noted that positioning an antenna along its vertical axis can result in minimizing radiation to floors above and below the location of an access point. While antenna positioning is important, it may also be possible to control the use of a particular antenna when your wireless LAN device supports antenna diversity. For example, consider Figure 5.3, which illustrates the display of the Advanced (Infrastructure) tab from the Cisco 340 Series Properties dialog box. Note that Cisco provides the 340 series wireless LAN adapter user to

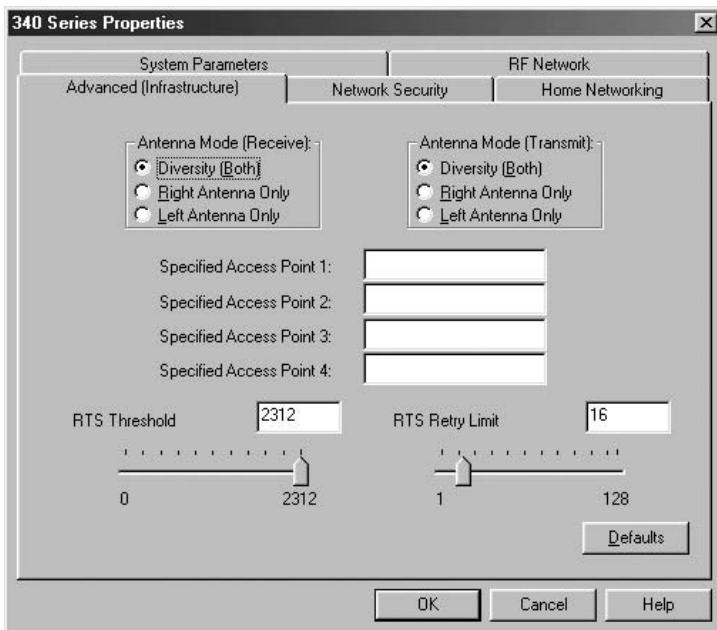


Figure 5.3 The Cisco 340 series configuration permits a user to specify the antenna or antennas to be used for both transmit and receive mode of operations.

select the use of diversity or the right or left antenna for both receive and transmit modes of operation. Thus, when using a product that supports an antenna diversity and antenna selection capability, you obtain the ability to control the antenna or antennas to be used in addition to their positioning. As well as controlling antennas, some access points provide you with the ability to control the transmit signal strength. By lowering the transmit signal strength, you can reduce the range of the RF signals generated by an access point.

In Chapter 3 we also noted that we could use a directional antenna and shielding to further reduce the possibility of an unauthorized third party being able to listen to the signals generated by one or more access points. Because the antennas built into PC Card wireless adapters have a relatively short range, you should primarily focus your efforts upon obscuring the RF signal of your access points. You can use a notebook computer with a sensitive directional antenna and signal strength monitoring software to observe the RF signals as you move about the office and its outside perimeter.

While most wireless LAN adapter cards are bundled with a utility program that can be used to observe signal strength and signal quality at a particular moment, some products also include a site survey capability. An example of a site survey capability is included with the Cisco 340 series wireless adapter card, with an example of the display of the site survey screen shown in Figure 5.4. The purpose of a site survey is to assist a wireless network designer in planning locations for the best placement of access points. In a Cisco environment a 340 series device reads the current status from the wireless adapter four times per second and displays bar graphs and digital indicators of the signal strength and signal quality. The Cisco 340 supports both active and passive operations, with a passive mode resulting in listening for RF network traffic while an active mode of operation results in the

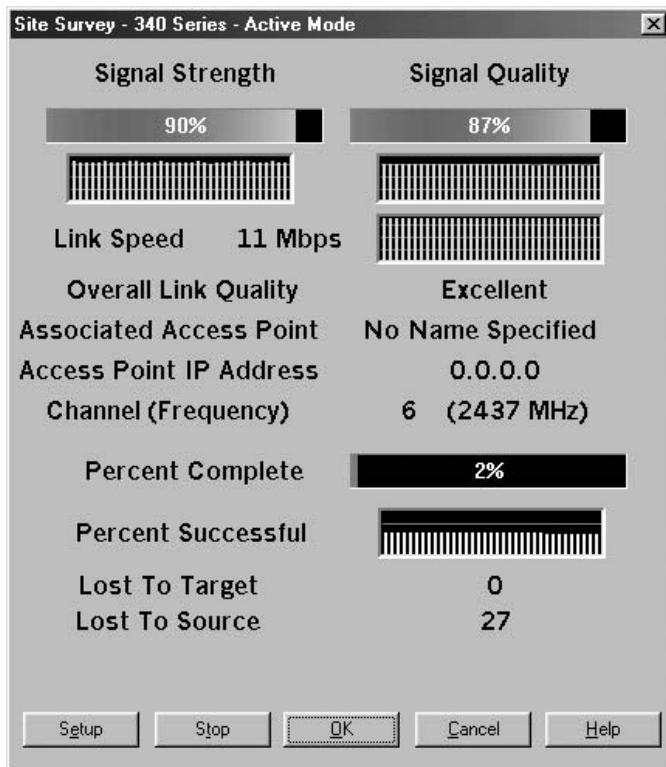


Figure 5.4 The site survey capability of Cisco wireless LAN adapters can be used to determine the quality and strength of RF signals at different locations inside and outside a building.

transmission and reception of frames to and from the associated access point. While you would normally look for a high level of link quality and signal strength when performing a site survey, if attempting to obscure RF signals to unwanted areas you would look for inverse settings. That is, you would focus your attention on the use of shielding, antenna positioning, transmit level strength and the use of one or two antennas to minimize RF signals to areas outside the physical control of your organization, such as to other floors in a building or to the parking lot.

Cisco equipment is similar to other vendor products in that various numeric values for link quality and signal strength are combined and equated to English rating designators. In a Cisco environment, overall link quality provides an indication of a wireless LAN adapter to successfully communicate with an access point and is derived from the current signal strength and current signal quality. When both values exceed 75 percent the overall link quality is considered excellent. If both values exceed 40 percent but one or both are less than 75 percent, the overall link quality is considered good. When both values are greater than 20 percent but one or both less than 40 percent, the overall link quality is fair. The last English rating is poor, which occurs when one or both values are less than 20 percent.

5.3 Masquerade

If a third party can eavesdrop on your wireless LAN communications it becomes possible for that party to pretend to be a legitimate user of the network. Masquerade can be very dangerous as it provides a literal ‘open door’ to your network resources.

5.3.1 Overview

The ability of an unauthorized third party to masquerade as a legitimate user of a wireless network can range from being a very simple to a complex undertaking, with the degree of complexity based upon the security in effect. If your organization’s wireless LAN does not employ any security it becomes a relatively simple process for an unauthorized third party to determine the SSID in use by an access point and gain access to your organization’s network. If your network has WEP enabled it becomes more difficult for an unauthorized third party to gain access to your wireless network; however, as noted previously in this book, WEP is easily compromised via passive monitoring. Depending upon the level of security used by your wireless LAN you can make it extremely difficult to near

impossible for an unauthorized third party to masquerade as a legitimate user. However, if they gain an RF capability to your network you can add an additional barrier through the use of authentication, authorization and accounting functions that we will discuss as a countermeasure to the masquerade threat.

5.3.2 Countermeasures

There are several countermeasures you can consider to reduce the potential of a third party accessing your network as a legitimate user. Those methods include what are referred to as triple-A: authentication, authorization and accounting. Under the IEEE 802.11 standard, authentication can be open or shared key. The first method of authentication, open system, represents a null method and provides no actual method of authentication. Because the composition of a static key can be determined through the use of several readily available programs, shared key authentication is also vulnerable. As we will note in Chapters 6 and 7 when we cover proprietary and standards based security techniques, there are several methods you can consider using to harden authentication. Two of those methods include the use of MAC addresses and LEAP authentication. Here LEAP references a proprietary Cisco ‘lightweight’ version of the Extensible Authentication Protocol (EAP).

Figure 5.5 illustrates the display of the Network Security tab from the Cisco 340 Series Properties dialog box. Note that by default no server based authentication is supported. Similarly by default, access point authentication is based upon open or null authentication since the WEP is not set. Later we will examine the configuration and use of different authentication methods in detail.

While authentication verifies the identity of a user, authorization permits a user to access network resources. Authorization is not part of the IEEE 802.11 standard. Instead, authorization is commonly performed via the assignment of a User-ID and password to different network resources, such as network servers, for the administration of routers and other devices. By properly configuring authorization parameters you can minimize the ability of a third party to access network resources. In doing so you should avoid well-known User-ID assignments, such as the use of first and middle initials prefixed to a last name since anyone with a telephone directory or knowledge of employees can then easily determine User-IDs. Similarly, the assignment of passwords should include alphanumeric characters to eliminate the possibility of a dictionary attack being successful.

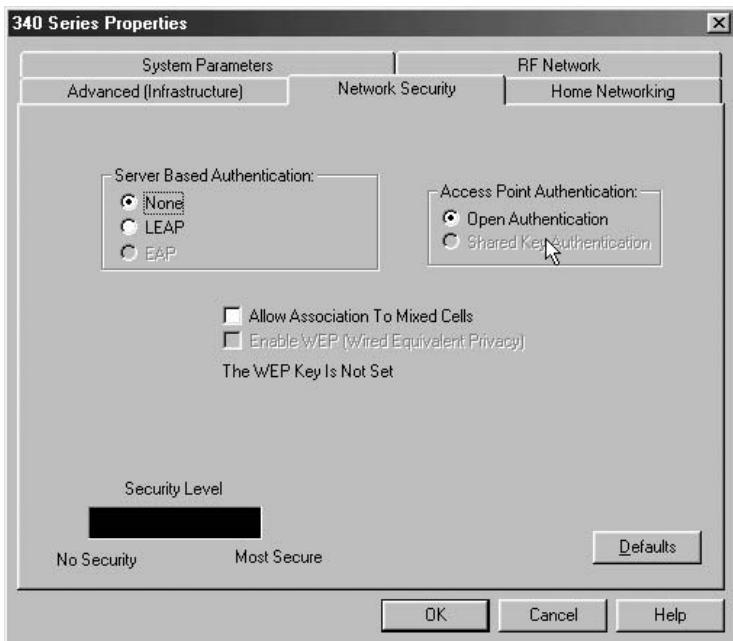


Figure 5.5 The Network Security tab in the Cisco 340 Series Properties dialog box provides the ability to select a server based authentication method and the type of authentication to be used.

While authorization is important, it should be noted that it can be compromised if static WEP keys are used or if WEP is disabled. This is because an unauthorized third party could obtain the ability to monitor communications and literally discover the ‘keys to the kingdom’ by recording User-ID and password sequences. Thus, to safeguard authorization in a wireless LAN environment you need to have strong encryption.

A third countermeasure to masquerade and the last ‘A’ in triple-A is accounting. By logging requests for access to different network resources you can create a database of activity which can be used in different ways. First, you can obtain an historical record that can be used to generate exception reports indicating attempted actions that warrant review. For example, repeated attempts to log onto a server could either result from someone forgetting their password or from a person attempting to gain access to an account that is not assigned for their use. Secondly, a log of activities can serve as a legal document if the need arises to take action against anyone who either attempted or actually broke into one or more systems.

5.4 Data modification

A third modification attack is one of the most insidious examples of a security vulnerability associated with wireless LANs. The reason it is insidious results from the fact that it can occur without the recipient of the modified data being aware of the modification.

5.4.1 Overview

A data modification attack results from the fact that the ICV used by wireless LANs is a CRC-32. As noted earlier, the CRC-32 is linear with respect to a bit flipping process. This means it is possible for an unauthorized third party to modify data in a frame and change the ICV so that the receiver is none the wiser.

5.4.2 Countermeasures

Because the ICV is linear it is possible to change both frame data and the composition of the ICV. This means that you can encrypt the 802.11 frame within a layer 3 (network layer) wrapper to preclude the ability of a third party to tamper with frames such that the tampering can go undetected. Encrypting and wrapping the 802.11 frame can be accomplished via several methods which includes the use of a Web browser's built-in security feature, using IPSec or via the creation of a VPN, which is likely to be based upon the use of IPSec. Another option is to use equipment that supports the Temporal Key Integrity Protocol (TKIP), which represents a series of measures that harden wireless LANs to include preventing undetected tampering of frames. In Chapter 7 we will examine these methods.

5.5 File sharing

One often overlooked security vulnerability can occur if Windows file sharing is enabled on one or more wireless LAN stations. This security vulnerability can happen even when your network is hardened through the use of authentication, encryption, and accounting because under most versions of Windows it is difficult to authenticate file-sharing users.

5.5.1 Overview

Under Microsoft Windows you can initiate the sharing of files and/or the use of your printer, allowing other network users to gain access to your computer files

or the printer attached to your computer. Thus, any unauthorized third party that is able to gain access to your organization's network may be able to gain access to files on different computers if file sharing is enabled on those computers. This threat to security is applicable to both computers using wireless and wired communications if your wireless network infrastructure is connected to the Internet. The actual degree of vulnerability depends upon the version of Windows used and its applicable settings. In the next two sections we will briefly look at Windows 95 and Windows 2000 to note some of the differences in capabilities between different versions of Windows. We will then use our brief examination as a foundation for discussing several countermeasures we can consider to reduce the security threat associated with file sharing.

5.5.2 Windows 95

In a Windows 95 operating system environment you can enable file sharing through the network icon in the control panel. Figure 5.6 illustrates the display

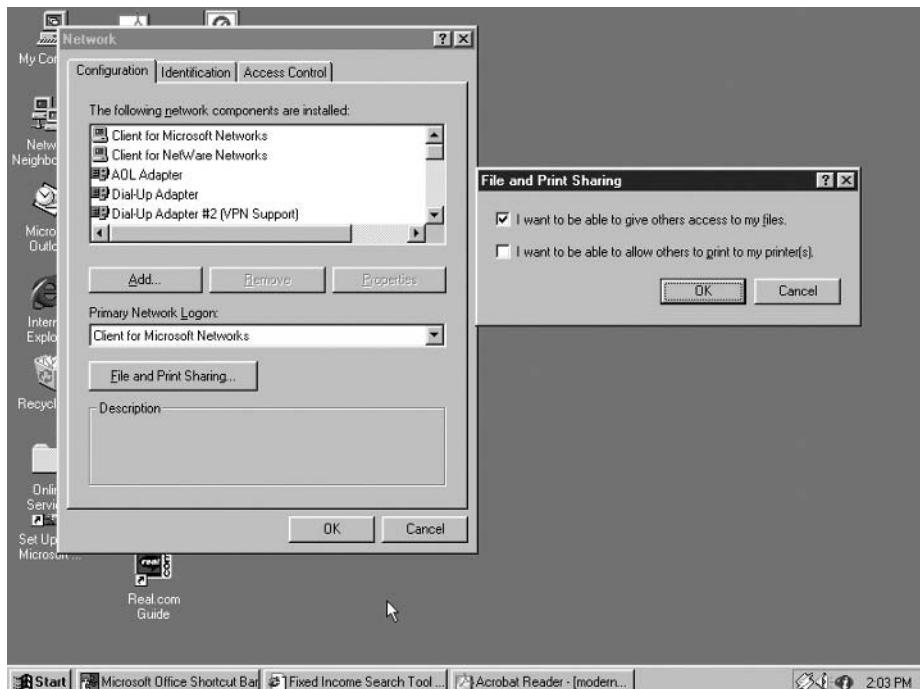


Figure 5.6 Under Windows 95 file and print sharing are placed into effect from the Network dialog box.

of the Network dialog box in the left portion of the screen. Clicking on the button labeled 'File and Print Sharing' displays the box with that label. You can then check one or both boxes to enable users to access files or printers on, or connected to, your computer. The right portion of Figure 5.6 shows the File and Print Sharing dialog box.

Once file sharing is in effect, it is a relatively easy process for other network users to view and access files on another computer. For example, consider Figure 5.7 which uses a series of four overlaid windows to illustrate how you can use Network Neighborhood to view computers on the entire network as well as those in your workgroup. In Figure 5.7 the top left window shows the Network Neighborhood with Mdpc-3 representing a computer in this author's workgroup. Clicking on 'Entire Network' results in the display of the second window with that label. Next, the computer Ssc10 was selected, after which the folder labeled 'sys' was selected, resulting in the display of the window labeled 'sys on Ssc 10', shown in the foreground of Figure 5.7. From this

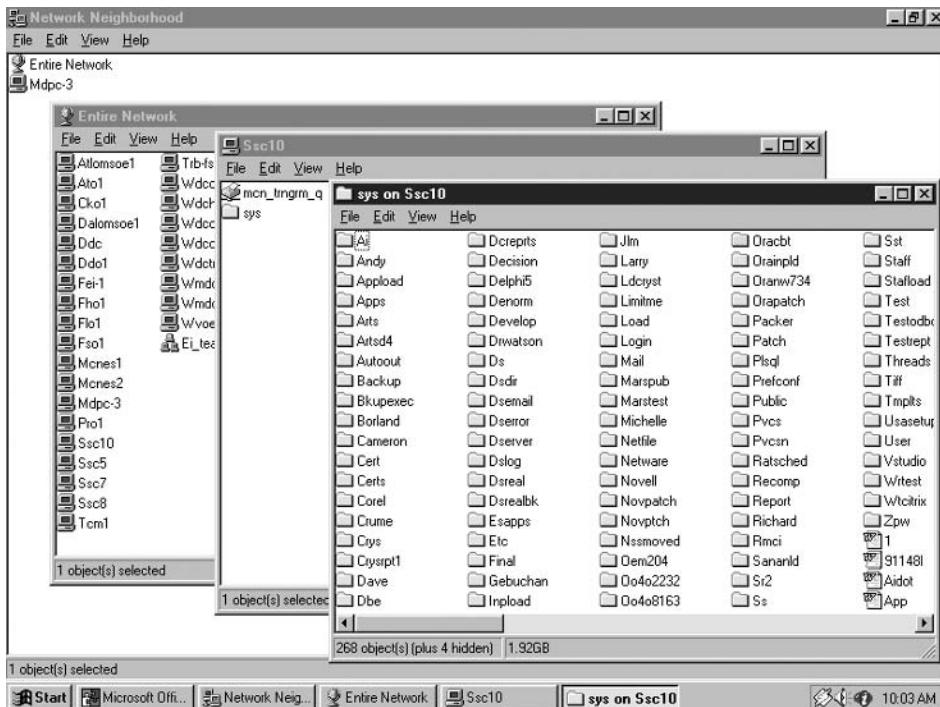


Figure 5.7 Using Network Neighborhood to locate shared files and folders on a network.

window you can access a variety of files and folders that are shared with other network users.

Under Windows 95 you can control access to shared resources by using passwords or by listing the names of people you want to have access to these resources. Access control under Windows 95 occurs via the Access Control tab in the Network dialog box. Figure 5.8 illustrates the display of that tab in the foreground of the dialog box. Note that you can select either the assignment of a password or user-level access control, the latter providing access based

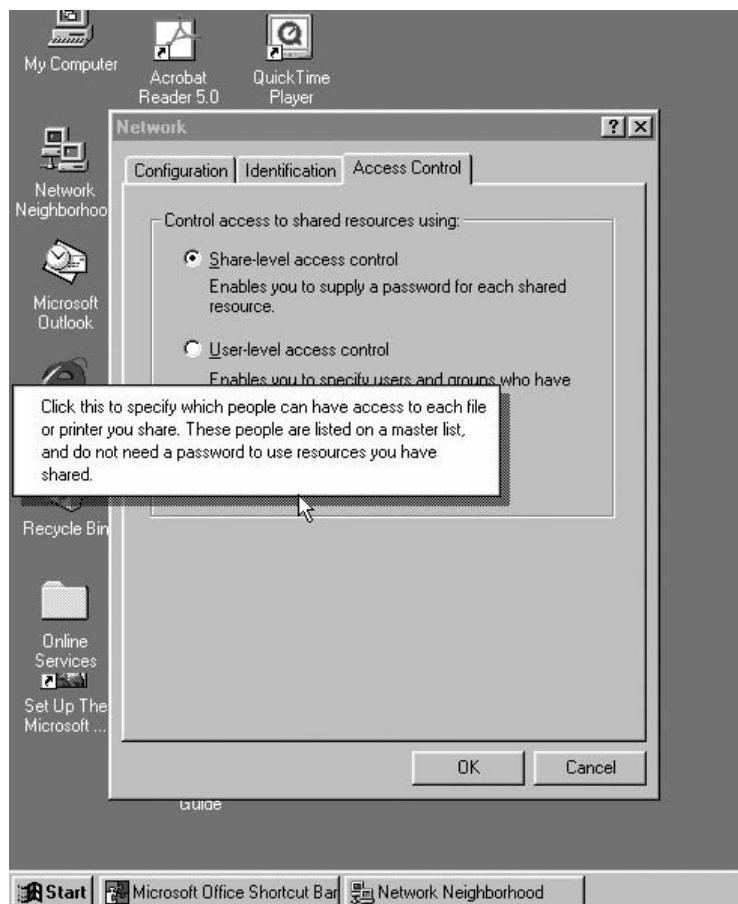


Figure 5.8 Access control to shared resources under Windows 95 can occur via the assignment of a password to each share or through a master list of persons.

on a predefined master list of users. Now that we have an appreciation for file sharing under Windows 95, let's look at Windows 2000.

5.5.3 Windows 2000

Under Windows 2000 the selection of file and printer sharing represents a network service. Due to this, its implementation is slightly different in comparison to Windows 95.

Figure 5.9 illustrates a sequence of four overlaid windows that show the sequence of operations required to install file and print sharing under Windows 2000. First, you would open the Network and Dial-up Connections box, shown in the upper left corner of Figure 5.9. Right clicking on the local area connection icon permits you to select the Local Area Connection properties entry in a pop-up menu, resulting in the display of the second dialog box in the figure. If you click on the button labeled 'Install' the dialog box labeled

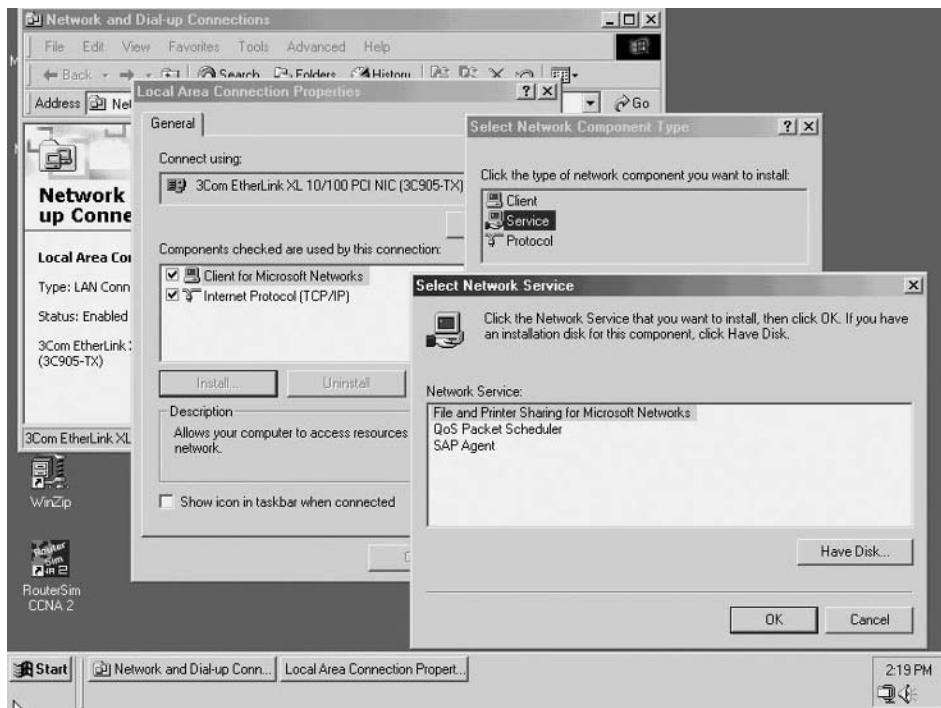


Figure 5.9 Under Windows 2000 File and Printer Sharing is selected as a network service.

'Select Network Component Type' will be displayed. This dialog box appears in the third window in Figure 5.9. From that dialog box you would select 'Service,' since file and print sharing is considered to represent a service. This action would result in the display of the Select Network Service dialog box shown in the foreground of Figure 5.9, with File and Printer Sharing shown as the top network service available for selection.

Once file and print sharing is in effect, Windows 2000 is similar to Windows 95 in that you can simply right click on a file or folder to select sharing. Figure 5.10 illustrates the pop-up menu resulting from right clicking on a drive icon. Note that the Sharing entry in the pop-up menu is shown highlighted.

Once you select a file, folder or drive for sharing you can restrict the maximum number of users allowed and set permissions for shared access as illustrated in Figure 5.11.

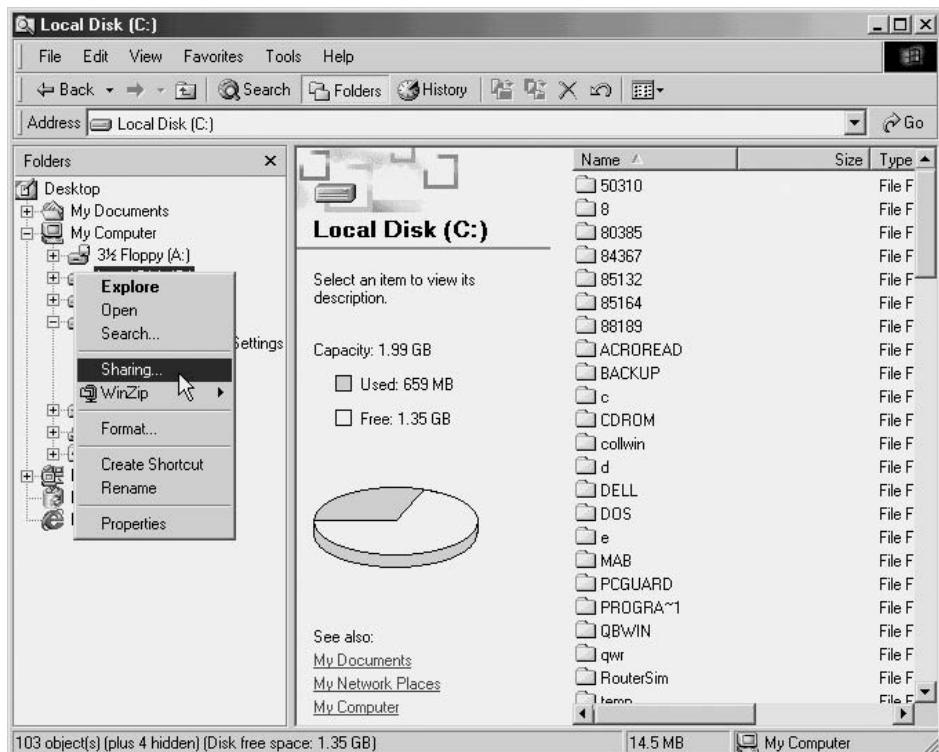


Figure 5.10 Right clicking on a file, folder or drive permits the sharing of the selected resource.

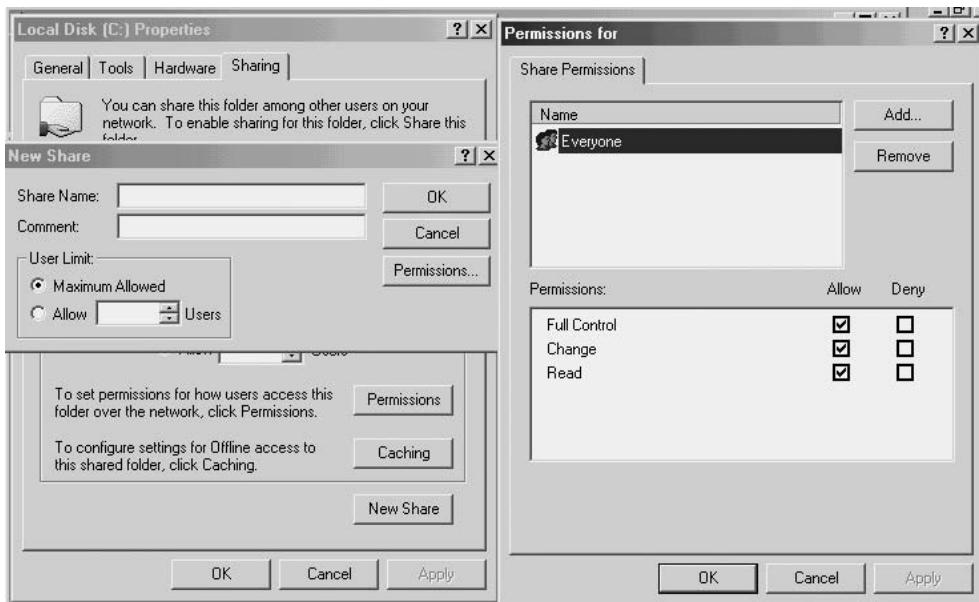


Figure 5.11 Under Windows 2000 you can assign a variety of permissions for accessing shared resources.

As indicated in the background in the left portion of Figure 5.11, the properties dialog box for the selected resource will include a tab labeled 'Sharing' once file sharing is in effect. When you click on a button labeled 'Share this folder,' a dialog box labeled 'New Share' will be displayed. That dialog box is shown in the foreground of the left portion of Figure 5.11. Using this dialog box you can enter a new name for the share, which is what users will view when they connect to the shared resource. You can also add a comment about the shared resource as well as limit the number of users who can connect to the shared resource at one time. Unlike Windows 95, under Windows 2000 you can set shared resource permissions. To do so you would click on the button labeled 'Permissions,' resulting in the display of the dialog box shown in the right portion of Figure 5.11. In examining the share permissions dialog box note that you can use the upper window to assign permissions to both individuals and user groups. In comparison, the lower window provides you with the ability to allow or deny specific permissions. Thus, in comparing Windows 95 and Windows 2000 resource sharing it is obvious that the latter provides a higher degree of sharing controls.

5.5.4 Countermeasures

One obvious countermeasure to the vulnerability associated with the sharing of resources is not to do so. In fact, if you scan the Internet or read various trade publications you will note that most references to security and resource sharing tell the reader to turn the service off. However, there are many legitimate reasons to employ resource sharing and disabling its capability could result in a significant loss of organizational productivity. That said, it may be advisable to employ resource sharing in conjunction with both wireless and wired security measures. From a wired network perspective you can secure resource sharing with a protocol other than TCP/IP, in effect precluding the ability of users on the Internet to obtain access to shares. From a wireless network perspective it is a relatively easy task for an unauthorized third party to monitor network traffic. Thus, hardening your wireless traffic by employing encryption and authentication, can make it more difficult (maybe literally impossible) for an unauthorized third party to obtain the ability to figure out how to access protected shared resources. However, it is important to also note that hardening wireless and wired network access to computers with shared resources is no substitute for ensuring sharing is correctly performed. That is, when using a particular version of Windows you should ensure that resource sharing is configured with appropriate permissions.

5.6 Jamming

When we hear the term ‘jamming’ we may think of some old war movies in which a soldier, sailor or airman would sit in front of some electronic equipment and turn a series of dials to disturb enemy communications. In a wireless LAN environment jamming can occur without the use of specialized equipment because the manner in which FHSS and DSSS communications occurs is well-known. In addition, as we will shortly note, the design of the wireless LAN protocol makes it very susceptible to jamming by simply modifying software to transmit certain types of frames.

5.6.1 Overview

IEEE 802.11 wireless LANs operate on well-known frequencies in the 2.4 GHz and 5 GHz frequency bands. While it is theoretically possible for a disgruntled employee or another third party to acquire broadband jamming equipment, it is far easier to use the frames provided under the standard as

a weapon. For example, assume someone modified driver software to continuously transmit probe or RTS frames. For either situation these actions can have a similar effect to jamming. This is because issuing a probe frame results in a probe response frame. If a station is programmed to continuously issue probe frames the sequence of probe and probe response frames precludes the ability of other stations to gain access to the air. Similarly, the issuance of a repeated sequence of RTS frames will result in a sequence of CTS frames tying up the airway in response to the RTS frames. Because it is possible for a third party to simply park a van in the parking lot of a building and use a directional antenna to focus their broadcasts towards a building jamming can occur from both within and from outside a facility.

5.6.2 Countermeasures

There are several countermeasures you can consider using to reduce or minimize the potential for your wireless LAN to be jammed. First, periodic monitoring of your network when throughput appears to decrease can be used to determine if someone is jamming your organization's network. By using a protocol analyzer you can note if an exceedingly high level of a particular type of frame is literally clogging the air. If so, you can use the signal strength indicator, available with most utility programs that are bundled with different wireless LAN adapter cards, to locate the direction from which the frames are being broadcast. By moving a laptop or notebook computer around you may be able to locate the source of the apparent jamming and then take appropriate action.

Another technique that can be considered to minimize the effect of jamming is to turn off the ability of clients and access points to use the RTS-CTS frame sequence. This frame sequence is used to overcome the hidden node problem; however, when the RTS-CTS frame sequence is used it can significantly reduce overall network throughput. For this reason most wireless LAN adapter products by default disable the use of the RTS-CTS frame sequence. If your equipment enables the RTS-CTS frame sequence by default or if you enabled the sequence and do not have a hidden node problem, you could consider disabling the sequence. To do so most programs bundled with your wireless LAN hardware include a facility that enables the RTS threshold to be set to a high value that disables the features.

Figure 5.12 illustrates the SMC Networks wireless LAN adapter setup menu. If you look at the window labeled 'Property' you will note that the fifth entry is RTS Threshold. By moving the highlight bar over that entry you can

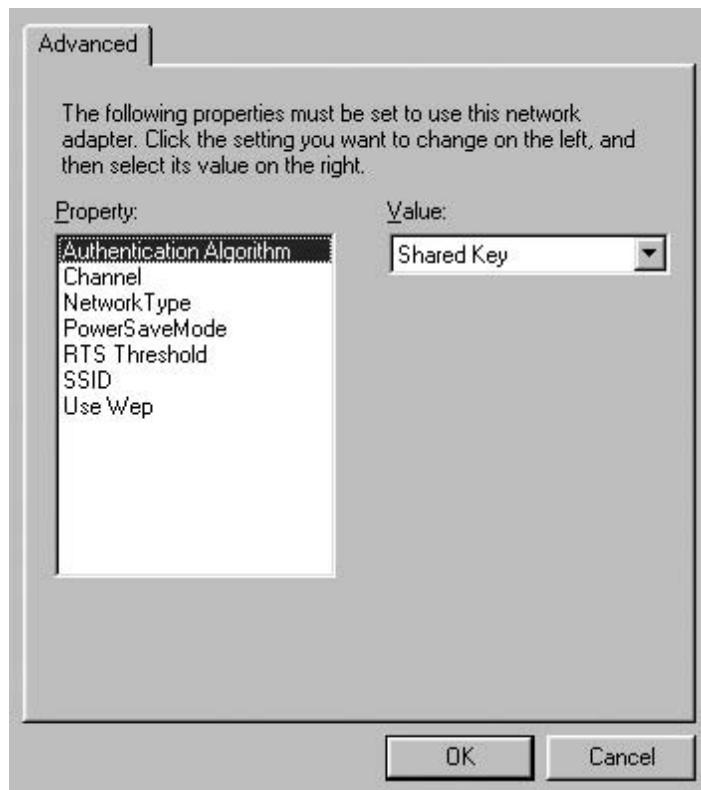


Figure 5.12 Most utility programs that are bundled with wireless LAN products include the ability to enable or disable the RTS-CTS frame sequence.

either enable or disable the use of the RTS-CTS frame sequence. If you disable the RTS threshold on each wireless LAN device in your network the broadcast of RTS frames as a mechanism to jam your network will obviously be minimized.

5.7 Encryption attacks

Under the IEEE 802.11 standard and its various extensions WEP provided the mechanism to encrypt communications. While we have previously discussed the technical reasons for WEP being vulnerable, we will briefly review those reasons in this section as a mechanism to build a foundation for our discussion of countermeasures.

5.7.1 Overview

The RC4 encryption algorithm used by WEP is also securely used for Web browsers. Unfortunately, the manner by which WEP uses the RC4 algorithm results in the ability of third parties to mount several types of encryption attack that can compromise the security of your organization's wireless LAN. As a refresher, WEP uses a 24 bit IV that is transmitted in the clear as a mechanism to enable the data portion of each frame to be encrypted on an individual frame basis without dependency on prior frames. Although this scheme permits frame independence with respect to encryption, it weakens encryption. This weakening occurs due to the 24 bit length of the IV, which results in IVs theoretically repeating approximately every five hours. In actuality, because the IV is generated randomly by each station, the more stations in the network the higher the probability of IV collisions, the latter representing a term that indicates repeating IVs. This situation can be viewed as being similar to the fact that the probability of two or more people having the same birthday increases as the number of randomly selected people increases, a situation referred to as a birthday paradox.

Because the probability of IV collisions increases as the number of stations in a wireless network increases, the amount of time required to wait for an IV collision can be considerably less than an hour. Since the IV is concatenated with the WEP secret key for use by the RC4 algorithm, this enables a frequency analysis of monitored frames with the same IV to serve as a mechanism to decrypt the encrypted portion of captured frames.

A second significant problem associated with WEP and its use of RC4 results from the fact that the composition of encrypted data transported in the secure portion of a frame when WEP is enabled can easily be guessed. For example, when 802.11 frames are transporting Internet traffic the first series of fields in the frame commonly represents the IPv4 header. As indicated in Chapter 4, when we discussed the vulnerabilities of WEP, weak RC4 keys combined with an educated guess of the composition of certain fields transported within an IEEE 802.11 encrypted frame, enabled software programs to be written that can recover the WEP key in use. Although such programs require the use of a database consisting of between 4 and 6 million frames, it is a relatively simple process to passively monitor the traffic flowing on a wireless LAN. Once the WEP key in use is recovered, all previously captured traffic using that key and future network traffic encrypted with the recovered key can be decrypted. Rather than say WEP is 'unsafe at any speed' there are certain countermeasures that can negate the potential security risk resulting from encryption attacks.

5.7.2 Countermeasures

Although the use of a relatively small (24 bit) IV represents a key weakness of WEP, the design of 802.11 frames precludes the use of a longer IV without losing compatibility with the large base of existing equipment. Thus, it is impractical to lengthen the IV as a mechanism to reduce IV collisions, and the ability of an unauthorized third party to passively monitor communications and obtain a database in a relatively short period of time that can be used to recover the WEP key in use.

Recognizing the vulnerability of WEP, several vendors developed proprietary security enhancement techniques that involve dynamically changing the WEP key. Because the WEP key is changed either on a frame by frame basis or after a predefined number of frames or time interval transpires, this solution to the security vulnerability of WEP works. The reason it works is that WEP is vulnerable only when a sufficient number of IV collisions occur using the same key. Thus, if the frequency of the key change is greater than the IV collision rate, the database obtained by passively monitoring wireless LAN traffic cannot be employed for WEP key recovery nor for a frequency analysis attack.

The dynamic changing of WEP keys can be viewed as a layer 2 solution to a layer 2 security problem. In addition to various proprietary solutions to encryption attacks that involve dynamic WEP key changes there are also several standards based solutions. Such standards based solutions include tunneling 802.11 frames within a layer 3 VPN, the use of a Web browser in its secure mode of operation, and two emerging encryption methods that eliminate the vulnerability of WEP. In Chapter 6 we will examine several proprietary security enhancement techniques, while in Chapter 7 we will look at standards based security methods that can be employed to overcome the vulnerability of WEP.

5.8 SNMP

It is a well-known fact that the Simple Network Monitoring Protocol (SNMP) represents the literal key to managing multiple devices in a TCP/IP environment. Unfortunately, based upon research performed at Oulu University in Finland during 2001, it was discovered that the implementation of SNMP could result in a variety of vulnerabilities that may mean using it represents a security hazard. In addition, any discussion of SNMP needs to consider the fact that three basic versions of the protocol exist, with only the latest version, SNMPv3, providing an acceptable level of security. Thus, in this section we

look at two separate but related SNMP security issues. For the first issue we will briefly discuss how coding flaws could assist hackers. This discussion, while focused upon the wireless LAN environment, is also applicable for wired LANs and the wide area network connections that make up the Internet. Concerning the second issue, we will briefly discuss the three versions of SNMP. Once the preceding is accomplished we will focus on countermeasures to secure SNMP.

5.8.1 Coding flaws

During 2001 researchers at Oulu University in Finland discovered that poor programming in Abstract Syntax Notation One (ASN.1) resulted in some security related flaws in SNMP. As investigators continued their research into ASN.1 coding, they found that the use of this language, which compresses data into abstract descriptions as a mechanism to reduce the size of complex programs, often failed to check the length of messages. Due to poor coding, the use of ASN.1 in many SNMP implementations enables oversized messages to result in a memory overflow problem that could allow hackers to execute malicious code appended to an oversized message. While many trade publications ran rather hyped articles about this new vulnerability, in reality it represents an expansion of a well-recognized vulnerability into a new area. That well-recognized vulnerability of buffer overflow exploitation resulted in numerous attacks against Microsoft's Internet Explorer and other vendor software products that have a relatively long history. Although buffer overflow attacks have occurred for over ten years, the complexity of modern software appears to result in multiple holes awaiting discovery by hackers, with Code Red being just one recent example of an exploitation occurring many years after the basic buffer overflow attack was recognized as a problem facing Internet Explorer. What made many trade press articles hype the ASN.1 buffer overflow problem was probably due to the fact that this language dates to the 1980s and forms the basis for implementing SNMP in bridges, routers, gateways, and channel service units that provide the foundation for Internet and intranet communications.

5.8.2 SNMP versions

There are currently three versions of SNMP in use. SNMPv1, which is commonly referred to as SNMP, represents the initial version of this management protocol. Under SNMP the ability to obtain and/or write access to various SNMP counters, referred to as Management Information Base (MIB) counters, is controlled via the use of what is referred to as 'community strings.' Here the

community string represents a string of alphanumeric characters that function as a password when attempting to gain access to an SNMP agent where the MIB counters reside.

Figure 5.13 illustrates the use of the Agere Systems' Orinoco wireless PC Card under Windows XP and the Orinoco AP Manager program to access the SNMP MIB on an Orinoco RG-1100 residential gateway, the latter representing a combined access point and router. The Orinoco Client Manager, shown in the upper right portion of Figure 5.13, indicates that the client PC Card operating on this author's Toshiba notebook has an excellent radio connection to network 394896, which represents an Orinoco Residential Gateway. A second dialog box shown in the foreground of Figure 5.13 is the Access Point (AP) Manager provided by Agere Systems for managing the vendor's series of

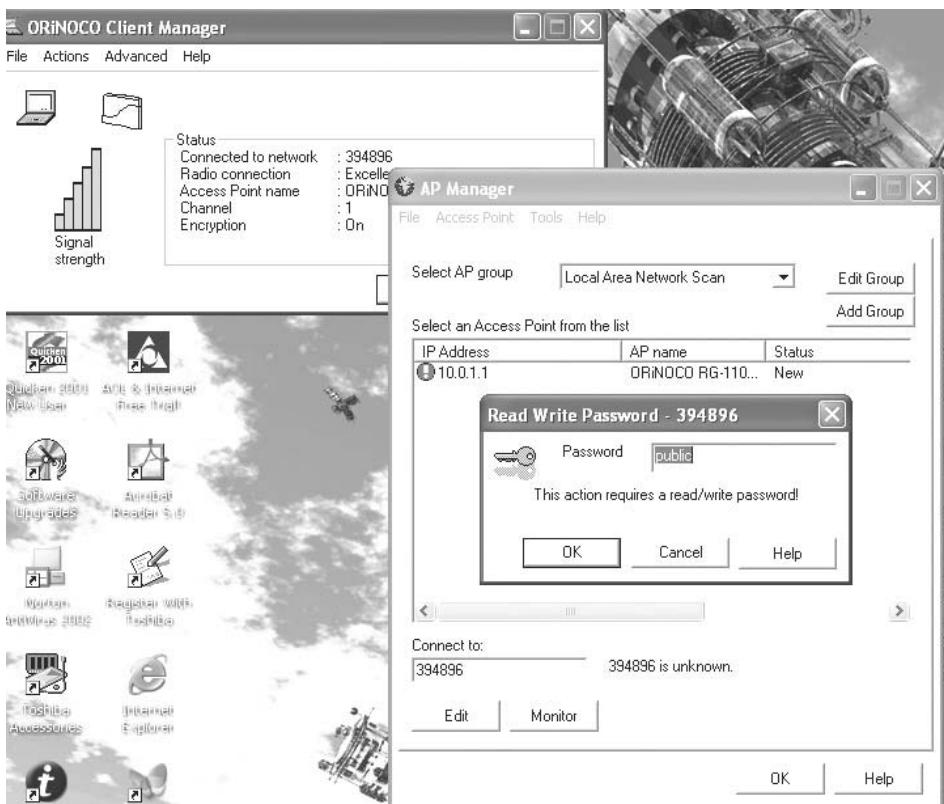


Figure 5.13 When using the Orinoco AP Manager you need to enter the last five digits of the network name to access an Orinoco Residential Gateway.

Orinoco products. In the AP Manager dialog box you will note that an attempt to access the Orinoco RG-1100 through the AP Manager results in a request for the entry of a ‘read/write password.’

In examining the dialog box that superimposed the AP Manager dialog box you will also note that Windows XP by default uses the community string or password of ‘public.’ Fortunately, that community string does not work on the Orinoco RG-1100. Instead, the password used by SNMP on the RG-1100 is the last five digits of the network name, which is also the setting used to establish the WEP key for encryption, and by default is enabled on the residential gateway, one of a small number of products configured in this



Figure 5.14 Although the Agere Systems’ AP Manager indicates the 6-digit network name should be used to connect to a Residential Gateway, this author used the last 5 digits of the network name.

manner. Thus, to gain access to the RG-1100 via the AP Manager, you would need to enter the numeric string 94896, which is the same string required for a wireless client's WEP key to be configured with to communicate with the RG-1100.

Although the default configuration of the RG-1100 results in encryption being enabled and the last five digits of the network name functioning as both the WEP key and community string or password, its use provides a false sense of security. This is because the composition of a static WEP key can be recovered via the use of readily available programs, such as AirSnort or NetStumbler. In addition, if a third party gains physical access to the Residential Gateway (RG) all they need to do is examine the network name fastened on a label affixed to the bottom of the gateway. Because Agere Systems ships their RG's with encryption on by default, using the last five digits of the network name as the WEP key and as the SNMP community name, it becomes relatively easy to learn the key. All one has to do is look at the label at the bottom of the RG and remember the last five digits of the network name.

Although the community name used by this author to successfully access the RG-1100 was the last five digits of the network name, if you select the default value of Public the AP Manager tells you to use a different value. That value is the full 6 digit name, as indicated by the display shown in Figure 5.14. Note that in Figure 5.13 the Orinoco Client Manager indicates that encryption is ON and an excellent connection exists to the RG. Thus, the dialog box shown in Figure 5.14 would appear to indicate that access to the RG was due to an invalid password and not due to an inability to access the unit. When this author entered the last five digits of the network name, he was then able to monitor the access point, resulting in the display of a new screen with eleven tabs which is shown in Figure 5.15.

Once you connect to an access point via SNMP the main screen of the Monitor Access Point program will appear, similar to that illustrated in Figure 5.15. In examining the box labeled 'System Identification' note that the Object ID is shown as. 1.3.6.1.4.1.1751.1.4.8. As a refresher, the Object ID defines the location of a managed object within the global naming tree. To access a particular MIB counter for reading or writing you need to know the IP address of the managed device and its object identifier. Once you know both and also know the community name and WEP setting, you can literally work through the MIB to note the MIB objects supported by a particular wireless device.

From the System tab you will note that when this author accessed the AP at IP address 10.0.1.1 it had been up for approximately 21 minutes. By clicking



Figure 5.15 The System tab of the Monitor Access Point display indicates the object ID.

on other tabs located on the screen, shown in Figure 5.15, we can access a variety of network related information that a third party could use to attack our organization's network. For example, once logged onto an access point a third party could learn the MAC and IP addresses of other devices without having to monitor the network. Because Agere Orinoco residential gateways are shipped with a predefined IP address, it is a relatively easy process to attempt to connect to an RG once you locate its signal.

Continuing our discussion of versions of SNMP, the first version, as previously mentioned, is very weak with respect to security due to its reliance on community names as passwords that are transmitted in the clear. In addition, under SNMP there is no method for authentication, which represents an additional weakness. Recognizing this lack of security resulted in the Internet community beginning to revise SNMP. Unfortunately, two competing camps could not agree on a fix, resulting in SNMPv2 mainly enhancing the performance of the original version of SNMP. It wasn't until the year 2000 that SNMPv3 became a standard. The original version of SNMP is by far the most widely used version of SNMP. It will probably be several years until SNMPv3 capabilities are widely available in vendor wireless products.

5.8.3 Countermeasures

There are two areas that have to be addressed when discussing SNMP vulnerabilities – ASN.1 coding and SNMP hardening.

The previously mentioned flaws in ASN.1 that make certain vendor products vulnerable to buffer overflow attacks can be alleviated by obtaining the applicable software patch and applying it to installed products. As an interim measure, if no software patch is available, you may wish to elect to turn off SNMP until a patch becomes available for the product.

Concerning SNMP hardening, depending upon the product used and its configuration and monitoring capability, you may be able to consider several actions. First, if possible, you should change the community name to an alphanumeric string that is not in the dictionary. Doing so will prevent a dictionary attack being used. Secondly, since SNMP is transported to wireless devices via IEEE 802.11 frames it makes no sense to harden SNMP access without ensuring your basic wireless communications are hardened. To accomplish the latter, as a minimum you need to enable WEP and ideally use dynamic WEP keys or one or more of the enhanced proprietary or evolving standards based security measures discussed in Chapters 6 and 7. As a precaution it is always a good idea to periodically examine the use of managed objects as a mechanism to determine if unauthorized people gained access to your organization's equipment.

For example, when using the Agere Systems' AP Monitor program you can click on the SNMP tab to determine management traffic. Figure 5.16 illustrates the display of the SNMP tab for the AP at IP address 10.0.1.1. By applying appropriate software patches, changing the default community name and enabling basic wireless security and enhanced security options, you can harden SNMP so that it maintains its usefulness without making the network manager uncomfortable about its potential vulnerability.

5.9 Broadcast monitoring

Based upon the manner in which access points operate it is possible to monitor wireless broadcast traffic and learn information about wired network traffic. This vulnerability occurs because of the manner in which access points operate as a two port bridge. Thus, to understand this vulnerability we will review the operation of a bridge and how that device follows the 3F rule. That is, a bridge and an access point, which is a wired to wireless network bridge, constructs and uses its port-address table via the process of flooding, filtering and forwarding frames.

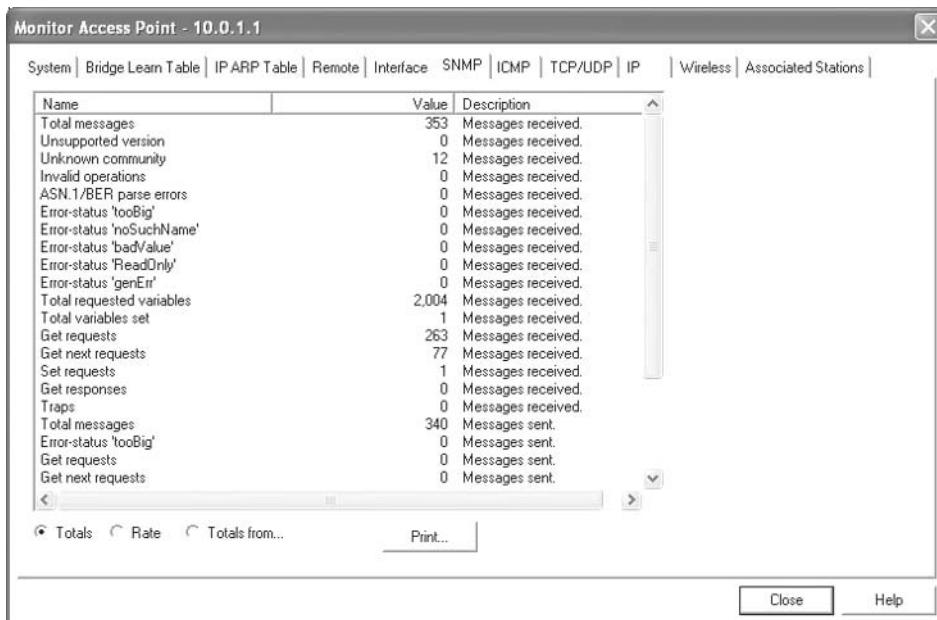


Figure 5.16 The Agere Systems' AP Monitor program's SNMP tab can be used to determine management activity associated with different wireless devices.

5.9.1 Overview

To illustrate how broadcast monitoring can result in the content of frames destined to other wired stations being broadcast over the air, consider Figure 5.17 which illustrates a simple network infrastructure consisting of an access point connected to a hub. Two wired stations are connected to the hub, with their MAC addresses indicated for simplicity as A and B. Similarly, two wireless stations are shown for ease of illustration with MAC addresses of C and D.

When the access point is powered on, its port-address table is empty. Thus, if station A transmits to station B, the frame will also flow to the access point. Because the access point does not initially know where the destination B address resides (on the wired or the wireless infrastructure), it performs a flooding operation, transmitting the frame onto all other ports than the port the frame was received on. This action results in the frame being broadcast over the air.

Based upon the preceding bridge function, note that a frame transmitted from one wired device to another literally finds its way to being broadcast over the air. This means an initial frame flowing to a server or another device is

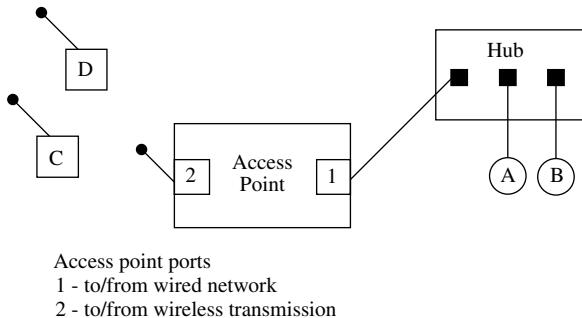


Figure 5.17 An access point functions as a two-port bridge.

available for monitoring by any unauthorized third party within transmission range of the access point.

Returning to our discussion of bridging, because station A transmitted to station B, the access point notes that address A is on the wired infrastructure. Thus, the initial entry in the access point's port-address table becomes:

Port	Address
1	A

Now let's assume station B responds to station A. As the frame from station B flows to the access point, the AP checks the contents of its port-address table and notes that station A resides on port 1 where the frame originated from. Thus, there is no need to forward the frame and the access point filters or discards the frame. However, the access point notes that the source address of the frame is B and since it does not have an entry for frame B in its port-address table, it proceeds to update the contents of that table. Thus, the contents of the access point port-address table now becomes:

Port	Address
1	B
1	A

To conclude our examination of the security risk associated with the address learning process let's assume that station C transmits to station D. Because station C is a wireless device its transmission can be read as it flows to the

access point. Since the access point has not learned where station D resides at this particular point in time, it floods the frame. However, because in an infrastructure mode of operation all communications between wireless devices flow through an access point, the frame is both transmitted onto the wired infrastructure and transmitted over the air. Thus, it also becomes possible for a wired network user with a sniffer to capture some frames that are directed to other wireless stations due to the manner by which wireless access points operate. After the access point floods the frame it updates its port-address table as shown below:

Port	Address
1	B
1	A
2	C

When station D responds to C the access point consults its port-address table and notes that the destination resides on the wireless LAN. Thus, the access point forwards the frame back onto the air and updates its port-address table since the AP recognized that station D resides on the wireless LAN. The contents of the port-address table of the access point are now updated as shown below:

Port	Address
1	B
1	A
2	C
2	D

While the risk of frames that should stay on one infrastructure that flow onto the other during the bridge learning process is small, periodically the access point updates its tables and old entries are discarded. This means that it is possible throughout the day for frames to flow onto an infrastructure where they do not belong. Because by default WEP is disabled on most devices, this results in another vulnerability you need to consider.

5.9.2 Countermeasures

In addition to the normal countermeasures associated with wireless LAN security previously described, you can minimize the problem of broadcast

monitoring via a network architecture change. If you connect the access point to a router or use a combined router/access point, transmissions from the AP can flow at layer 3 to another router connected to your organization's wired network. The use of this network structure eliminates the broadcast of frames from your wired network onto the wireless network. Obviously, there is a cost to this countermeasure as two routers are now required to service the wireless infrastructure.

5.10 Accessing a management console

Another attack method worth noting is the use of a Web browser or Telnet program to access the management console of an access point.

5.10.1 Overview

Most access points include a management console capability which enables someone to view and modify the configuration of the access point. On high-end access points you can typically use a serial port, SNMP, a Web browser and possibly Telnet to access the management capability of the device.

Because most access points support DHCP they use a block of RFC 1918 addresses. Since most access points by default use a predefined RFC 1918 address they are not too difficult to locate. In fact, if you point your browser to the SMC Networks Web site you can view their product manuals and note the default IP addresses assigned to different products. If you do you will note that the RFC Class C IP address 192.168.123.254 is assigned to the Barricade wireless router by default. Even if a user changes that address, since the product only supports 192.168.123.0 network addresses, all a third party has to do is start at dot 1 (.1) and scan addresses up to 192.168.123.254 to locate the wireless router. Once an access point is located it is a relatively simple process to scan RCF 1918 blocks of addresses until you stumble across the console display for an AP. After you locate the IP address of the console you can attempt to gain access to the device either through the use of the default password shipped with most products or through a dictionary attack. If the person managing the device was a sloppy administrator it becomes a relatively simple process to gain access and in effect control all or a portion of the network.

5.10.2 Countermeasures

When working with manageable devices you should always change the default password. In doing so you should use an alphanumeric password. That

password should be at least 8 or 9 characters in length to minimize the potential for an unauthorized third party to rapidly cycle through all possible letters, beginning with a single character position and expanding upon the number of positions. By using alphanumerics you alleviate the possibility of being subject to a successful dictionary attack since such passwords as born2soon, smile4you and good12345 are not in any dictionary known to this author.

5.11 Theft of hardware

A few years ago one of the more common airport threats was not terrorists but crooks who would work in pairs at the airport scanner. One person would go through the scanner, while the second would get in front of a person that put his or her laptop or notebook computer through the baggage scanner. The second member of the team of crooks would use several delay tactics, such as slowly emptying the change in their pocket as they went through a metal detector, to impede the computer owner from reclaiming his or her device in a timely fashion. The delay was typically of sufficient duration so that the partner in crime was able to grab the computer and be halfway out of the airport before the owner realized what had happened.

5.11.1 Overview

While airport problems have certainly changed, unfortunately con men and women and basic thievery has not. If an unauthorized party obtains a laptop or notebook that has a wireless LAN adapter card that was configured, they have also gained knowledge of one or more preconfigured security measures installed on the laptop or notebook. This means that an unauthorized third party who gains access to a computer used by your staff may be able to use the computer to illegally access your organization's network.

5.11.2 Countermeasures

One of the key countermeasures to equipment theft is employee education. Employees should be aware that it is imperative to report the loss of equipment which includes network enabled devices. In addition, it is equally important to change the settings on the security mechanism used by your organization on a periodic basis. Doing so can minimize the adverse potential resulting from the unreported loss of network enabled equipment.

5.12 Rogue access points

Because the cost of access points have fallen to the point where they can be acquired for petty cash reimbursement, many organizations now face the threat of rogue APs. In this section we will look at this emerging threat to an organization's network security and how to counter the potential security problems associated with this type of communications device.

5.12.1 Overview

Because the cost of access points and a few wireless LAN adapter cards can be easily hidden as a supply expense many departments in large organizations are setting up their own wireless LANs. While the use of a wireless LAN can certainly enhance productivity and facilitate the addition or relocation of stations within an office, when performed without appropriate coordination this network can also represent a security problem. This is because the use of one or more rogue access points is not coordinated with the network manager or LAN administrator due to their very nature of being 'off-the-cuff' equipment. Because rogue access points are unknown to the rest of the organizational network, the use of hardened security techniques (such as VPNs, RADIUS servers or port-based authentication) is normally omitted. This can result in rogue APs becoming the weakest link in an organization's network.

5.12.2 Countermeasures

There are several types of monitoring tools that network managers and LAN administrators can consider using to locate rogue access points. Because most PC Cards include a utility program that indicates signal strength, you can use this type of program in a laptop or notebook computer and move about the building to determine if one or more unofficial access points are in operation. You should consider setting the SSID to either the keyword 'any' or a blank as either setting will normally enable a client station to observe any access point signal within range, regardless of the SSID of the AP.

A second countermeasure to counteract the threat of rogue APs is obtained by acquiring a monitoring tool specifically developed to locate rogue access points. One such tool is the IBM Distributed Wireless Security Auditor, which was introduced by IBM during June 2002. This product uses authorized wireless clients as sensors to detect unauthorized access points, reporting their learned IP and MAC addresses to a central database. That database contains a list of all authorized access points, allowing a search to determine if the discovered AP is known and authorized or unknown and more than likely

unauthorized. Once you locate one or more unauthorized access points, you can inhibit their use through layer 2 or layer 3 filtering on switches or routers. Once people operating the rogue devices realize they need the assistance of networking personnel to access the Internet or devices on the corporate intranet, they will very likely seek assistance from the communications staff. At that time steps can be initiated to examine the security features of the rogue wireless equipment and initiate any appropriate action to harden the device.

chapter six

Proprietary Security Enhancement Techniques

In this chapter we will look at several non-standardized methods that can be employed to enhance wireless LAN security. The methods we will examine have one common feature – they are not endorsed by a standards making organization. Whether this is good or bad depends primarily upon the requirement of your organization to obtain equipment from different vendors that must interoperate in a secure manner. If your organization is comfortable acquiring wireless LAN equipment from a single vendor, then the use of proprietary security enhancement techniques may be suitable to secure your operational environment. In comparison, if your organization needs to acquire wireless LAN products from multiple vendors, the use of one or more proprietary security enhancement techniques discussed in this chapter will normally preclude you from obtaining an equipment interoperability capability. An exception to this interoperability problem will occur if one vendor licenses the use of a proprietary function from another vendor. Although we will describe several proprietary security enhancement techniques in this chapter, we will leave it to the reader to determine if such techniques were licensed for use by other vendors.

While the security techniques described here are proprietary this does not mean they are not provided by equipment offered by multiple vendors. What the term proprietary means in the context of this chapter is that the security features are not standardized. It should also be mentioned that while the security techniques described are not standardized, they are often used in conjunction with one or more standardized methods. Because the use of a non-standardized proprietary security technique with a standardized technique

can reduce or eliminate the potential for equipment interoperability, the proprietary techniques are described and discussed as a separate entity in this chapter. So, lets now take a look at those techniques.

6.1 MAC address authentication

Authentication represents a process which verifies if a specific hardware or a user (or both) has permission to access a network. As we will shortly see, the IEEE 802.11 standard provides authentication based upon the configured WEP key. While it can be argued that a user configured the key and this represents user authentication, this is not true since another person gaining access to the computer with a previously configured WEP key could be authenticated. Thus, WEP's shared key authentication represents a hardware authentication method and not user authentication.

6.1.1 IEEE 802.11 authentication

Under the IEEE 802.11 standard and its extensions there are two methods available for authenticating users, or more correctly, a user's computer, since the person operating the computer is not known. The first method is referred to as shared key encryption and is based upon a client station transmitting an authentication frame to an access point. The access point generates a message consisting of random text, which is transmitted back to the client station. The client station encrypts the received text using its previously configured WEP key and transmits the encrypted message back to the access point. The access point then decrypts the message and compares it to the original. If they are equal the client station is permitted to use the resources of the access point and, in effect, is accepted into the network.

The second method of authentication supported by the IEEE 802.11 standard is Open System authentication. Under Open System authentication any station may become authenticated, resulting in many people referring to this method as null authentication.

In researching material for inclusion in this book, this author reviewed the IEEE 802.11 standard and many technical publications. Although some publications describe MAC address authentication as if it represents an IEEE standard, this is not correct. Instead, MAC address authentication represents a proprietary technique that can be implemented in several ways. Regardless of the method of implementation, MAC address authentication represents a mechanism that verifies the identity of the hardware and not the user.

6.1.2 Implementation methods

There are two basic methods that can be used to implement MAC address authentication. One method involves configuring MAC addresses in an Access Point (AP) while the second method requires the use of a server that is normally connected to the wired network located on the wired side of the access point.

6.1.3 Access point utilization

The first method involves configuring a MAC address control list in each access point. Under this access control method client stations, whose MAC addresses were previously stored in an access point, are provided with the ability to access the network.

6.1.4 Using a RADIUS server

The second method used for MAC address authentication is based upon the use of a RADIUS (Remote Dial-In User Service) server. When a client station connects to an access point the AP queries the RADIUS server with the client's MAC address to determine if the station should be allowed to gain access to the network. The RADIUS server will respond to the access point based upon checking its database for the MAC address provided by the AP.

The primary advantage associated with using a RADIUS server results from the fact that other configuration information can be stored in the server's database. Such information can include username and password, making it possible to perform user authentication and client station or hardware authentication. Thus, the use of a RADIUS server makes it possible to perform hardware and user authentication.

6.1.5 Dataflow

Figure 6.1 illustrates an example of the dataflow that occurs when MAC address authentication is accomplished through the use of a RADIUS server connected to a wired LAN. Note that the access point functions as an intermediary between the client station and the wired network to include the RADIUS server. As we will note in the next chapter, the dataflow for MAC address authentication, when used with a RADIUS server, is similar to the IEEE 802.1x port based authentication dataflow.

6.1.6 Limitations when using an AP

When MAC address authentication occurs using addresses configured in an access point, the AP will block any unknown adapters from connecting to the

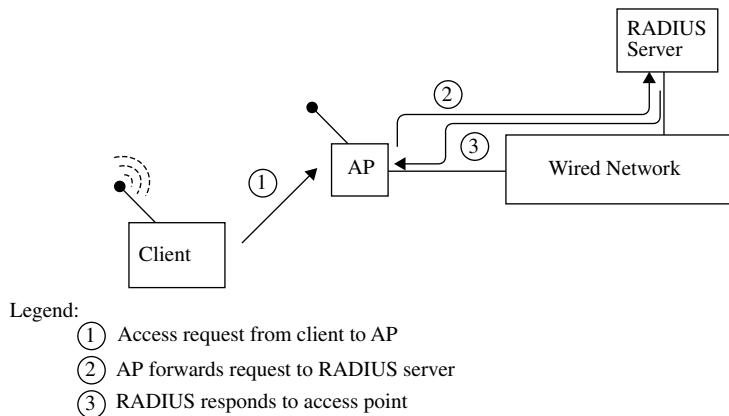


Figure 6.1 Dataflow for MAC address authentication occurring on a RADIUS server.

network. Unfortunately, regardless of the status of WEP encryption the source address of stations can be easily monitored and spoofed by an unauthorized third party. That third party only needs to be within radio frequency range of a client station or access point responding to a client.

As noted earlier, the use of a directional antenna pointed towards an access point located near the window of a building makes it relatively easy for a person sitting in a van in a parking lot to use a notebook computer with a wireless LAN adapter card to monitor and record station addresses. Because many wireless LAN adapter cards support locally administrated addressing, it can be a simple process to override the burnt-in MAC hardware address, replacing it with a software-coded address that mimics one of the source addresses being monitored which is using the network. This technique, referred to as address spoofing, can be used to overcome MAC address authentication when such authentication occurs in the access point.

6.1.7 Limitations using a RADIUS server

When MAC address authentication occurs through the use of a RADIUS server the limitations associated with this technique depends upon how the RADIUS server is used. If the server is used to simply store MAC addresses then the previously described limitation associated with the storage of MAC addresses in the access point are applicable to using the server. Hopefully this would not be the case since this would be a waste of the capabilities of the server.

A more common use of the RADIUS server would be to add support for the use of the Challenge Handshake Authentication Protocol (CHAP). To better understand the capabilities of CHAP, let's digress a bit and first discuss the Password Authentication Protocol (PAP) as a mechanism for the comparison of the two.

6.1.7.1 PAP

The Password Authentication Protocol (PAP) represents a very basic form of authentication. Under PAP a user's name or identification and their assigned password are transmitted over the network and compared at a destination device to a table of name-password pairs stored on the device. Although the passwords are commonly stored in encrypted form in the table, the transmission of both the user's name or identifier and their associated password occurs in the clear. Thus, if you used PAP as a mechanism to obtain user authentication in a wireless LAN environment and MAC address authentication to authenticate the client hardware, both would be capable of being spoofed if you either enabled WEP or agreed with its usual default of being disabled. Now that we have an appreciation for PAP let's turn our attention to CHAP.

6.1.8 CHAP

The Challenge Handshake Authentication Protocol (CHAP) represents a much more secure user authentication method than PAP. Under CHAP an authentication agent, who is typically a network user, transmits a one-time random value and an ID value. Both the authentication agent and client share a pre-defined secret value that the client uses in its response. That is, the client concatenates the random value, ID and secret and computes a one-way hash value using Message Digest 5 (MD5). The hash value is transmitted by the client to the authenticator. The authenticator computes its own hash value using MD5 and compares its resulting computation to the value received from the client. If the two values match the client is authenticated.

Because only the MD5 hash is transmitted to the authenticator it is not possible for a third party to reverse-engineer the shared secret. In addition, because the ID value is varied with each subsequent CHAP authentication process, it is not possible for a third party to initiate a replay attack. Thus, CHAP represents a considerably more secure user authentication method than PAP.

6.1.8.1 CHAP Variations

One popular variation of CHAP is MS-CHAP. MS-CHAP represents a Windows-specific variant of CHAP used by Microsoft remote access and network

and dial-up connection products. Although MS-CHAP is similar to CHAP as defined in an RFC, its response packet is in a format specifically designed for Windows networking products. A second variation of CHAP worth noting was also developed by Microsoft. Referred to as MS-CHAPv2, this second version of CHAP represents a mutual authentication protocol under which both the client and server must provide their identities. In addition to adding mutual authentication, MS-CHAPv2 uses stronger initial data encryption keys and different encryption keys for sending and receiving information, which adds a degree of security beyond MS-CHAP. If your organization operates a Windows 2000 server you will note that for VPN connections the server will offer MS-CHAPv2 prior to MS-CHAP. Microsoft has its specific attributes for MS-CHAP and MS-CHAPv2 authentication via RADIUS defined in RFC 2548.

Because the use of a RADIUS server can support both user and hardware authentication, it provides a higher level of security than simply storing MAC addresses in an access point. Although it is still possible for an unauthorized third party to discover the MAC address in use, this is only a portion of the checking that can be performed when a RADIUS server is used. Thus, the use of a RADIUS server for both hardware and user authentication is more secure than the use of hardware authentication.

6.1.9 Visitor considerations

Another limitation that should be considered and which is applicable to any authentication method is the effect of the method upon visitors. If your organization's location receives many visitors from other locations who require wireless access to the corporate network, this will result in the need for an additional effort by the network manager or LAN administrator in configuring the server database. In addition, depending upon organizational policy, it is very likely that the changes to the server which enable visitor access to the network will need to be removed when they leave.

6.2 Closed system option

In this section we look at a security method that can be easily implemented by vendors on their access points. This security method, which is referred to as a closed system option, permits the network manager or LAN administrator to configure an access point to override any existing network name or SSID setting on an access point.

6.2.1 Overview

As a review, an access point has the ability to filter wireless client stations based on the network name or SSID used by the client. Because there can be multiple access points within radio frequency range of an access point, the use of the keyword ‘any’ or a blank for the network name on a client station enables that station to obtain a list of APs for selection. If only one AP is within radio frequency range of the station the wireless client station can attach to the network by using ‘any’ or a blank for the network name regardless of the setting of the name on the access point.

To prevent a third party from easily attaching to an access point, some APs include a closed system option. Under this option the access point will block client stations that attempt to connect to the network using ‘any’ or a blank for the network name. One example of the use of the closed system option can be found on certain Orinoco access points.

6.2.2 Limitations

The key limitation associated with the closed system option is the fact that the network name can be easily discovered by passive monitoring. Thus, although the closed system option makes it more difficult for an unauthorized third party to connect to an access point, it does not prevent that action from occurring.

6.3 System access pass phrase

One interesting proprietary method for enhancing wireless LAN security is obtained through the use of a system access pass phrase. This term is used by KarlNet, Inc. to reference a string of up to 32 characters that is encrypted in a one-way hash to prevent eavesdropping on the wireless medium. The system access pass phrase is used in place of the SSID or network name to obtain a secure mechanism for establishing a connection between wireless systems.

6.3.1 Overview

KarlNet focuses upon wireless point-to-multipoint solutions that enable multiple buildings to obtain communications interoperability. The company uses its own proprietary protocol referred to as TurboCell as an overlay to such existing radio protocols as the IEEE 802.11 standard to minimize the effect of packet loss. Because inter-building communications occur using RF the

company added two enhancements to its TurboCell protocol to improve upon the 802.11 security model. Those enhancements include TurboCell two-way authentication and RADIUS server support.

6.3.2 Network access

In a standard IEEE 802.11 wireless LAN the network name or SSID is used as a mechanism for a client to associate itself with an access point. In a KarlNet TurboCell environment the system access pass phrase is encrypted in a one-way hash to prevent eavesdropping on the wireless medium. As an additional level of protection the system access pass phrase is also protected by the use of a license number associated with the TurboCell software driver. Through the use of a license number users can be restricted to a particular access point and are precluded from changing their pass phrase to gain access to a different TurboCell network which they are not authorized to access.

6.3.3 Limitations

The use of an access pass phrase represents one of three methods used by KarlNet devices to provide TurboCell authentication. The other two methods include MAC address or hardware authentication and user authentication occurring by the client specifying a username and password used by CHAP. Both hardware and user authentication are supported through the use of a RADIUS server. Although the use of the access pass phrase and support for hardware and user authentication preclude an unauthorized third party from accessing a TurboCell network, these security features do not prevent an uninvited third party from monitoring and recording network traffic. If a TurboCell network relies on the use of WEP for encryption, this means that the underlying network is vulnerable. Thus, while the access pass phrase and use of hardware and user authentication protect the network from unwanted access these features do not protect network traffic. Because WEP is vulnerable to compromise via key recovery, this means the TurboCell, which is used for inter-building communications, could have its transmission at risk.

Similar to other authentication methods beyond a shared key mechanism, another limitation of a pass phrase concerns visitors. That is, when a visitor requires the use of a TurboCell network, the configuration of the RADIUS server must be modified.

6.4 Dynamic key exchange and weak key avoidance

Earlier in this book we noted that there are several readily accessible software programs that can be used to recover the WEP key in use. Such programs work

by first obtaining a database of approximately five to six million frames. Those frames are then analyzed based upon the fact that certain initialization vector values are, in effect, weak keys. Because certain IV values are predictable and it is relatively easy to guess the value of certain fields of IP traffic contained in a wireless frame, a program such as AirSnort can recover the WEP key from an analysis of a sufficient database of frames.

There are basically two methods that can be used to block AirSnort and similar programs from performing their dastardly deed. Those methods are dynamically changing the WEP key in use or changing the manner by which IV settings occur.

6.4.1 Dynamic key exchange

Dynamic key exchange results in an access point periodically exchanging WEP keys with its clients. Although this may appear to be a relatively simple process, both client and access point must be programmed to support the same method of key exchange, referred to in some literature as key rollover. In addition, if keys do not change frequently it is possible that a sufficient base of frames can be captured by a third party to recover the key in use. If this happens, all previously recorded traffic which used that key is subject to being compromised.

6.4.2 Overview

Some vendor products permit the network manager or LAN administrator to define the number of frames that can flow over the network prior to a key exchange occurring. Other products permit the network manager or LAN administrator to define a time interval at which key exchanges occur. When a time interval is employed care must be used to ensure that the interval is less than the time required to transmit several million frames. If not, a sufficient database could be constructed by a third party that would enable the WEP key to be recovered. Then, once the key is recovered, previously captured encrypted frames and subsequently transmitted frames could be decrypted.

6.4.3 Limitations

Because dynamic key exchange can represent a proprietary technique one limitation is a lack of interoperability between different vendor products. An exception to this limitation is an evolving standards based key exchange mechanism that will be discussed in Chapter 7.

Another limitation associated with dynamic key exchange concerns visitors. Because the methods employed to support dynamic key exchange were proprietary when this book was prepared, a visitor would need to have the same vendor hardware as other clients located at the visited site.

6.4.4 Weak key avoidance

A second method that can be employed to harden WEP encryption is to modify the firmware of wireless stations. That modification is designed to enable the random IV selection process to skip over predefined IVs that represent weak keys.

6.4.5 Overview

The goal behind weak key avoidance is to modify the random IV selection process to skip over weak keys. In actuality, the IEEE 802.11 standard does not define how IVs are selected, so vendors are free to use any criteria. However, because some keys are more susceptible to having their encrypted results reverse-engineered than other keys, skipping over weak keys provides a method for making life more difficult for people using AirSnort and similar programs.

One example of weak key avoidance is Orinoco WEPplus stations. Originally developed by Agere Systems, its Orinoco product line was sold to Proxim during 2002.

6.4.6 Limitations

As in dynamic key exchange, the use of firmware to skip over IVs that produce weak keys is proprietary to a specific vendor. An exception to this is a feature within the Temporal Key Integrity Check Protocol, which will be discussed in the next chapter. When using a proprietary method to skip over weak keys, this action can adversely affect visitors from another company site that use a different vendor wireless product even if they configure their client with the same initial WEP key. This is because, for example, the Orinoco products have firmware that skip over IVs that create weak keys while other vendor products do not. Thus, the use of other vendor wireless products could represent a literal weak link that would enable an unauthorized third party to construct a database which could be used to recover the key in use.

6.5 Protecting wireless clients from the public network

One interesting aspect associated with the field of wireless LAN security is the primary focus upon authentication, authorization and encryption. While each

of these functions is very important, they are all oriented towards providing a secure connection from each wireless LAN client to an access point and through that AP onto the wired network. What is very often overlooked is the fact that the wired LAN most organizations wireless clients are connected to is in turn connected to a public network, such as the Internet. Although many organizations protect their private network from the public network through the use of a firewall or router access list, not all organizations use the former or configure the latter. In addition, many smaller organizations or branch offices of larger organizations may not have the personnel or monetary resources to obtain a high level of protection for their internal network through the use of a firewall or by configuring a conventional router access list. Instead, such organizations may be dependent upon the filtering capabilities of the combined access point router used to provide multiple wireless LAN clients with access to a cable modem or DLS connection to the Internet.

6.5.1 Overview

The use of a combined access point router represents your first line of defense when connecting to the Internet. Recognizing this fact, some equipment vendors include a layer 3 packet filtering capability in their products. While there are no standards covering the manner by which packet filtering occurs, a *defacto* standard is the capability and functionality afforded by Cisco routers. Thus, to obtain a foundation for a comparison of capabilities, let's briefly review the functionality of Cisco access lists.

6.5.2 Cisco access lists

Cisco supports two basic types of access lists – basic, more commonly referred to as standard, and extended.

6.5.2.1 Standard Access List

A standard access list is limited to filtering on the source address and uses the following format:

```
access-list list number [permit|deny] source address wildcard mask
```

The list number ranges from 1 to 99 and defines the list as a standard IP access list, denoting that the statement is part of one or more statements that make up the access list. Following the list number is either the keyword ‘permit’ or ‘deny,’ which matches packets with the defined source address and wildcard

mask and either permits the packets to flow through the router, or if deny is used, sends matching packets to the great bit bucket in the sky.

The source address represents a dotted decimal IP address. To support defining a group of addresses, Cisco used the reverse of a subnet mask, which is referred to as a wildcard mask. That is, a binary ‘1’ is used to represent a don’t care condition while a binary ‘0’ is used to represent a match. Thus, to enable all packets from the 198.78.46.0 network to flow through the router the standard access list statement would be created as follows:

```
access-list 1 permit 198.78.46.0 0.0.0.255
```

In the preceding example, the wildcard mask of 0.0.0.255 represents a don’t care condition for matching the host portion of the IP address while the zeros in the mask require the network portion of the address to be matched. Thus, the wildcard mask of 0.0.0.255 permits packets whose network address is 198.78.46.0 to flow through the router regardless of the host address.

6.5.2.2 Extended Access List

In comparison to the standard access list that is restricted to filtering upon source addresses, an extended access list is far more powerful. An extended access list can filter on source and/or destination address, source and/or destination port and many additional parameters which includes specifying a range of ports. The general format of a Cisco extended access list is shown below:

```
access-list list number [permit|deny]
<protocol><source address><wildcard mask><source
port><destination address><wildcard mask><destination
port> keyword(s)
```

Like a standard access list, the list number in an extended access list defines the type of access list and associates statements to a particular access list. For example, an extended IP access list has a list number from 100 to 199. Both source and destination addresses represent IP addresses in dotted decimal format. Similarly, the wildcard mask following source and destination addresses are a dotted decimal number for which a binary ‘0’ represents a match while a binary ‘1’ represents a don’t care condition. Source and destination ports can be defined via numerics or mnemonics with http and www equal to 80 when defining Web services.

The protocol entry can be used to specify a specific protocol for filtering, such as IP, ICMP, TCP or UDP. When you create an access list with several

statements it is important to remember that the IP header in a datagram prefixes ICMP, TCP and UDP. Thus, if you create an access list statement that allows IP with certain parameters, you cannot then create a subsequent deny TCP statement with those parameters as statements are processed top down and the match on the first statement would preclude the next statement from being executed.

There are many keywords that can be used with Cisco access lists to control their functionality. One popular keyword is 'established,' which results in the filtering of TCP datagrams with their ACK or RST bit set.

Statements in both standard and extended access lists are processed sequentially, top down. Once a match occurs between the parameter or parameters defined in a statement in the access list and one or more fields in the packet, the packet is either permitted or denied to flow through the router. Each router port can have two access lists, one applied in the inbound direction and another applied in the outbound direction. Here the terms 'inbound' and 'outbound' are with respect to the router.

In a Cisco router environment, many additional features were added to access lists through the release of new versions of the vendor's Internetwork Operating System (IOS). One example is time-based access lists which are not actually separate access lists, but add the capability to define when one or more statements in an access list should go into effect.

Until late 2002 Cisco access lists were not supported on that vendor's wireless equipment. However, in late 2002 Cisco added support for its IOS to a new series of wireless products. Because IOS supports standard and extended access lists, it is now possible in a Cisco equipment environment to control the flow of data to and from a wired network via access lists operating on an access point.

6.5.3 SMC Networks Barricade packet filtering

Due to the complexity of Cisco access lists more vendors offer a limited functionality menu driven packet filtering capability in their combined access point router. One example of this type of access list menu is provided by SMC Networks in their Barricade Broadband router, which represents a combined access point and router developed to provide wireless network connections to a wired LAN, in addition to routing via a cable modem or DLS connection to the Internet.

Figure 6.2 illustrates the SMC Networks Barricade Broadband router access control screen. If you look at the address field in the browser screen display shown in Figure 6.2, you will note the RFC 1918 address of 192.168.123.124.

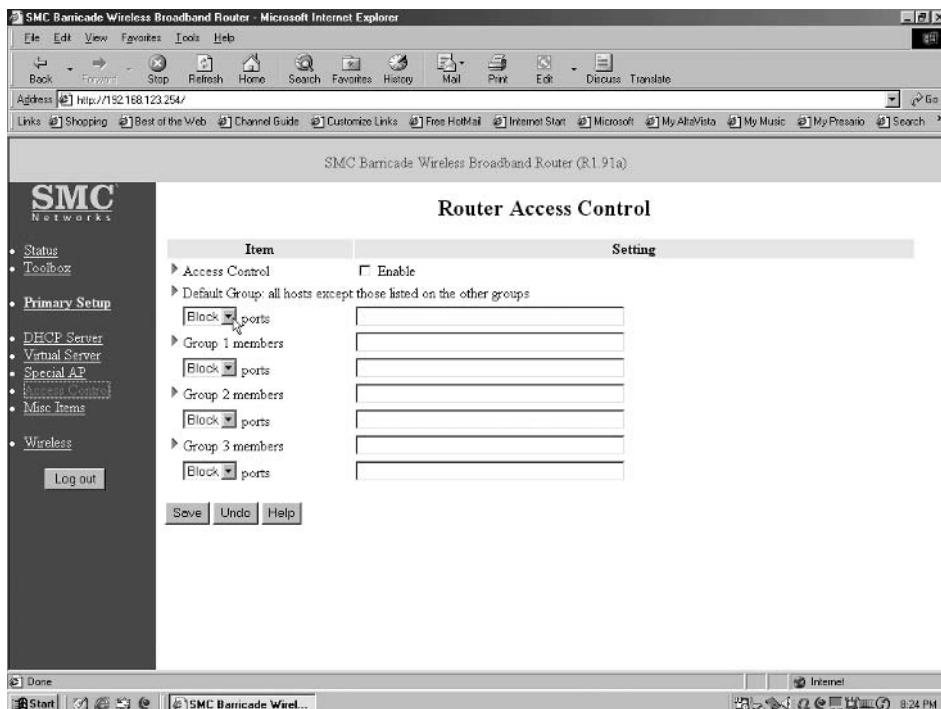


Figure 6.2 The SMC Networks Router Access Control menu provides a one-way filtering capability from wireless LAN clients through the router.

That is the default IP address assigned to the router which you might wish to consider changing to make it more difficult for an unauthorized third party to attempt to access your router's administration capabilities. Concerning the potential access of the administrative capabilities of a router, most access points and routers, in addition to combined access point routers which includes the SMC Networks Barricade, are preconfigured with a default password. That password should be changed during the initial configuration process of the device since its composition can easily be determined by visiting the vendor's Web site and viewing their online manuals.

Returning our attention to the Router Access Control display in Figure 6.2, SMC Networks provides you with the ability to assign clients to three different groups (1, 2, 3) and configure a default setting for all hosts other than those listed in the other groups. Clients are assigned to Groups 1, 2 or 3 by the use of the host portion of their IP address. For example, to assign clients with the IP addresses 192.168.123.10 through 192.168.123.25 you would place the entry

10–25 in the field labeled ‘Members’ for Group 1. Under each group including the default group is a pull down menu, with each entry shown by default set to ‘Block.’ This setting will block or deny packets that match the defined members and port entries for the members. The other pull-down menu entry is ‘Allow’ which enables frames matching the members and ports entry for a group to flow through the router.

The ports entry requires you to place the port number for a specific application or series of applications. For example, to allow wireless clients with RFC 1918 addresses 192.168.123.10 through 192.168.123.25 to surf the Web and Telnet to various Internet sites, you would enter 10–25 in the members field for a particular group and 23, 80 for the ports field. Here 23 represents the Telnet port number while 80 represents the port Web traffic flows on.

6.5.4 Limitations

The access control method provided by SMC Networks only filters on outbound transmission. So while the SMC Barricade access control facility can be used to control access from behind the combined access point router to the Internet, it does not support a reverse capability. However, by carefully tailoring access control it becomes possible to develop a secure wireless LAN communications capability whether or not the router is connected to the public Internet or the corporate network. For example, by configuring access control to only allow secure http (https) through the router, you can restrict all communications from wireless LAN clients to secure layer 3 communications.

By securing traffic through the router to https via port 443 you can restrict communications through the router to HTTP over TLS, where TLS represents the successor to SSL. Doing so enables you to connect a secure Web server in front of the combined access point router, resulting in secure communications flowing to your organization’s wired network. As an alternative or supplement to the preceding, any Internet connection in front of the router will be restricted to secure communications.

While the use of HTTP over TLS provides secure browsing, it has certain limitations. For example, restricting outbound wireless LAN traffic through the combined access point router to secure Web browsing could restrict the ability of users to access email, make Telnet connections and use other TCP/IP applications. Here the restriction would be based upon the use (or lack of) of certain vendor products that support TLS as an access mechanism to multiple applications.

Because the prior access control example showed a one-way filtering capability on the SMC Networks Barricade router, we need to examine another

router menu screen to obtain more additional information about the capability of this communications device. That menu is the Miscellaneous Items menu that is shown in Figure 6.3. This menu includes five entries, which we will now focus upon.

The first entry in Figure 6.3, ‘IP address of DMZ Host,’ provides a network administrator with the ability to specify a computer that can bypass the protection of the firewall feature of the Barricade router. When you enter a host address and enable this feature it allows the specified address to have unrestricted 2-way communication through the router.

The ‘Remote Administrator Host’ entry, when enabled, provides access to the router’s administration capability remotely. Because the use of an IP address of 0.0.0.0 permits any host to remotely connect to the router to perform administrative tasks, enabling the default can be dangerous. When

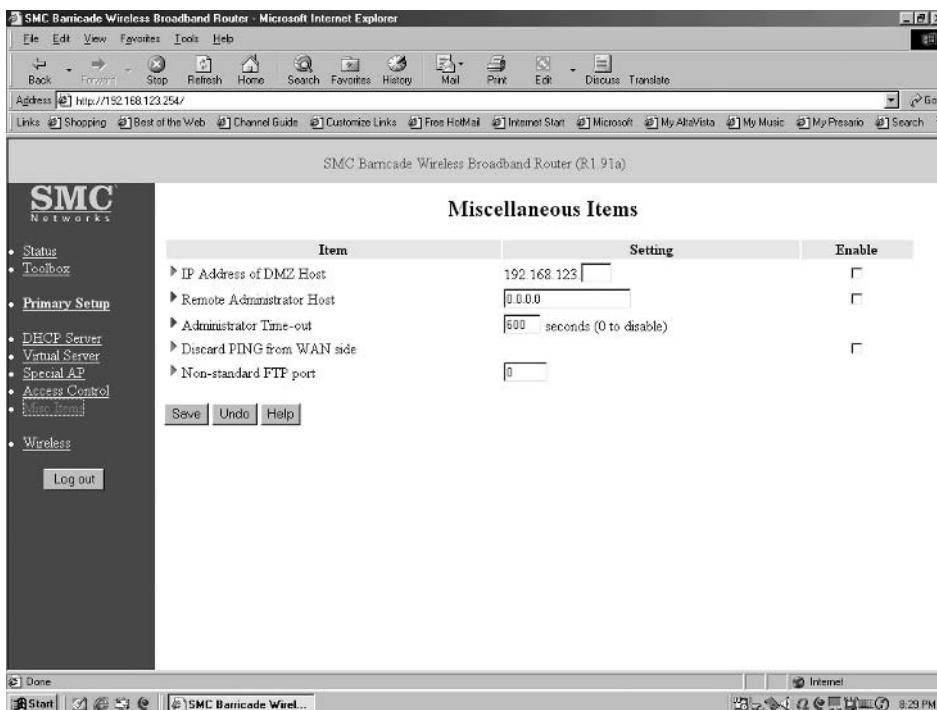


Figure 6.3 Through the use of the SMC Networks Barricade router’s Miscellaneous Items screen, you can control remote administrative access to the device, discard Pings arriving on the WAN, and support the use of a non-standard FTP port.

remote administration is set it uses a default inactivity timeout value of 600 seconds or 10 minutes, after which the Barricade router will automatically close the administrator session. If you set this entry to a value of 0, it disables the inactivity timeout feature and permits hosts establishing an administrative session to retain a connection regardless of their activity.

The ‘Discard Ping from WAN side’ represents a limited ICMP filtering capability. When this feature is enabled no host on the wide area network in front of the router can Ping the device.

The last option in the Miscellaneous Items menu is ‘Non-standard FTP port.’ When this feature is enabled it provides you with the ability to hide an FTP server from observation by a host on the public network by entering a port number other than FTP’s port 21. Because the Barricade broadband wireless router includes three 10/100 Mbps switched Ethernet ports, a network manager could configure this device to support an FTP server and other devices that are connected to the switch ports and wireless LAN client stations, hiding the FTP server from general observation via the use of a non-standard FTP port number. Unfortunately, this action can be easily discovered through the use of port scanner software. Thus, the use of a non-standard FTP port should not be viewed as a security mechanism.

6.5.5 Summary

While the use of Cisco Access lists or a fully featured firewall can provide a significant bi-directional packet filtering capability that can control Internet access to wireless clients, the same may not be true when using certain types of combined wireless access point routers. As indicated by our examination of the SMC Networks Barricade router, filtering is primarily used to control access from wireless clients to the Internet. The few Miscellaneous Items menu features, such as discarding Pings from the WAN side or using a non-standard FTP port, represent either a rudimentary security feature or a simple inconvenience to a hacker. The Barricade is no different from many other combined access point routers examined by this author.

If you need to limit the flow of traffic from the wide area network to wireless LAN clients you must consider the use of a firewall or a conventional router with a fully featured access list capability or the recently introduced Cisco access points that now support IOS. As an option you can consider installing personal firewall software on each client or activating the built-in limited function Windows XP filtering capability if your clients use that operating system.

6.6 Antenna orientation and shielding

Earlier in this book we noted a simple truth that the inability of a third party to pick up an RF signal also results in their inability to decode the signal. In this section we will note how you can consider orienting the antenna on your access point and also use shielding to minimize the RF signal strength that flows beyond the wireless clients the AP must service.

6.6.1 Overview

In Chapter 3 we looked at antenna signal strength and saw that it could be altered by orienting or positioning the antenna of an access point and through the use of shielding. We primarily focused on the signal strength of the RF signal transmitted by an access point because they use positional omnidirectional antennas and many APs also support the use of the connection of other types of antennas, such as directional antennas. In comparison, almost all client stations obtain a wireless LAN communications capability through the use of an antenna built into the PC Card that cannot be altered. Because we can position or modify the antennas used by most access points we can alter their signal strength.

6.6.2 Altering signal strength

When altering the signal strength of an access point we can note the received signal strength at various locations within and outside of the building where the AP resides. To do so we can use the utility program normally bundled with each client station. For example, if you were using a Cisco 340 series Aironet wireless LAN adapter you could use the Aironet Client Manager, bundled with the wireless LAN adapter, to measure signal strength as you move your laptop or notebook computer inside and outside the building where the access point is located. To facilitate the positioning of access point antennas or the use of shielding normally requires the efforts of two people, a laptop or notebook and a cell phone or email from the laptop to the person left behind at the AP. The person using the laptop or notebook computer would use the client utility program's signal strength indicator.

One example of a signal strength indicator is the Cisco Site Survey screen bundled with the Aironet Client Manager, which is shown in use in Figure 6.4. In this example the signal strength indicator is shown at 72 percent for a link speed of 11 Mbps. When positioning the antennas on the access point or using shielding you want to minimize signal strength towards zero at a data rate of 1 Mbps for those areas outside the control of your organization. In

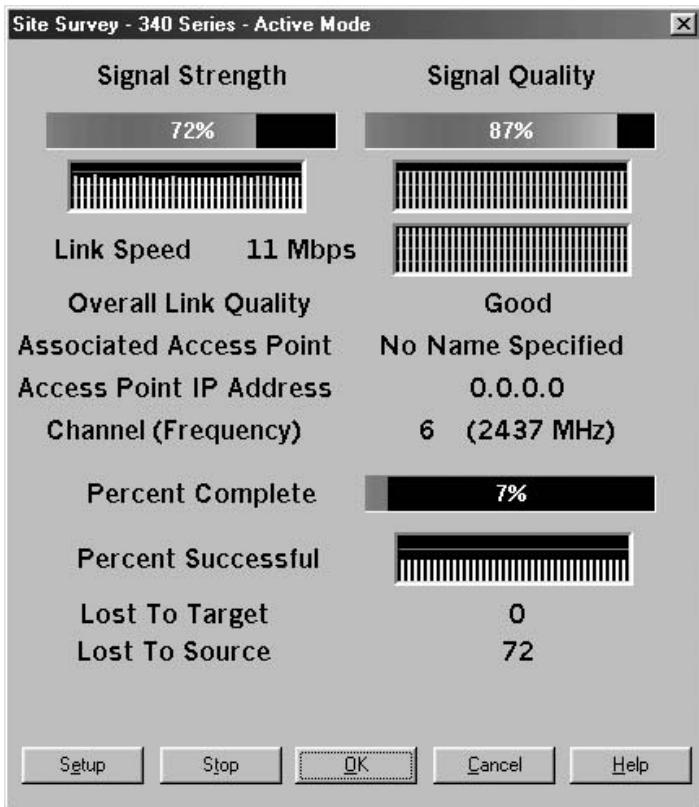


Figure 6.4 The Cisco 340 Series LAN adapter software includes a site survey screen that indicates the signal strength of the received signal.

a tall building with different companies on each floor this would involve minimizing signal strength flowing onto different floors as well as outside the building. In comparison, if your organization controls access to the entire building your primary focus would be upon limiting the strength of the RF signal outside of the building. Doing so would prevent anyone from sitting in a parking lot while monitoring and recording your transmissions.

6.6.3 Limitations

The key limitation to antenna orientation and shielding is the topology of your wireless LAN. If your wireless LAN clients are distributed throughout a floor around an access point you need to use an omni-directional antenna.

In addition, shielding would be limited to minimizing RF energy flowing to other floors in the building. However, it may be possible to relocate the access point to the wall in a building that enables shielding to the rear of the AP. Thus, antenna orientation and shielding plus the use of different utility programs to monitor signal strength at different locations can represent a time-consuming process.

6.7 Minimizing transmit power and antenna control

In this book we have often noted that an unauthorized third party who cannot hear your wireless LAN signal cannot intercept your communication. There are basically two methods that can be used to minimize RF energy. In the prior section we reviewed antenna orientation and the use of shielding. In this section we will describe a second possibility that can be obtained when your equipment supports more than one transmit power level and you can control the use of multiple antennas. Because some readers may confuse the power management function of wireless LANs with their transmit power level, we will first focus on the former.

6.7.1 Power management

IEEE 802.11 stations incorporate a power management capability that enables laptops and notebooks operating on battery power to conserve power. Stations changing their power management mode of operation inform the access point they are associated with of this through the appropriate setting of bits within the frame control field of transmitted frames. Upon receipt of notification that a station is in a power save mode of operation the access point will buffer frames destined to the client, transmitting them at designated times.

When a station is placed in a power save mode of operation it will periodically listen for beacon frames transmitted by the access point. Upon receipt of a beacon frame the station will wake up and transmit a poll to the access point. The access point will then either acknowledge the poll or respond to the station by transmitting any buffered frames destined for the station.

A station can be in one of two different power states, referred to as awake and doze. In the awake mode a station is fully powered. By comparison, in a doze power mode a station is not able to transmit or receive and consumes a very low level of power.

By default a client station's power save mode is set to OFF. Most client hardware includes either a utility program or an initial configuration screen that enables you to turn the power save mode to ON. Figure 6.5 illustrates

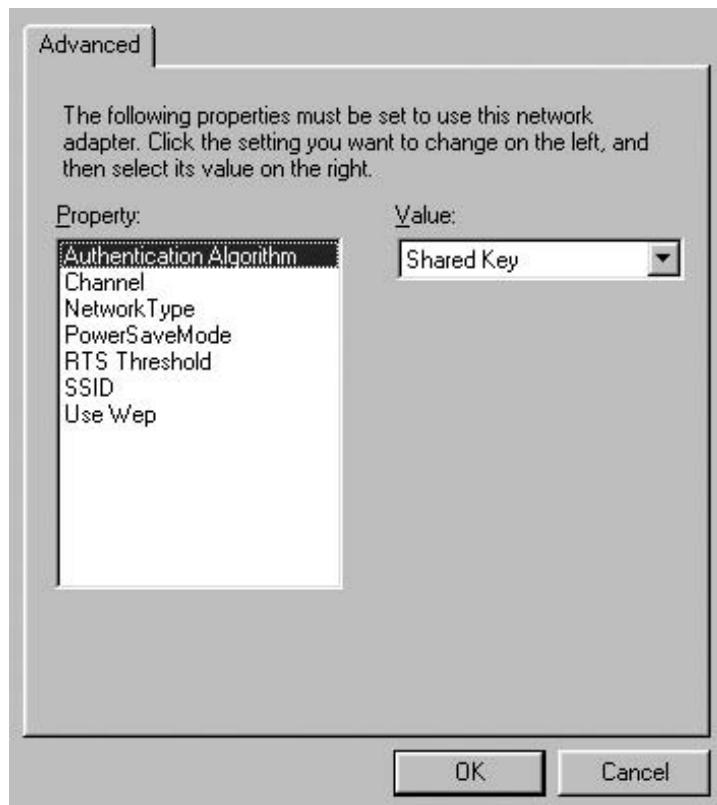


Figure 6.5 The SMC client setup menu permits you to enable the client's power save mode of operation.

the initial SMC Networks Client EZ Card setup menu display. By moving the highlight bar over the 'PowerSaveMode' property in the left portion of the screen, you will be able to either enable or disable the mode by selecting the applicable entry from the pull-down menu in the window labeled 'Value.'

Setting the power save mode to ON has no actual effect upon the ability of a third party to listen to RF energy emitted by the device. This results from the fact that when the station wakes up from its doze mode, it will transmit at its previously set transmit power level. Thus, a power save mode in effect toggles the transmit power level between zero (doze mode) and the previously set transmit power level. Instead, you can limit the ability of an unauthorized third party from hearing your client transmissions by controlling the use of the antenna and/or limiting the transmit power of the device.

6.7.2 Antenna control

Under the IEEE 802.11 standard there is no limit to the number (N) of antennas a device can support, although in a practical sense two is the maximum. Each antenna can be selected for transmit or receive functions which can vary either dynamically or be set for a static operation. Thus, if your client or access point has multiple antennas you may be able to use the utility program bundled with the hardware to both control antenna usage and monitor the affect of the RF signal strength pattern. You would monitor the signal strength pattern by using a notebook with a wireless PC Card and move about the area, observing the signal strength as you control the antennas on clients access points.

6.7.3 Power level control

A second method you can use to make life difficult for an unauthorized third party lurking in the shadow of the garage or parking lot is obtained by controlling the transmit power level of your hardware. Under the IEEE 802.11 standard eight transmit power levels can be defined, ranging from TxPowerLevel1 to TxPowerLevel8, with the actual level left to the hardware developer within the constraints of the Federal Communications Commission regulations governing operations in the 2.4 GHz and 5 GHz frequency bands. Figure 6.6 illustrates the use of the RF Network tab on a Cisco 340 Aironet client utility program to adjust the transmit power of that device. By default Cisco Aironet clients are set to use 1 mW of transmit power; however, as indicated in Figure 6.6, transmit power can be reset to 30 mW. In this particular example the Cisco 340 Aironet client card is limited to two transmit power settings, although up to eight could be supported by devices compliant with the IEEE 802.11 standard. By carefully examining the transmit power settings on your wireless LAN hardware, in conjunction with a mobile notebook using a signal strength monitor, you can determine not only an appropriate setting for communications within your infrastructure, but also a setting that minimizes RF radiation outside your infrastructure area. By using the transmit power setting in conjunction with the antenna placement of your hardware, antenna positioning and the use of one or dual antennas, you may be able to maximize RF communications within your infrastructure while minimizing radio frequency radiation outside of the infrastructure. Although the process associated with adjusting or replacing antennas, positioning equipment, installing shielding and adjusting transmit power can be quite lengthy, the achievable result can minimize organizational risk. As stated several times in this book and repeated once more for emphasis, if an unauthorized third party cannot hear your communications they cannot listen to them. While the adjustment

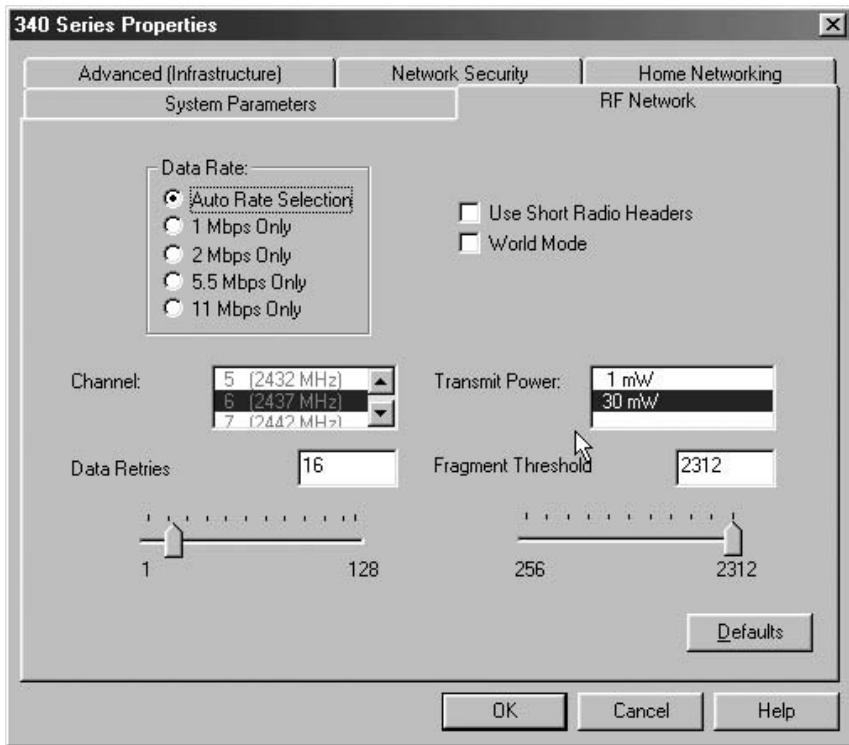


Figure 6.6 The Cisco 340 client utility program permits transmit power to be set to either 1 mW or 30 mW.

of transmit power, the positioning of antennas and the use of shielding is no substitute for encryption, it represents one additional technique you can consider to harden your network.

6.7.4 Limitations

There are two key limitations associated with antenna control and minimizing transmit power of client stations. First, not all products necessarily support one or both features. Secondly, it can be quite time consuming to adjust antennas and transmit levels for an optimum level of performance within an infrastructure that minimizes RF radiation outside of the infrastructure. Depending upon the location of access points and clients it may not be possible to minimize RF radiation outside of your organization's infrastructure. In fact, because clients located far from an access point may not be able to reduce

their transmit power level it is not always possible to minimize the transmit power to reduce RF energy flowing outside your organization's building even when your equipment supports this capability.

6.8 Wireless intrusion detection

In this section we will look at a specific vendor product that provides a wireless LAN intrusion detection capability. Referred to as AirDefense, this product included some features that appeared to be unique at the time this book was prepared.

6.8.1 Overview

AirDefense represents a novel approach to wireless LAN security. Instead of attempting to establish an active defense mechanism through encryption, the use of authentication, or another scheme, AirDefense represents a passive monitoring technique which consists of distributed radio-based sensors in the form of software operating on Windows based computers. The software works in conjunction with wireless LAN PC Cards to determine if there are unauthorized access points or wireless packets flowing on the air from unknown users. It also searches for access point vulnerabilities. The combination of AirDefense software and wireless LAN PC Cards results in a sensor that applies a series of algorithms to a database of predefined wireless LAN information to detect changes to the network. If certain changes occur, such as the flow of packets to a previously unknown station, software will indicate this on a management console, enabling the LAN administrator to take action.

6.8.2 Limitations

Although AirDefense can be considered as equivalent to an intrusion detection system, it does not provide any defense against the passive monitoring of a network. For example, if an unauthorized third party located in a parking lot is able to monitor and record your wireless LAN traffic for future analysis, AirDefense would be none the wiser. Then, if your wireless LAN simply used a static WEP key the third party could recover the key in use and decode your user's transmissions. While AirDefense may be able to detect the third party attempting to break into your wired LAN through an access point, it does not provide any additional security to your existing communications. Thus, its use should be considered as a supplement to hardening your existing wireless infrastructure.

6.9 LEAP

LEAP, an acronym for Lightweight Extensible Authentication Protocol, represents a derivative of the standardized Extensible Authentication Protocol (EAP) whose use will be described in Chapter 7. LEAP was developed by Cisco Systems and is a popular example of several EAP-based derivatives that can be used within the IEEE 802.1x port level access control protocol standard that is covered in the next chapter.

6.9.1 Overview

As its name implies, Cisco Systems' Lightweight Extensible Authentication Protocol (LEAP) represents an authentication method for verifying the identity of a user. Though similar to the IEEE 802.1x standard, LEAP is proprietary and only works with Cisco Aironet equipment. LEAP includes support for refreshable WEP keys on a per-client, per-session basis. Although dynamic keys do not alleviate the weakness associated with using RC4 with a 24 bit IV, it makes it impractical to attempt to exploit the weakness of the encryption algorithm since the key interval does not remain static long enough for a sufficient database to be created for a key recovery process.

LEAP represents one of several authentication algorithms supported by Cisco Aironet wireless LAN products. Other authentication algorithms supported by Cisco Aironet wireless LAN products include EAP-Transport Layer Security (TLS) and probably, by the time you read this book, an emerging algorithm referred to as Protected EAP (PEAP) which was an Internet draft when this book was prepared.

The IEEE 802.1x standard represents a port-level access control protocol. Although we will focus upon this standard in the next chapter, it should be noted that this standard leaves the choice of the authentication algorithm and the manner in which encryption keys are managed up to each EAP authentication method employed. Under the Cisco Systems LEAP algorithm a combination of username and password is employed for authentication. Authentication under LEAP occurs mutually between the user and the access point the user is attempting to connect to. This two-way method of authentication protects an organization from an unlikely but still possible setup of an unauthorized or rogue access point. In addition, as previously noted, the WEP key is assigned on a per user, per session basis, which functions as a mechanism that hardens the vulnerability of WEP.

6.9.2 Operation

An Aironet client station configured to use LEAP initially operates like other wireless clients. That is, the client listens for beacons from a wireless access point which announces the presence of the AP. When the client hears the beacon, it transmits a DHCP request along with its SSID to the AP. The access point will forward the request on behalf of the client to an authentication server connected to a wired network behind the AP. The client will also transmit its username to the AP, which is also forwarded to the authentication server.

Upon receipt of the DHCP request and client username the authentication server returns a challenge that flows back to the wireless access point. The access point forwards the challenge to the client as an EAP message based upon the IEEE 802.1x protocol.

If the client does not receive the appropriate challenge it will proceed to disassociate itself from the wireless access point and look for another AP to associate with. Assuming the client receives the challenge, it runs the challenge through the Cisco LEAP algorithm. In doing so the client mixes the challenge and user password together to create a hash value which is transmitted to the authentication server via the access point.

At the authentication server the user password is run through the Cisco LEAP algorithm which processes the challenge and client response. The derived value is then compared to the value the server received from the client. If the two values match, the client is assumed to be authenticated and the authentication server transmits a success message to the access point which forwards this message to the client.

Because LEAP represents a mutual authentication process the client now needs to reverse the LEAP process to authenticate the server. To do so the client transmits a challenge to the authentication server via the access point. Assuming the server responds correctly and the server is authenticated, the client transmits a success message through the AP to the server. In doing so the AP opens access to the client which enables access to network facilities.

The receipt of a success message by the authentication server functions as a mechanism for distribution of a WEP key. That is, the Cisco LEAP RADIUS server will transmit a WEP key for the client session to the AP that will be stored in the access point.

6.9.3 Configuration

Because the configuration process associated with using Cisco LEAP provides some valuable information about the use of authentication and pitfalls that can occur when other devices, such as routers and firewalls, are located between

the client and server, we will briefly describe certain aspects associated with enabling LEAP. Although you must obviously configure your access point, client stations and server, as we will shortly note, you may need to make modifications to your organization's routers and firewalls if such devices reside between the clients and authentication server.

6.9.4 Configuring the access point

Cisco access points can be configured to support several types of authentication. When using LEAP you would browse to the AP, select the Services menu from Setup, and then click on the 'Security' option. From the Security option you would select 'Authentication Server' which will provide a menu you can use to define up to four authentication servers.

When you use the Cisco authentication configuration screen you will need to define the version of the 802.1x standard which will run on the access point. You will also need to specify the IP address, server type, UDP port number and shared secret value for each server. The server type would be set to RADIUS, while the port number would be set to 1645. Because a RADIUS server uses UDP for communications, this means that if your organization has a router or firewall located between the access point serving the client and the authentication server, you need to ensure the intermediate device is configured to allow traffic on UDP port 1645 to pass.

The Cisco authentication configuration screen for a Cisco 350 access point supports either EAP or MAC address authentication. Because they are mutually exclusive, you would select the checkbox for EAP authentication. For each server a preconfigured timeout of 20 seconds can be changed. This timeout value represents the period of time the access point will wait prior to selecting the next configured authentication server.

Once you enable LEAP you can return to the Security Setup screen and click on 'Radio Data Encryption' to enable WEP. You would configure a broadcast WEP key by entering a 40 or 104 bit key value. In addition, you also have the option of specifying a broadcast key rotation.

6.9.5 Client configuration

Once you configure the access point and RADIUS server you need to configure each client to support the use of LEAP. To accomplish the latter you would use the Cisco Aironet Client Utility (ACU) program that is bundled with your wireless adapter card.

Figure 6.7 illustrates the System Parameters tab display on a Cisco 340 Series ACU screen. The System Parameters tab is shown placed in the foreground of

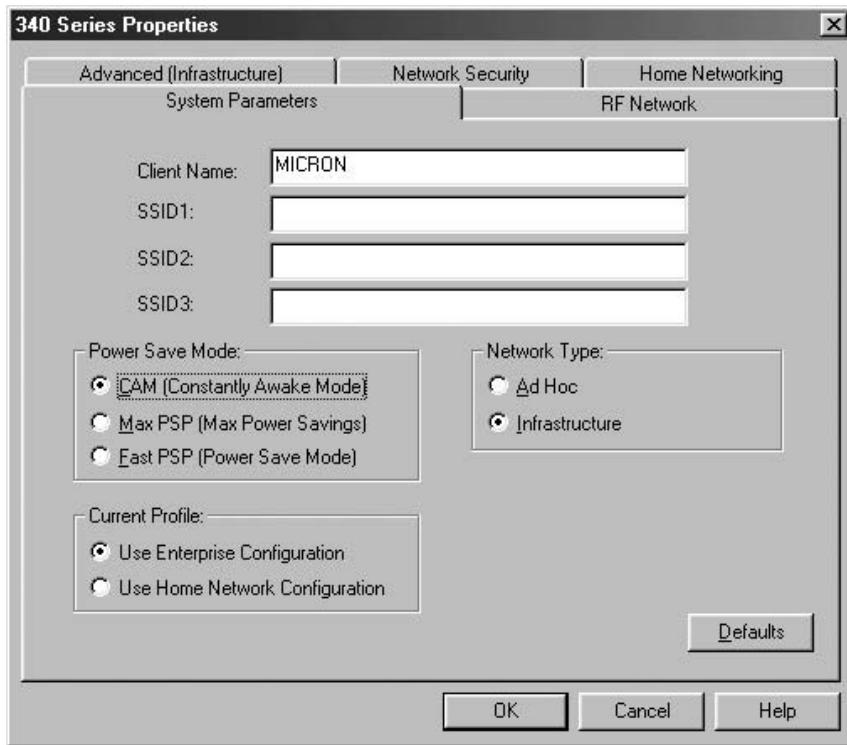


Figure 6.7 The System Parameters tab on the Cisco 340 Series Aironet client utility program.

the screen. You would enter the appropriate SSID in the SSID1 box to enable the client to access the network controlled by the access point you wish to use. If you are using a Cisco 350 Aironet client, the display of the System Parameters tab will be slightly different, with the 'Current Profile' section shown in the lower left portion of Figure 6.7 omitted. Once you enter an appropriate SSID and ensure the default setting of 'Infrastructure' for the network type is selected, you would click on the tab labeled 'Network Security.'

The Network Security tab for the Cisco 340 Series Aironet Client Utility program is displayed in Figure 6.8. If you carefully examine this figure you will note that although you can set server based authentication to LEAP or EAP, you cannot use this screen to change keys. As we will shortly see, Cisco 340 and 350 series clients use a separate encryption manager program for key setting. Because WEP is not set at the present time the Network Security tab shown in Figure 6.8 indicates this situation. In addition, because no server

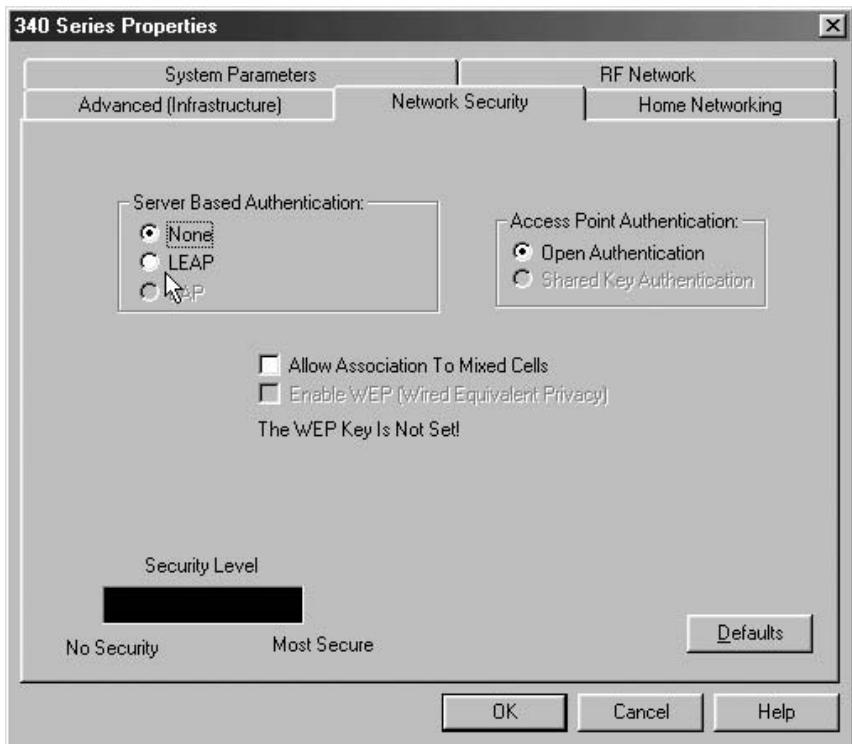


Figure 6.8 The initial display of the Cisco 340 Aironet Client Utility program's Network Security tab.

based authentication has yet to be selected the Security Level horizontal bar is shown darkened as a warning.

6.9.6 Enabling WEP

As previously noted, when using Cisco equipment the method used to enable WEP depends upon the model or series of equipment used. If you are using Cisco 340 or 350 series equipment and selected LEAP, you can check the box on the Network Security tab in the Aironet Client Utility program located to the right of the entry 'Enable WEP', as shown in Figure 6.9. However, setting that box and clicking on the button to the left of the LEAP entry will not by itself secure your transmission. To set the WEP key when using 340 or 350 series hardware requires you to use a separate program referred to as the Client Encryption Manager.

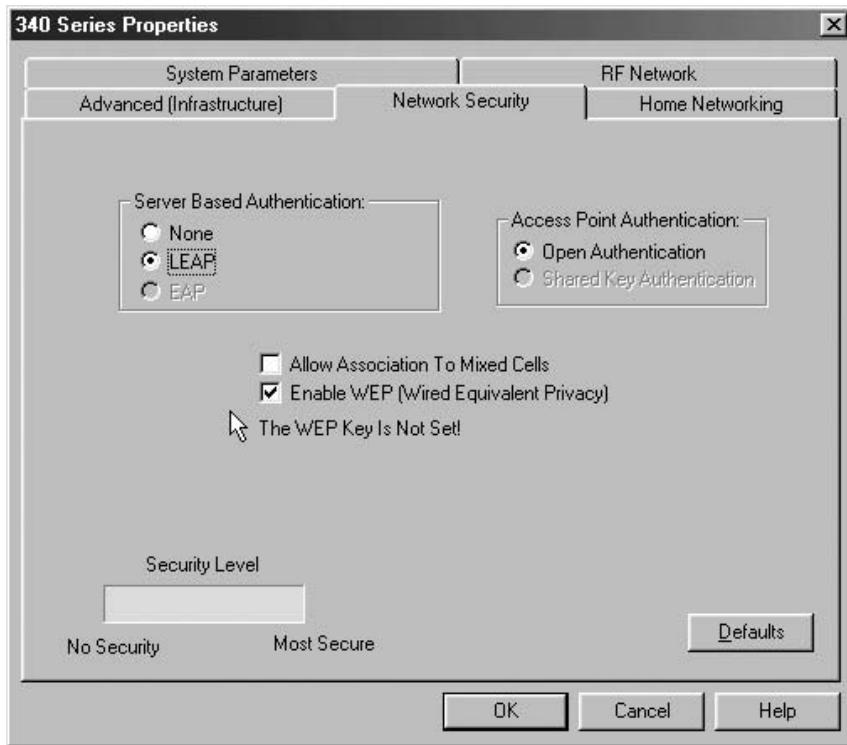


Figure 6.9 When using Cisco 340 series hardware, selecting the Enable WEP box does not set the key. To do so you need to use the Client Encryption Manager program.

Figure 6.10 illustrates the initial screen display of the Cisco Client Encryption Manager program used to set WEP key(s) for 340 and 350 series equipment. Note that to use this program after it is first installed, you will need to enter the default password 'cisco' which is known to anyone that has access to the Cisco Web site or a Cisco 340 or 350 manual. Thus, one of the first actions you should take after installing this program is to change the default password. Otherwise, someone who has a little bit of knowledge about this can potentially access your computer which could result in the discovery of the WEP key or keys being used.

Continuing our examination of the use of the Cisco Encryption Manager program, Figure 6.11 shows the first screen displayed after you enter the password to access the program. Note that the Client Encryption Manager has two pull-down menus, Commands and Help, with the commands menu

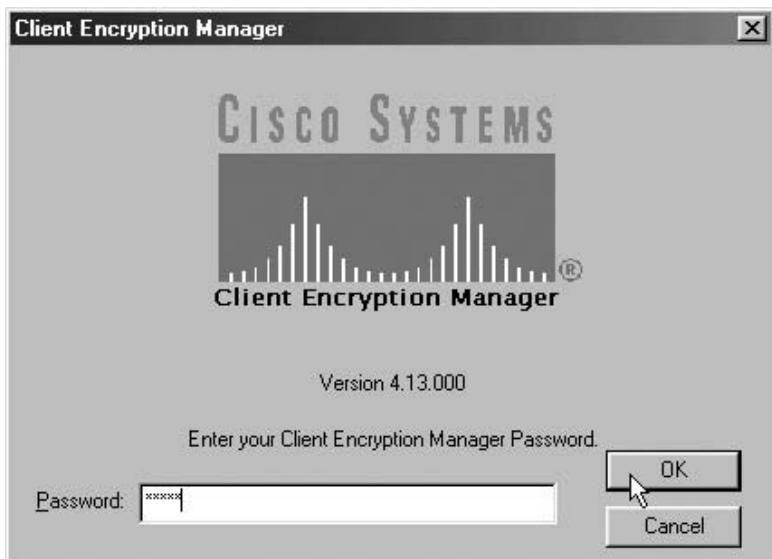


Figure 6.10 The initial use of the Cisco Client Encryption Manager requires the entry of the default password 'cisco.'

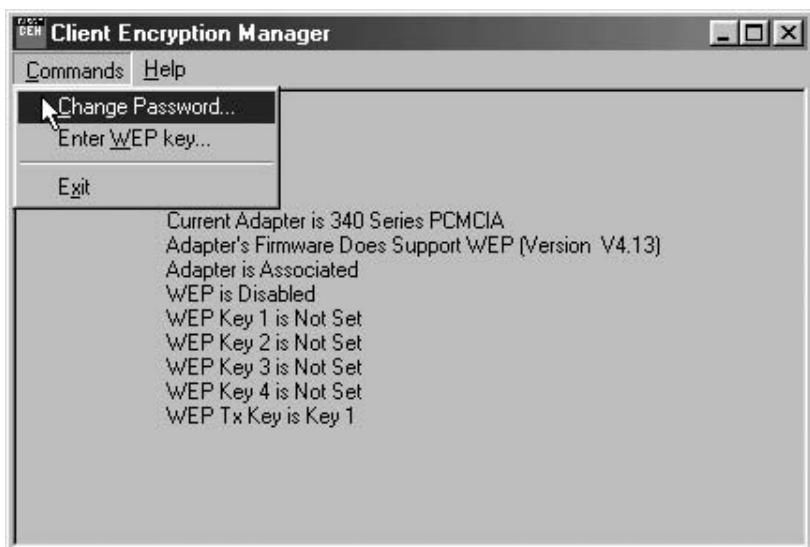


Figure 6.11 The Cisco Client Encryption Manager used with 340 series hardware provides users with the ability to set four WEP keys.

shown pulled down. The first entry in that menu enables you to change the password associated with accessing the program. In comparison, the second entry, which we will shortly explore, provides you with the ability to enter one or more WEP keys. If you look at the foreground of the display shown in Figure 6.11 you will note that information is displayed concerning the status of the wireless LAN adapter and the WEP keys. By default the first WEP key is set as the transmit key which is indicated in the last line of the display.

When the screen shown in Figure 6.11 was captured, encryption was not enabled on the client or the associated access point. This results in the display informing us that the adapter is associated but WEP is disabled. Since this is the first time the Client Encryption Manager will be used, all four WEP keys are shown as not being set.

In concluding our examination of the use of the Cisco Client Encryption Manager we will look at the manner by which WEP keys are set. Figure 6.12 illustrates the WEP key entry screen displayed by the Cisco Client Encryption Manager program. By default, WEP keys are considered to be persistent and set to a 40 bit length, requiring the entry of 10 hex digits per specified key. Also by default the first key is set to be used as the transmit key. If you are

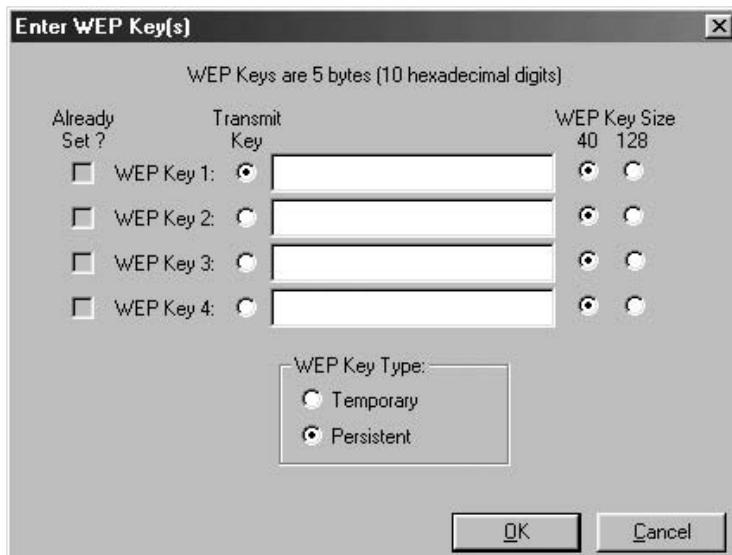


Figure 6.12 When Cisco 340 series clients are used, the Client Encryption Manager provides the mechanism to set or alter WEP keys.

using Cisco 350 series equipment you can select LEAP and set an applicable WEP in a similar manner.

6.9.7 Limitations

One limitation associated with the use of LEAP is the fact that it is limited to Cisco equipment. Thus, the use of LEAP precludes operating a mixed vendor equipment network. A second limitation of LEAP results from the fact that keys are changed on a per-session basis. This means that it is possible for an unauthorized third party to capture a sufficient amount of session traffic which means that they could recover the key for one session. Although this situation is highly unlikely it is still theoretically possible. Because LEAP employs server based authentication this means that a worst-case security hole is one where the third party might be able to record a lengthy session, recover the key and decode the captured transmissions for the session, but still could not get beyond the access point.

chapter seven

Standards Based Security

In this concluding chapter we will look at an umbrella standard referred to as port-based access control, two evolving encryption standards and the use of IPSec. The port-based access control standard, more commonly referred to as the IEEE 802.1x standard, is designed to provide an enhanced method of access control for both wired and wireless LANs. As we will shortly see, it can be considered to represent an umbrella technology because it supports several methods of authentication.

A second standard we will examine, referred to as the IEEE 802.11i standard, represents an evolving work in progress. This standard is primarily focused upon an enhanced method of encryption and covers the Temporal Key Integrity Protocol (TKIP) and the Advanced Encryption Standard (AES). In concluding this chapter we look at the IPSec standard and how it can be used to create a virtual private networking capability via an IEEE 802.11 transport facility.

7.1 The IEEE 802.1x standard

The goal of the IEEE 802.1x standard is to provide an architectural foundation for access control, authentication, and key management for wireless LANs. In addition, this standard is also applicable for wired LANs in an Ethernet switched network environment.

7.1.1 Overview

The IEEE 802.1x standard is based upon the Internet Engineering Task Force (IETF) Extensible Authentication Protocol (EAP), which was defined for wide area network operations in RFC 2284. The 802.1x standard extends EAP

from Point-to-Point Protocol (PPP) operations to a LAN environment so that it becomes extensible to many authentication methods, such as smart cards, certificate based authentication, one-time passwords and even the use of biometrics.

7.1.2 General operation

The top portion of Figure 7.1 illustrates the manner in which a client station gains access to a wireless LAN infrastructure in an 802.1x environment. As

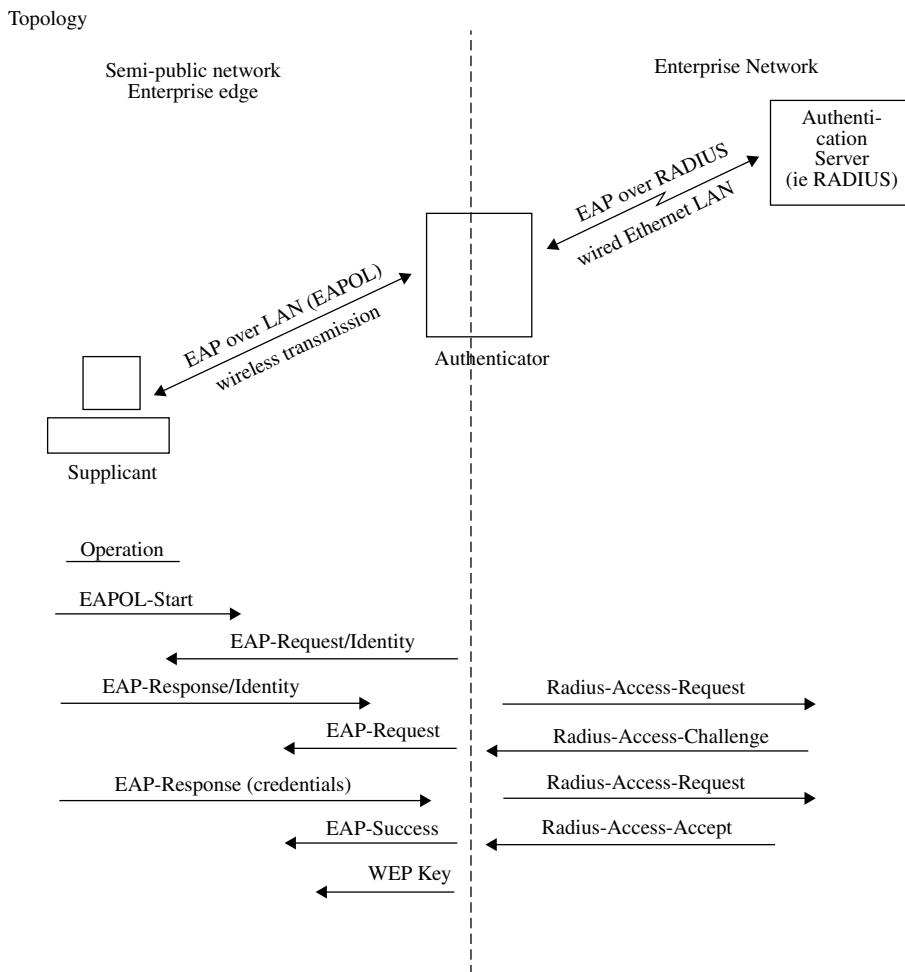


Figure 7.1 IEEE 802.1x topology and operation.

in many other IEEE standards, the 802.1x standard added several new terms to our networking vocabulary. One new term is supplicant, which is the term for a client station under the 802.1x standard. As we will note later, support for the supplicant under this standard is built into the more modern Windows XP operating system. A second term introduced under the 802.1x standard is authenticator, which refers to the facility which controls access to a LAN. In a wired LAN environment a LAN switch port represents the facility that controls access to the network. In comparison, in a wireless LAN environment the authenticator is the access point that provides access to the network.

7.1.3 Data flow

For both wired and wireless LANs the supplicant commences operation to gain network access by transmitting a request to the authenticator. The authenticator responds to the access request by requesting the identity of the supplicant. At this point the supplicant is not authenticated. The authenticator, which in a wireless LAN environment is an 802.1x compatible access point, responds by opening a logical port for passing only EAP packets from the supplicant (client) to an authentication server located on the wired side of the access point. This type of logical port is referred to as an uncontrolled port. The access point blocks all other traffic from the currently non-authenticated supplicant, such as HTTP, FTP and POP3 packets, until the access point can verify the identity of the client.

Once the identity of the supplicant is received by the authenticator, it will forward this data to the third major component of the 802.1x standard. That component is the authentication server. The actual manner in which the supplicant, authenticator and authentication server interact will depend upon the type of authentication server used. In the lower portion of Figure 7.1, the interaction between the three major IEEE 802.1x components is shown based upon the use of a RADIUS server for authentication. In this example note that after the RADIUS server accepts the credentials of the supplicant, the access point will not only allow access but could also automatically distribute a WEP key to the supplicant. In actuality, it is left to the vendor to define the type of authentication and encryption to be used and to also define if keys are automatically distributed. For example, one vendor could implement 802.1x port-based authentication through the use of a RADIUS server with the client employing a User ID/password combination, transmitted as a one-way hash for validation by the server. In comparison, another vendor could support the use of a credit card size token authentication scheme, such as SecureID. SecureID results in authorized employees being issued with a credit card sized token

generator which has a 6-digit readout. Every minute the displayed number in the readout is changed through the use of a pseudo-random algorithm embedded in the card. A person using a Secure ID is prompted by a server to enter their display number and a secret Personal Identification Number (PIN). Because the PIN is secret the loss of the SecureID card by itself does not compromise access to the network, although the person losing the card should obviously report this to the network administrator.

Software on the server uses an algorithm that updates a similar pseudo-random number generator in tandem with the SecureID card assigned to a client. When the client enters the 6-digit number displayed on the card and their PIN number, this information is forwarded by the authenticator to the authentication server. Assuming the server uses the PIN to generate a 6-digit pseudo-random number that matches the transmitted number, the server will then inform the access point of the success of the authentication process.

Returning our attention to Figure 7.1 to examine data flow, in response to the EAP Over LAN (EAPOL) Start message the authenticator (think access point) responds with a Request/Identity message. The supplicant (think client) transmits a Response/Identity packet that flows through the logical uncontrolled access point port to the authentication server, which in this example is assumed to represent a RADIUS server. In actuality, communications occur between the client and the access point, which forwards the client response to the RADIUS server for authentication as a RADIUS-Access-Request. The RADIUS server responds to the access point with a Radius-Access-Challenge. This challenge specifies the type of credentials the client must provide to confirm its identity. The access point encapsulates the Radius-Access-Challenge in an EAP-Request, which is transmitted to the client. The client transmits its credentials in the form of an EAP-Response to the authenticator (again think access point) which forwards the response to the RADIUS server via the access point's uncontrolled port. The RADIUS server hopefully validates the client's credentials, transmitting an authentication key to the access point. The authentication key is encrypted, which protects its flow on the wired network and serves as a mechanism for the access point to transmit an applicable encryption key to the client. Thus, the bottom of Figure 7.1 shows the authenticator transmitting an EAP-Success message followed by a WEP key.

If the RADIUS server was not able to validate the client the server would return a RADIUS-ACCESS-REJECT message, which the access point would transmit as an EAP-FAILURE message to the client. If this situation should occur, no WEP key would then be sent to the client. Once a client is authenticated it can be periodically requested to reauthenticate itself. By configuring a suitable reauthenticate period you can alleviate one of the vulnerabilities

in the 802.1x standard we will describe later which theoretically permits a previously authenticated session to be hijacked.

7.1.4 The EAP protocol

As previously indicated, EAP represents a framework which provides vendors with the ability to support a variety of authentication methods. To obtain an appreciation for its flexibility in supporting different methods of authentication and some of the weaknesses associated with the 802.1x standard, we will now look at the EAP protocol stack and the transport mechanism used in the form of the EAP packet.

Figure 7.2 illustrates the structure of the EAP protocol stack. In examining Figure 7.2 note that the EAPOL protocol transports EAP packets between the authenticator and the supplicant. EAPOL is responsible for providing EAP encapsulation in addition to sending session ‘start’ and session ‘logoff’ notifications. EAP, in comparison, works directly with PPP, since the latter represents a wide area network protocol. At the authentication layer almost any type of challenge-response authentication scheme can be integrated with EAP. For example, at the authentication layer shown in Figure 7.2 SSL represents the original Secure Sockets Layer used to secure HTTP between clients and Web servers. TLS represents the Transport Layer Security protocol, which was developed as a successor to SSL. CHAP represents the Challenge-Handshake Authentication Protocol to include several Microsoft versions as discussed in Chapter 6.

Because EAP represents a network layer protocol it has the capability to directly route messages to a centralized server. Although this feature may appear to be insignificant, in actuality it has a significant effect upon the operation of the protocol. This is due to the fact that if EAP operated at the

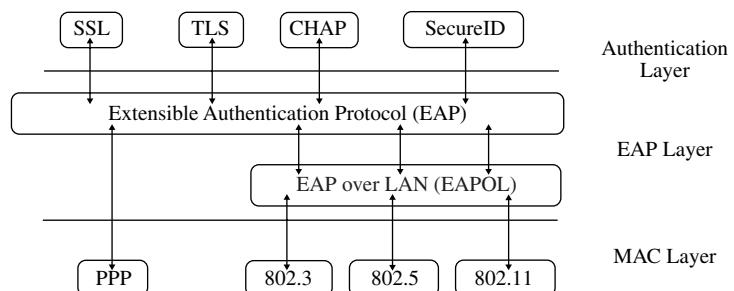


Figure 7.2 The EAP protocol stack.

MAC layer each network port to include multiple access points would then be responsible for authentication decisions.

7.1.5 Message types

There are four types of EAP messages – three of which were illustrated in the lower left portion of Figure 7.1. These four types are as follows:

- The EAP-Request message is transmitted to the supplicant indicating a challenge.
- The EAP-Response message flows from the supplicant as a reply to the EAP-Request message.
- The EAP-Success message flows from the authentication server.
- The EAP-Failure message also flows from the authentication server to the supplicant.

If you examine Figure 7.1 you will note that the first three EAP messages are shown. The fourth message, EAP-Failure, has the same direction as the EAP-Success message and is transmitted when authentication fails.

7.1.6 EAP packet format

Figure 7.3 illustrates the general format of an EAP packet. In examining Figure 7.3 note that the EAP header consists of three fields. The Code field

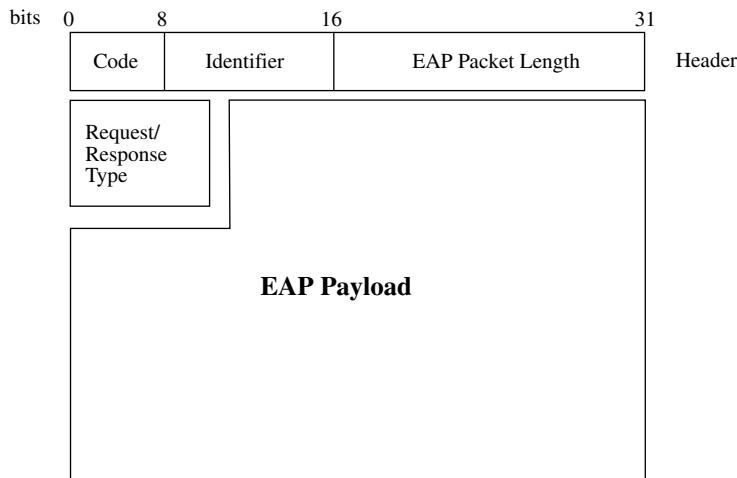


Figure 7.3 The EAP packet format.

is one byte in length as is the Identifier field. Those two fields are followed by the Packet Length field. This 16 bit field indicates the length of the packet to include the 4 byte header. The Request/Response Type field indicates the type of packet. That field is followed by the EAP payload, which represents an authentication method encapsulated within EAP Request/Response messages.

7.1.7 The dual-port authentication model

We previously noted that an unauthenticated supplicant requires a method to have their authentication request flow through an access point. In this section we will probe deeper into the manner by which this action is accomplished, noting the difference between logical controlled and uncontrolled access points.

During the authentication process, an access point needs to permit the initial flow of EAP traffic prior to the authentication server replying with a success or failure message to the request for network access. To enable the flow of EAP traffic before the authentication request is granted results in the authenticator employing a dual-port model. This model results in access points and switches compatible with the 802.1x standard providing two logical ports of access to the network, referred to as a Controlled Port and an Uncontrolled Port. The Uncontrolled Port by default filters all network traffic and only allows EAP packets to flow through the port. However, to provide backward compatibility with non-compliant 802.1x clients, such as when an organization is migrating to an authentication based access method, it is possible to configure an Uncontrolled Port to allow all network traffic through the port. In comparison, the Controlled Port only allows previously authenticated users to have their traffic flow onto the network. In a LAN environment which includes wireless LAN operations the EAPOL protocol transports packets between the supplicant and the authenticator through both Uncontrolled and Controlled Ports, with the Controlled Port used for all data flows beyond the initial session start.

7.1.8 Security limitations

Prior to examining the setup and operation of equipment in an IEEE 802.1x environment, a discussion of the security limitations of this standard is in order. Under a grant from the National Institute of Standards, Arunesh Mishra and William A. Arbaugh of the Department of Computer Science, University of Maryland published a paper in February 2002. Titled ‘An Initial Analysis of the IEEE 802.1x standard,’ this paper noted how the standard was subject to a ‘man-in-the-middle’ attack in addition to a session hijack, both resulting

from the use of one-way authentication under the standard. In this section we will describe and discuss the susceptibility of the 802.1x standard to being compromised. In addition, we describe how proprietary vendor solutions in the form of using an authentication server to distribute WEP keys and periodical reauthentication of the client can alleviate the problems described in the referenced paper.

While both EAP and EAPOL protocols can transport different types of authentication messages, by themselves they do not contain any capability for providing data integrity or privacy. Instead, data integrity in a wireless LAN environment occurs in the form of the use of the ICV within the wireless LAN frame. As we noted earlier, a CRC is used to provide the integrity check in the form of the ICV and its use is susceptible to a ‘man-in-the-middle’ attack. In addition, if you carefully followed the description of the authentication process shown in Figure 7.1, you probably noted that authentication is one-way, with the supplicant authenticated to the access point but the access point remaining unauthenticated to the supplicant. This reliance on one-way authentication represents a second vulnerability associated with the 802.1x standard that also permits a ‘man-in-the-middle’ attack.

7.1.8.1 Man-in-the-Middle Attack

Figure 7.4 illustrates the general structure of a ‘man-in-the-middle’ attack against the use of the IEEE 802.1x standard. Here the attacker can exploit the standard in two ways. First, because 802.11 frames use the ICV for data integrity, it is possible for a third party to flip bits flowing in frames between the supplicant and access point or in the reverse direction without either party being the wiser. While the attacker may not be able to know the result of their

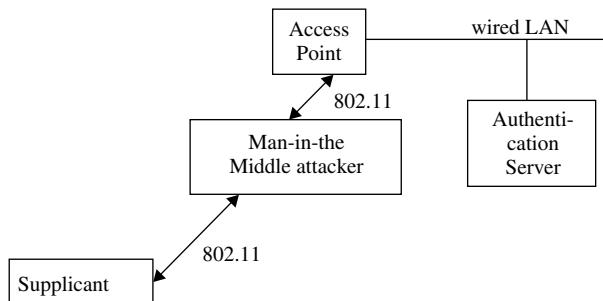


Figure 7.4 The reliance on the ICV and absence of mutual authentication results in the possibility of a man-in-the-middle attack.

attack as bits are flipped in a manner to provide a valid ICV value, the fact that data manipulation can occur and remain undetected is still a concern.

Several vendors have introduced proprietary methods to prevent bit-flipping attacks on encrypted packets. In a Cisco wireless LAN environment a recent addition to the vendor's 350 Series access point includes a facility to enable a feature referred to as Message Integrity Check (MIC). When MIC is implemented on both the access point and associated clients, it creates an enhanced method of frame verification which protects data from a possible undetected bit-flipping attack. The downside to MIC is the fact that its use adds a few bytes to each frame for the enhanced verification capability, in effect degrading throughput to obtain a tamper-proof capability.

A second flaw associated with the 802.1x standard is its lack of mutual authentication as a mandatory feature. While the use of a RADIUS server provides mutual authentication, the authentication process actually occurs using messages flowing between the access point and authentication server and not the supplicant and server. To overcome this problem it has been suggested that organizations should use EAP to transport Transport Layer Security (TLS), the successor to the secure Sockets Layer (SSL) used by Web browsers for secure communications. While EAP-TLS provides mutual authentication, it primarily protects communications to Web servers, which means communications to FTP servers, mail servers and other devices would not be protected against the 'man-in-the-middle' attack nor gain the advantage associated with the higher level of encryption used by TLS. An exception to the preceding results from the use of certain vendor products that support the transmission of SSL to a hardware box on the wired network. Using such hardware enables access to applications beyond Web browsing in a secure environment.

7.1.8.2 Session Hijack

Even when EAP-TLS is used to obtain mutual authentication it is possible for an unauthorized third party to hijack an 802.11 session. To accomplish this action an unauthorized and non-authenticated third party would first passively monitor 802.11 communications to learn the MAC addresses of the access point and supplicant to be attacked. Once this action was accomplished, the third party would monitor the wireless LAN traffic until it observed an EAP series of messages between a legitimate supplicant and an access point which results in the successful authentication of the supplicant. When this occurs the third party would transmit a MAC disassociate management frame, spoofing the MAC address of the access point. Upon receiving the disassociate

management frame the supplicant will do what it is designed to do and disassociate itself from the network. Unfortunately, the access point will be none the wiser and will remain in its authenticated state with respect to the disassociated supplicant. If the unauthorized third party now spoofs the MAC address of the previously authenticated supplicant it will gain access to the network. Figure 7.5 illustrates the manner by which an authenticated session could be hijacked through the transmission of an 802.11 MAC disassociate frame and the spoofing of the MAC access point and supplicant addresses.

While the prior discussion of a session hijack is serious, its affect will depend upon how vendors use the 802.1x authentication server. That is, the basic 802.1x standard provides an authentication mechanism without regard for whether or not WEP is enabled. If a vendor uses the authentication server to distribute dynamic WEP keys, then it is possible to counteract the session hijack. That is, assume upon successful authentication the server distributes a new key to the access point, which is forwarded to the supplicant. If WEP encryption was in effect, the unauthorized third party which issues a disassociate management frame and spoofs the MAC address of the legitimate supplicant would not have the new key. Thus, although the access point

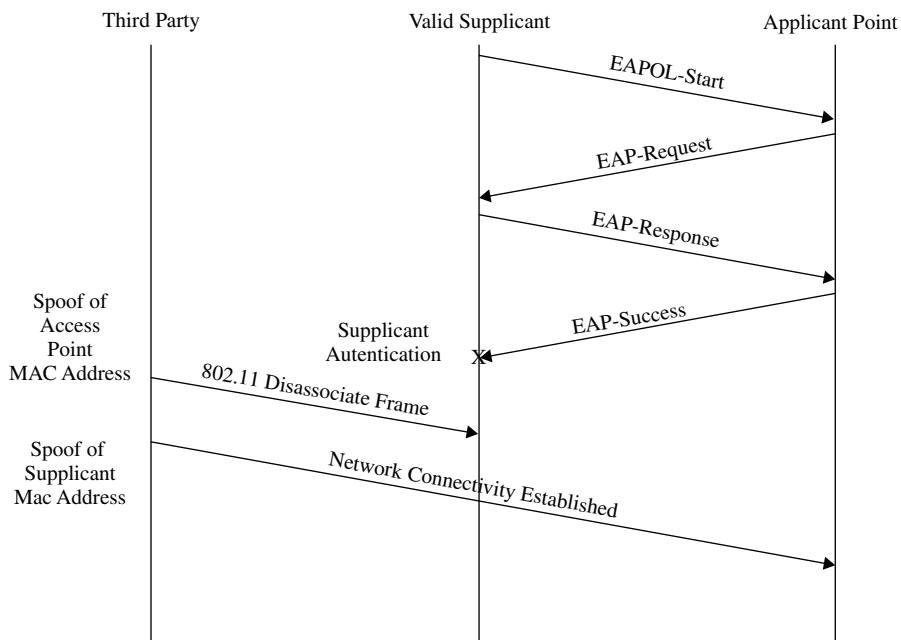


Figure 7.5 Hijacking an 802.1x authenticated session point.

would still believe the phony supplicant was authenticated, its transmissions would be rejected as it would not have the correct WEP key, resulting in the contents of the frame being non-readable.

A second area that could counteract the potential of a client hijack is obtained through the periodic reauthentication of the supplicant. Taken together, key distribution and periodic reauthentication would minimize the possibility of a session hijack. It is interesting to note that neither of these two areas were addressed in the previously referenced paper. Instead, the authors of that paper suggest per packet authenticity, a change to the EAPOL packet and the inclusion of a peer-to-peer based authentication model within the 802.1x standard. While they are quite correct that their suggestions would alleviate the previously described attacks, one must consider the overhead associated with any per packet authentication scheme. Because this could slow wireless transmission throughput to a crawl, it is probably unwise to consider this level of authentication. Now that we have an appreciation for the IEEE 802.1x standard and its security limitations we will conclude this section by examining the use of Cisco equipment in an 802.1x environment and Microsoft's support of the standard.

7.1.9 Using the Cisco Aironet 350

In concluding our examination of the IEEE 802.1x standard we will consider the use of the Cisco Systems Aironet 350 client and access point. We will first examine the setup of the Cisco client and then look at the vendor's access point.

7.1.10 Client setup

Figure 7.6 illustrates the initial installation of the Cisco Aironet Client Utility (ACU) program for use with a Series 350 wireless LAN card installed on the author's laptop. By default, server based authentication is disabled; however, you can simply select LEAP or EAP via the radio button to the left of each entry. As a side note, you can easily change the server authentication method after installing the ACU program.

The Cisco Aironet Utilities on the distribution CP that accompanied the 350 series wireless LAN adapter, used by this author, contained three separate programs. Those programs included an ACU program, a link state meter and a separate client encryption manager program. Figure 7.7 illustrates the selection of the three previously mentioned components. If you focus upon Figure 7.6 you will note that this author was using Version 4.13.000 of the Cisco Aironet Client Utilities software. Apparently, some versions of software

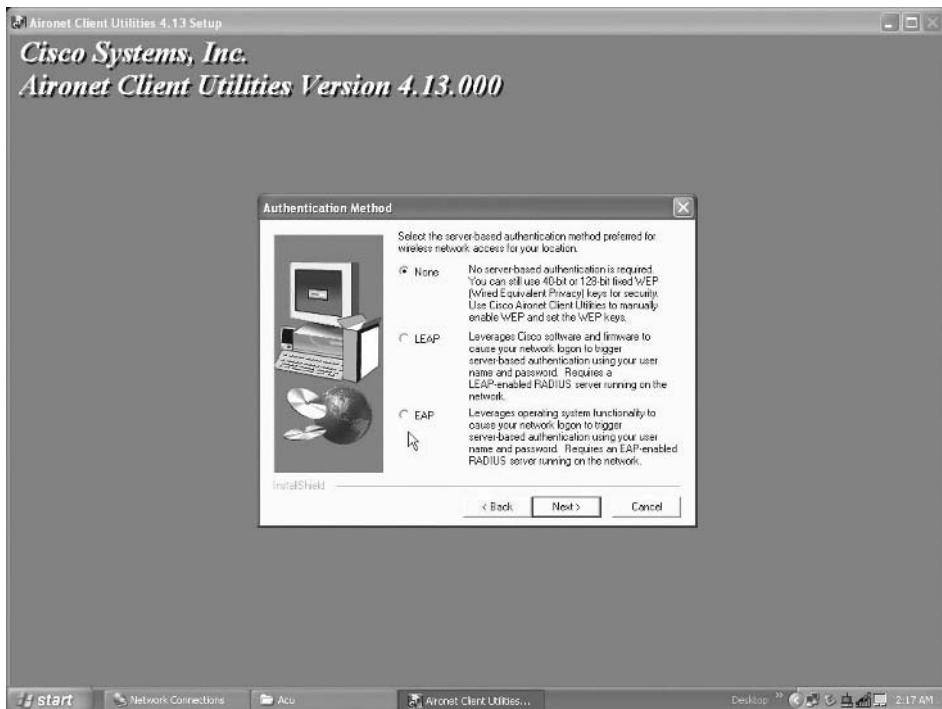


Figure 7.6 During the installation of the Aironet Client Utility program you are asked to select the type of server based authentication. Once the program is installed you can easily change this selection.

for use with Series 350 equipment integrate encryption settings with the ACP program while other versions do not. Once you complete the installation of the Cisco ACU on your computer you can directly launch the program.

If you are installing the ACU on a Windows XP system you need to carefully check the version of the software installed. For versions of the Cisco ACU prior to 4.14.002 there is a compatibility issue between the software and Windows XP. To alleviate this incompatibility or to obtain the benefit of a more modern release, it is recommended that you install the latest version of client utilities for Windows from Cisco.com. Cisco's URL for Windows updates is at <http://www.cisco.com/public/sw-center/sw-wireless.shtml>.

Once you install the Cisco Client Utility program for the 350 Series wireless adapter the initial screen will appear, this is similar to the screen shown for use with the 340 Series adapter in the previous chapter. That is, both screens will have three pull down menus – Commands, Options and Help.

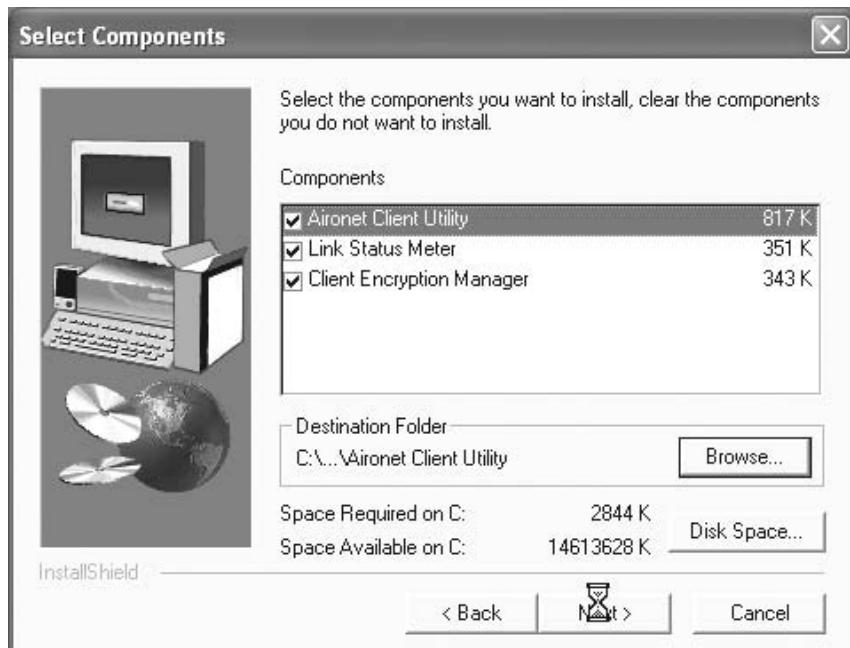


Figure 7.7 The Cisco Aironet 350 Series adapter used by the author included three software components – an Aironet Client Utility, Link Status Monitor, and Client Encryption Monitor.

The key difference between the two utility programs is that the more recent version of the ACU bundled with the 350 Series adapter has more command options which result in the ability to use separate programs from the ACU main program. This is illustrated in Figure 7.8, which shows the pull-down Command menu.

In examining the pulled down Command menu shown in Figure 7.8, note that through the use of this menu you can perform seven distinct functions in addition to exiting the program. The Edit Properties option, which is shown highlighted and which we will shortly examine, provides a similar capability to the 340 Series properties dialog box that we discussed in Chapter 6. The other options, as their names imply, provide you with the ability to view statistical information about the ongoing transmission, obtain link status information, perform a link test to determine the signal strength of a connection, perform a site survey and disable the adapter's RF communications. Now that we have an appreciation of the additions to the Command menu, in comparison to the menu used by the older Aironet 340 client, shown in the

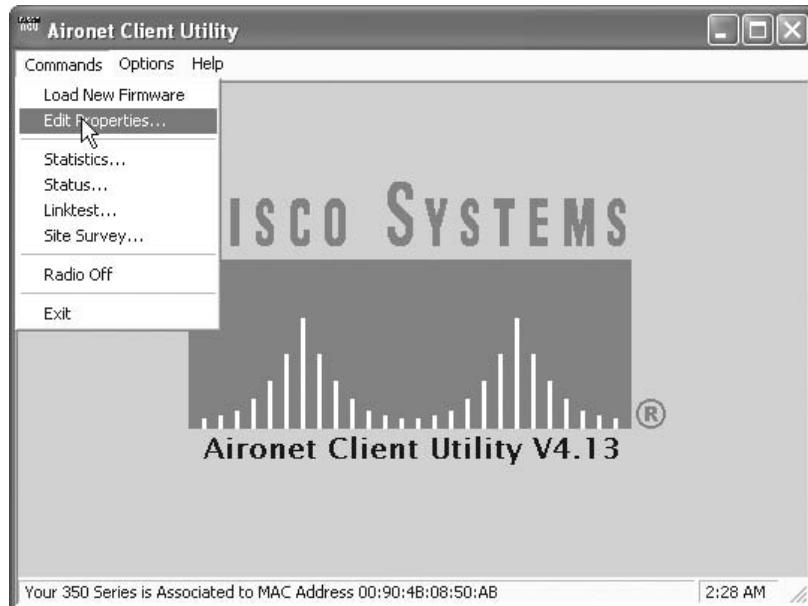


Figure 7.8 The Cisco Aironet Client Utility bundled with the 350 Series client PC Card includes a more extensive commands pull-down menu than software bundled with the 340 Series client.

previous chapter, let's look at the properties dialog box associated with a 350 series client.

Figure 7.9 illustrates the default settings of the System Parameters tab on the Cisco 350 Series Properties dialog box. If you compare the settings shown in Figure 7.9 for the 350 Series client to the settings for the 340 client previously shown in Chapter 6, you will note they are equivalent, while the display has changed slightly. The reason for the display change results from the fact that the screen captures for the Cisco 340 Series (shown in Chapter 6) occurred on a Windows 98 platform, while the screen captures for the Cisco 350 Series client (shown in this chapter) occurred on a Windows XP platform.

In examining the default settings shown in Figure 7.9 for the System Parameters tab, note a blank client name and the assignment of 'default' for SSID1. Normally, when you install a driver for Windows you would set the client name and SSID; however, you can use the ACU at anytime for those settings. In addition, as we will note later in this chapter, Windows XP provides you with a mechanism to access, view, configure and modify the SSID and WEP keys.

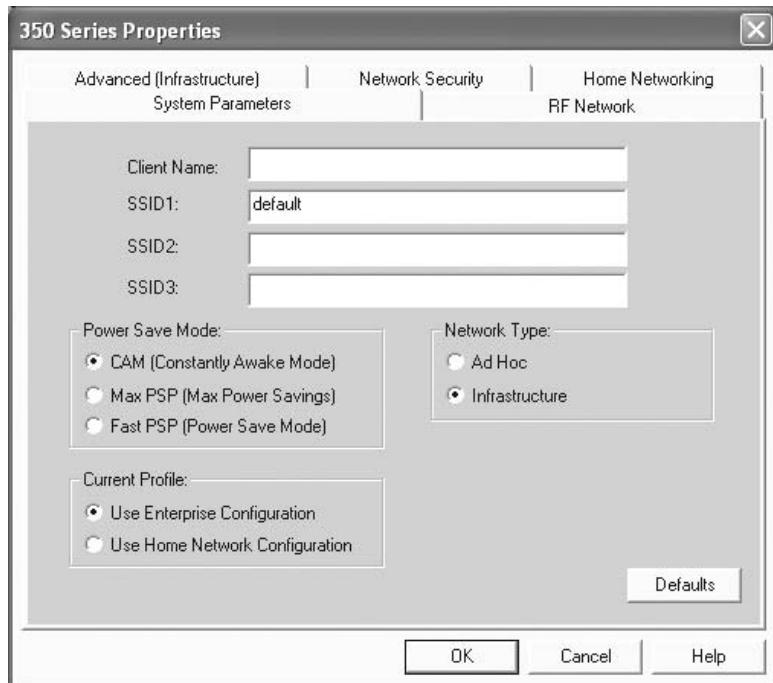


Figure 7.9 The System Parameters tab controls access to a predefined network and roaming operations.

The client name can be up to 16 characters in length and enables the access point administrator to determine which devices are connected to the AP without having to read and understand MAC addresses and their assignments. The four SSID boxes provide you with the ability to associate with one access point and define up to three additional network names for roaming. Each SSID can be up to 32 characters in length and a blank entry permits the client adapter to associate with any access point configured to allow broadcast SSIDs. If the access point you wish to communicate with was configured to disable broadcasts of the SSIDs, the SSID name entered in the applicable fields in Figure 7.9 must then match the SSID of the access point. Cisco is one of several wireless equipment vendors who provide an access point management system that allows broadcast SSIDs to be disabled. While this action makes it harder for an unauthorized third party to access the facilities of an access point, it does not provide security since the client transmission could be monitored. The other default settings shown in Figure 7.9 concern

power saving, network type and profile settings that are suitable for accessing an access point from a computer using AC power.

7.1.11 Network security

Continuing our examination of the Cisco 350 Series ACU program, Figure 7.10 illustrates the display of the Network Security tab in the foreground of the screen. Similar to the 340 Series Network Security tab shown in Chapter 6, the 350 Series allows you to define the type of server based authentication to be used. It also allows you to select the manner by which the client adapter will attempt to authenticate with the access point. If LEAP or EAP is enabled on the client adapter, open authentication will be the only available option. The shared key authentication option will become available for selection when the client adapter is assigned a WEP key via the use of the Client Encryption Manager (CEM) program and the key is enabled.

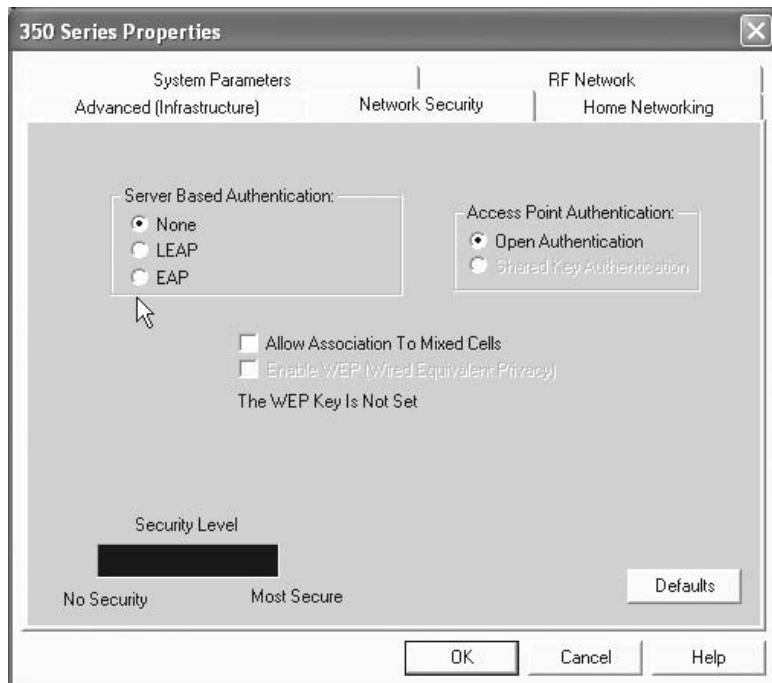


Figure 7.10 The Network Security tab on the 350 Series dialog box permits the selection of a server based authentication method.

In the lower middle portion of Figure 7.10 you will note the check box to the right of the label 'Allow Association to Mixed Cells.' If you set the use of data encryption on your access point to 'optional' you must select this checkbox, even if the client adapter is not using WEP. Otherwise, the client will not be able to establish a connection with the Cisco access point. By setting this box your client becomes capable of communicating with access points configured to communicate with WEP enabled and WEP disabled clients.

At the lower left portion of Figure 7.10, the Security Level horizontal bar indicates the level of security based on the parameters selected. The bar graph is colored solid green to denote a most secure network configuration when either LEAP or EAP is enabled and a session-based WEP key is assigned to the adapter by a RADIUS server. The bar will appear red when the network has some security features enabled and will be colored black when no security features are enabled.

Like the description of LEAP in Chapter 6, the use of EAP requires you to set WEP through the CEM. Once you log into the CEM program and select the 'Enter WEP key' option from the command menu, the screen shown in Figure 7.11 will be displayed. Note that like the setting of WEP for LEAP, you

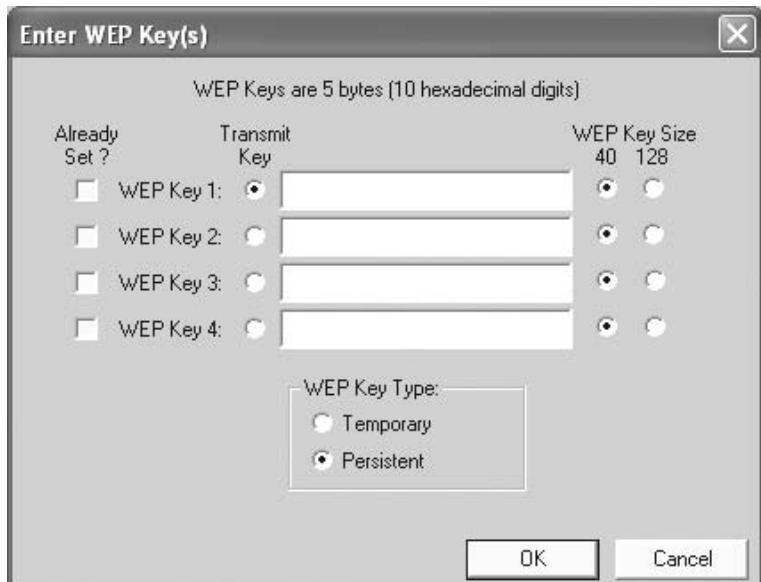


Figure 7.11 The Client Encryption Manager provides the mechanism to enter 40 or 128 bit WEP keys.

can specify up to four WEP keys, with each key being either 40 or 128 bits in length. You would enter 10 characters for 40 bit WEP keys and 26 characters to specify a 128 bit WEP key according to the Cisco display. However, the latter is a bit (no pun intended) misleading as you are actually specifying a 104 bit key, which, when added to a 24 bit IV, results in a 128 bit key.

In the lower portion of Figure 7.11 are radio buttons associated with the labels ‘Temporary’ and ‘Persistent.’ If you select ‘Temporary’, the WEP key will be lost when power is removed from the client adapter. In comparison, selecting the default of ‘Persistent’ results in the WEP key being retained when the power to the client is removed.

7.1.12 Using Windows XP

In addition to Cisco’s ACU and the CEM, under Windows XP you have a security configuration capability due to the built-in support of wireless networking and IEEE 802.1x authentication in this operating system. Figure 7.12 illustrates a sequence of screens that show the support of Windows XP for IEEE 802.1x authentication. In the background of Figure 7.12 the Network Connections window is shown. Clicking on the wireless network connection for the previously installed Cisco System 350 adapter results in the display of the dialog box labeled ‘Wireless Network Connection 4 Status’ which is shown in the left foreground portion of Figure 7.12. Note that under Windows XP the tab labeled ‘General’ for that dialog box indicates the duration of the existing connection, data rate, signal strength and activity, the latter in the form of a count of the number of packets transmitted and received. Clicking on the button labeled ‘Properties’ results in the display of the dialog box with that label, which is shown in the right portion of the display. Here the Properties dialog box for the wireless network connection has four tabs, with the Authentication tab displayed. You can use this tab to enable network access control using the IEEE 802.1x standard and also to select one of two types of EAP authentication directly supported by the Windows XP operating system – ‘MD5-challenge’ or ‘Smart Card or other certificate.’ When you select MD5-Challenge, which is the default, your User ID and password entered for network operations is employed by the MD5 algorithm to create a one-way hash value that is forwarded through the access point to a RADIUS server.

One of the more interesting aspects of using a wireless LAN network adapter under Windows XP is the fact that by default network access control using IEEE 802.1x is enabled. Thus, when you use a wireless connection to initially configure most access points, you will more than likely have to first disable the use of the IEEE 802.1x standard. The rationale for doing this results from

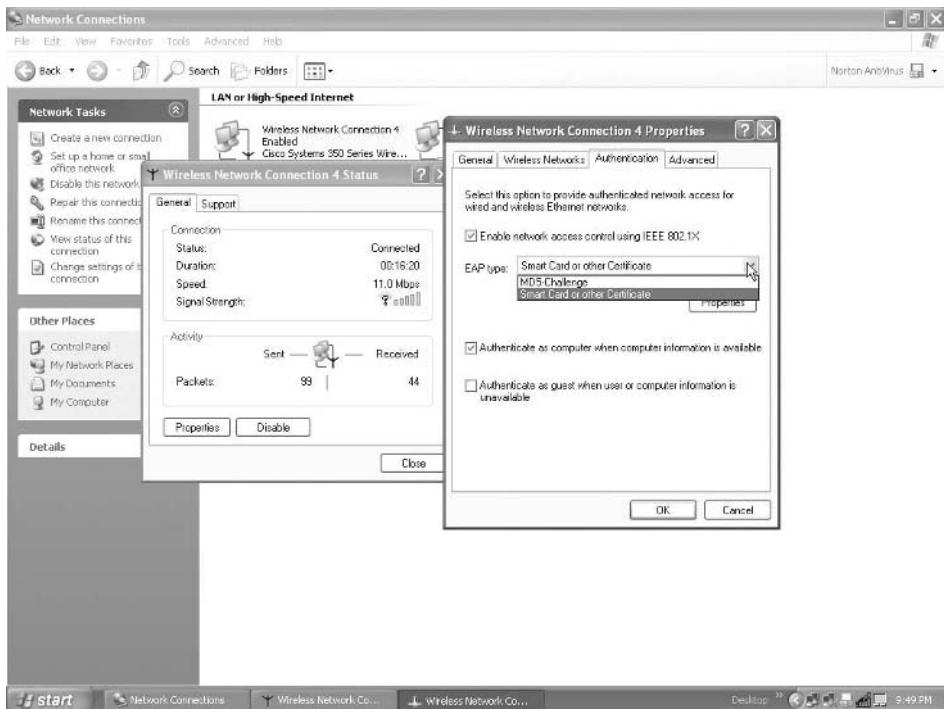


Figure 7.12 From the Windows XP wireless properties screen you can enable and select an EAP authentication method.

the fact that by default eight different access points examined by this author all shared the common characteristic of disabling security. Thus, enabling authentication on the client to configure an access point will result in the inability to access the access point. However, once you disable the use of EAP by Windows XP and configure an applicable Client IP address you will be able to access the access point. In the next section we will examine the configuration of the Cisco 350 Series Access Point to include the client IP address assignment necessary to configure the device.

7.1.12.1 Wireless Network Properties

In concluding our brief discussion of the use of Windows XP we will look at the settings on the wireless network properties dialog box. Figures 7.13 and 7.14 illustrate this dialog box under two different conditions. In examining Figure 7.13 note that you can use this box to specify the SSID, denote if the

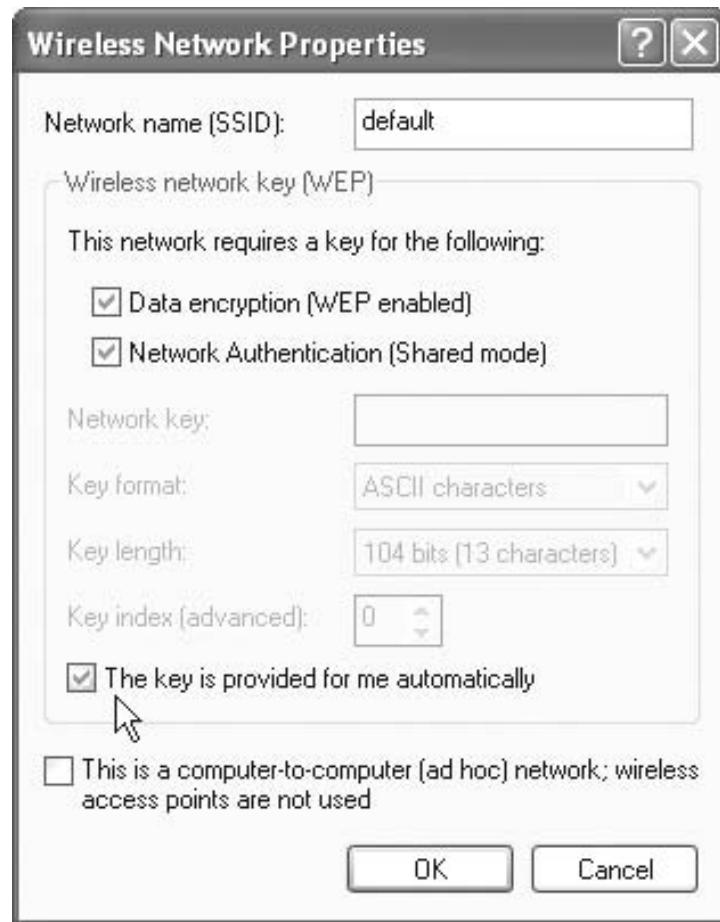


Figure 7.13 Using the Windows XP Wireless Network Properties dialog box to have a WEP key automatically provided to the client station.

network requires a WEP key for encryption and authentication and indicate if the key is automatically provided to the client. When you select the box to have the WEP key automatically assigned to the client station the ability to enter a network key, specify the key format, key length and key index will appear shaded as those items cannot be specified. However, if you do not specify that the key is to be automatically provided to the client you can then enter up to four WEP keys as well as specify the key length and key format.

Figure 7.14 illustrates the Wireless Network Properties dialog box after the provision for automatic key delivery was deselected. Note that the entries for

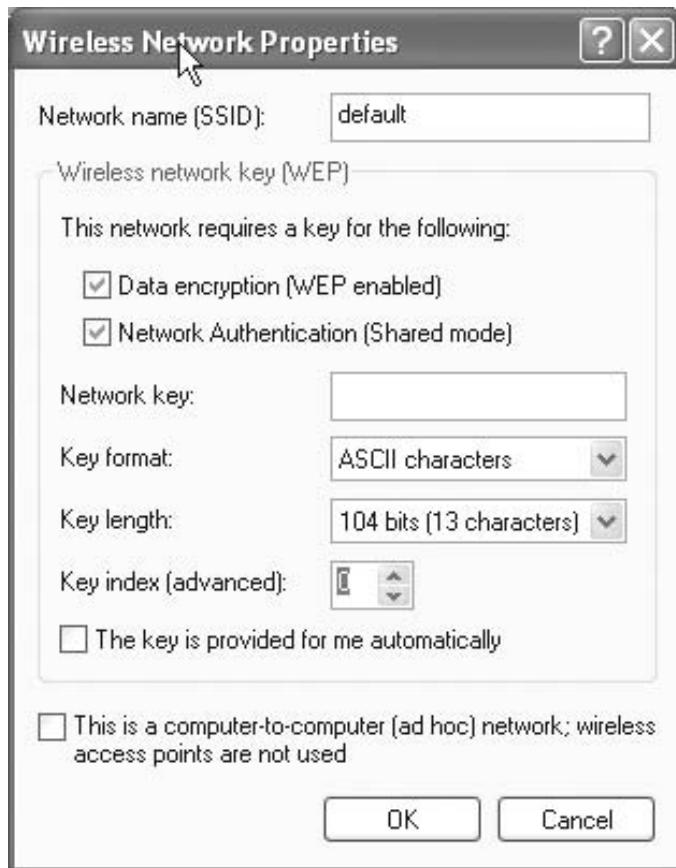


Figure 7.14 When you deselect the automatic distribution of the WEP key you can use the Windows XP Wireless Network Properties dialog box to set the values of up to four keys for the client.

the network key, key format, key length and key index can now be set. Thus, in a Windows XP environment you can use the operating system to set one or more WEP keys on the client or have the access point automatically distribute the key to the client. Now that we have an appreciation for the client setup process in a Cisco 350 series environment, let's look at the access point.

7.1.13 Access point setup

The Cisco 350 Series access point represents a sophisticated wireless device that contains numerous security related features. In this section we will

examine those features. However, prior to doing so a few words are necessary to discuss the methods you can consider using to access the access point.

7.1.13.1 Accessing the Access Point

The Cisco 350 Series access point is configured with the default IP address of 10.0.0.1. To access the access point for configuration purposes you can use a Web browser via an RF or wired LAN connection or cable a PC to the device's serial port. The latter enables you to use the HyperTerminal program bundled with Windows. Other methods available for configuring the Cisco 350 Series Access Point include the use of Telnet and SNMP.

When accessing the Cisco 350 Series Access Point via a direct wired Ethernet, through a switch or an RF connection, you need to configure your client to be on the same IP network. Otherwise, in an RF environment your client software will indicate a radio link exists; however, you will not be able to connect to the access point. In a wired environment you will simply obtain a message that your browser cannot access the Web page at 10.0.0.1.

7.1.13.2 IPSU

Bundled on the Cisco Aironet CD-ROM is a utility program called IPSU that warrants a brief description. Through the use of the IPSU program you can enter the MAC address of the access point and retrieve its IP address or set the IP address and SSID on the AP. Figure 7.15 illustrates the use of IPSU to set the IP address and SSID of an access point.

7.1.13.3 AP350 Browser Access

To access the Cisco 350 Series access point this author used a notebook computer with a wireless PC Card. Because the default address of the Cisco access point is 10.0.0.1, it became necessary to set the IP address of the notebook to an address on the 10.0.0.0 network. In doing so this author set the IP address of his notebook to 10.0.0.2.

7.1.13.4 Summary Status Page

Figure 7.16 illustrates the use of a Web browser to access the Cisco AP350. Note that the address entered into the browser, which is pointed to 10.0.0.1, is the default address of the access point. Upon access to the AP350 its Summary Status page is displayed, as shown in the previously referenced figure. If you carefully examine the display shown in Figure 7.16 you will note a series of selectable buttons labeled 'Home,' 'Map,' 'Network,' 'Associations,' 'Setup,'

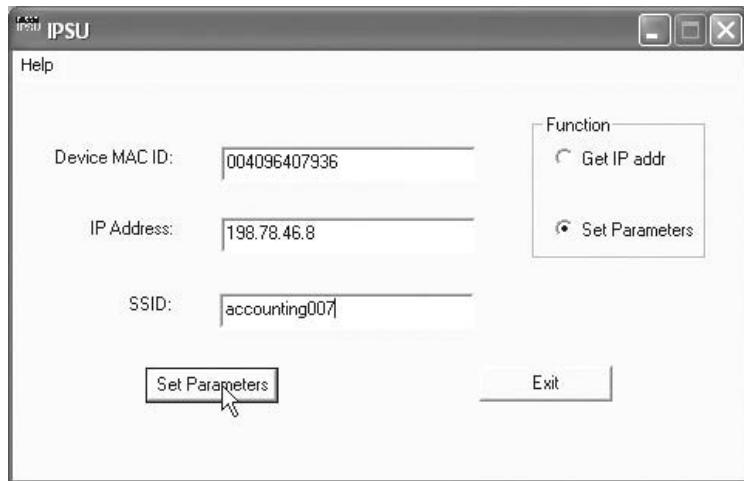


Figure 7.15 Using the IPSU utility program you can either set or retrieve the IP address of an access point.

The screenshot shows a Microsoft Internet Explorer window displaying the 'AP350-5a504f Summary Status' page. The page includes a Cisco Systems logo and navigation links for Home, Map, Network, Associations, Setup, Logs, and Help. It shows uptime of 00:10:26. The 'Current Associations' section indicates 1 client, 0 repeaters, 0 bridges, and 1 AP. The 'Recent Events' table lists several log entries, including associations and disassociations. The 'Network Ports' table shows one port with 'No Link' status. The browser's address bar shows the URL http://10.0.0.1.

Time	Severity	Description
00:08:15	Info	Station [10.0.0.2]00022d04740b Associated
00:08:15	Info	Station [10.0.0.2]00022d04740b Authenticated
00:01:11	Info	Station [10.0.0.2]00022d04740b roamed
00:01:11	Info	Disassociating [10.0.0.2]00022d04740b, reason "Sender is Leaving (has left) BSS"
00:00:20	Info	Station [10.0.0.2]00022d04740b Associated

Network Ports		Diagnostics		
Device	Status	Mb/s	IP Addr.	MAC Addr.
Ethernet	No Link	0.0	10.0.0.1	0040965a504f

Figure 7.16 Upon accessing the Cisco AP3550 its Summary Status page is displayed.

'Logs' and 'Help' that run horizontally across the top of the screen. To the right of the 'Help' button the system uptime is displayed, while under the highlighted series of buttons you can note current associations, recent events, and network ports. If you look under the Recent Events heading, you will note the station with the IP address 10.0.0.2 is shown from the last line in that section as being associated with the access point, then disassociating, roamed, authenticated and associated again. This author moved his notebook while initially connected to the AP to observe the effect upon the display of recent events. Because the access point at this moment in time was not connected to a wired Ethernet network, you will observe a link status of 'no link' for the Ethernet device under the section labeled 'Network Ports.'

Examining the highlighted buttons that run horizontally across to the top of Figure 7.16, selecting the 'Home' button displays the Summary Status page while the selection of the Map entry results in the display of a menu of links to other management pages you can select, such as Summary Status, Association Table, Events Logs, Network Ports, Network Diagnostics and Setup. Each of those entries can also be selected from individual entries in the illustration shown in Figure 7.16. Although we primarily want to look at the Setup menu and the Security menu, there are several other menus that warrant attention that we will either view or discuss.

7.1.13.5 Association Table

From the Summary Status page you can click on the 'Associations' button to obtain a list of devices associated with the access point. This table, which is shown in Figure 7.17, should be periodically checked if your organization has any doubts about the possibility that one or more unauthorized people are using the facilities of the access point. In actuality, if LEAP or EAP are used, unless the third party is somehow able to access and reconfigure the RADIUS server they will not be able to use the facilities of the access point to gain access to your organization's wired network. Thus, the periodic scanning of the Association Table is more appropriate if your organization is not using server based authentication. Because the Association Table indicates the IP and MAC addresses of devices, it can also be helpful for diagnostic testing purposes.

7.1.13.6 Event Log

The selection of the 'Logs' link from the highlighted bar of labels results in the display of the access point's Event Log page. This page lists system events

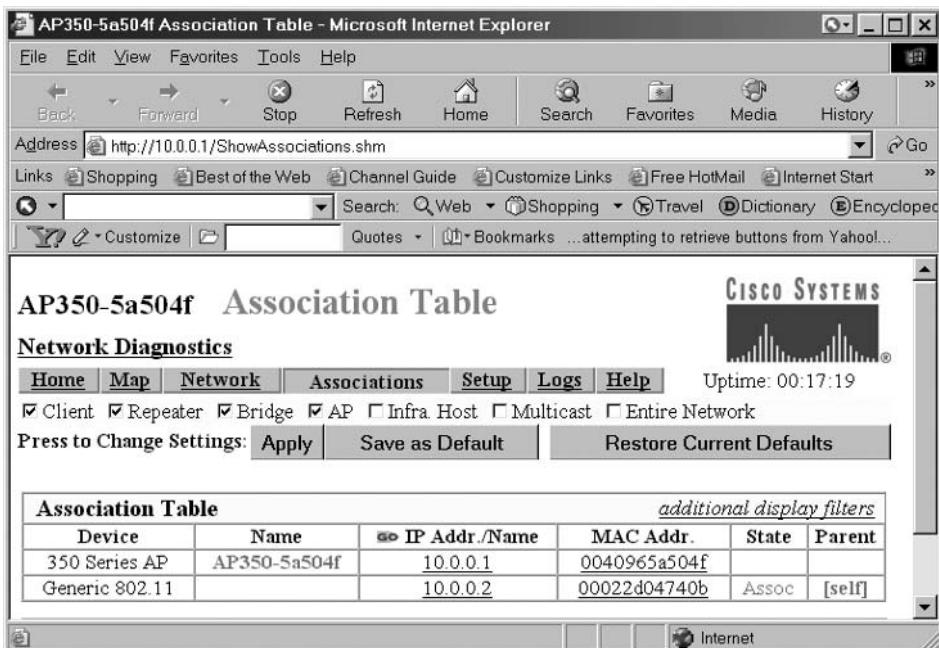


Figure 7.17 The Association Table indicates the IP and MAC address of devices on the RF network.

and their severity level in a format similar to the Recent Events area of the Summary Status page previously shown in Figure 7.16.

7.1.13.7 Help Facility

The help facility is worth mentioning as Cisco's assistance facility is different from the help facilities you are more than familiar with if you regularly use Windows. When you use the online help facility of the access point you are actually accessing a URL to the Cisco Web site. Thus, you need a connection from the access point to the Internet to take full advantage of this facility.

7.1.13.8 Express Setup

The Express Setup page represents a literal key to rapidly change or update basic settings associated with the Cisco AP350. Figure 7.18 illustrates the default display of the Express Setup page prior to making any changes to the configuration of the access point. Note that the setup page first displays

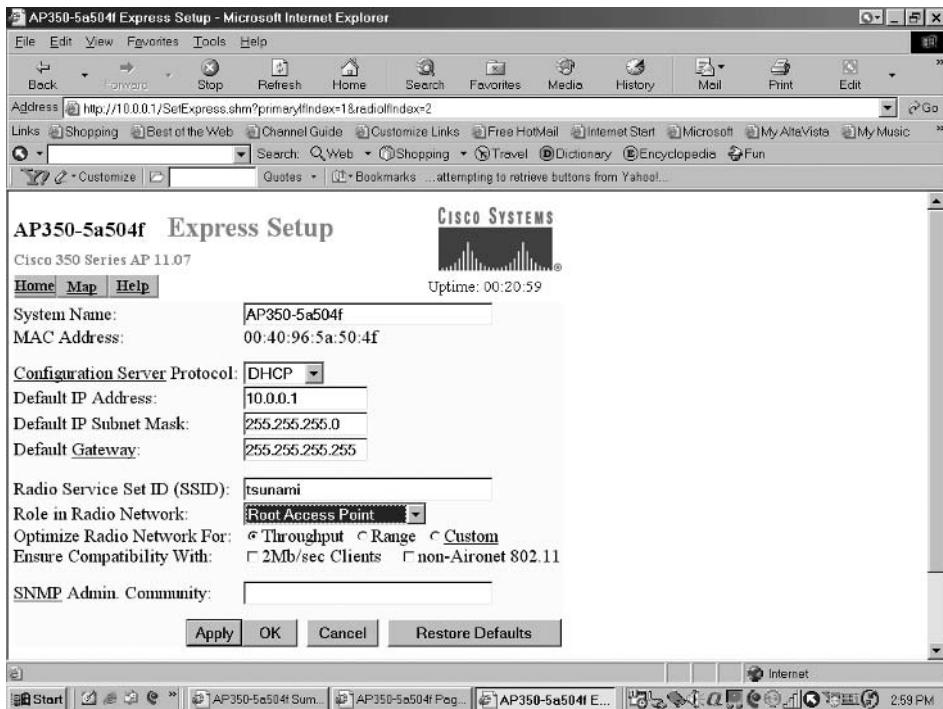


Figure 7.18 The Cisco AP350 Express Setup page can be used to examine the access point default settings and to change those settings.

the name and MAC address of the access point, followed by the configuration server protocol that is shown set to DHCP. The configuration server protocol drop-down menu also supports a setting of none and BOOTP, with the latter representing the Bootstrap Protocol, which should be selected when IP addresses are hard-coded based on MAC addresses.

As previously noted, the default IP address assigned to the AP350 is 10.0.0.1. The default gateway, which is shown as 255.255.255.255, indicates a situation where no gateway has been configured. The Radio Service Set ID (SSID) default setting is the well known word ‘tsunami’ used by Cisco and publicized in many articles, which indicates why this identifier provides an illusion of security since it can be overridden by entering a blank or the keyword ‘any’ on a client if an unauthorized third party attempted to access your organization’s network via the AP350.

The pull-down menu associated with the label ‘Role in Radio Network’ defines the manner by which the access point operates. Available options

include Root Access Point, which is the default, Repeater Access Point, and Site Survey Client. The default setting of Root Access Point is used when the AP is to be connected to a wired LAN. By comparison, you would select the Repeater Access Point entry if the access point functions as an extender between clients and the root unit, while you would select the Site Survey Client menu entry when performing a site survey for a repeater access point.

The next entry to select concerns the optimization of the radio network. Here the default is 'Throughput,' which can reduce the range of the access point's RF signal. If you select the 'Range' option you will maximize transmission distance but will more than likely reduce throughput. If you require the extra range and do not anticipate using the server based authentication capability of the access point, you may wish to use a notebook and walk the perimeter of your organization's location. Using a wireless LAN PC Card and a signal strength utility program, you can determine the potential effect associated with optimizing the access point for range on the leakage of RF energy outside the building or onto other floors. If this results in the ability of RF signals to be received outside the perimeter you should then consider hardening your network with a RADIUS server.

At the bottom of Figure 7.18 you will note that the SNMP community name by default is set to a blank. Although this may appear to be a security problem, it should also be noted that by default SNMP is disabled on the access point. Thus, you only need to consider specifying a community name if you wish to enable this feature.

Although the Express Setup page provides you with the ability to configure or modify several key system parameters via a common page, there are no security settings associated with that page. Thus, to secure your RF communications you need to utilize the Security Setup facility of the access point.

7.1.14 Security Setup

In concluding our examination of the Cisco AP350 we will focus upon its Security Setup facility. In actuality, the Cisco access point includes several features scattered across different menus that can have an effect upon your security. Thus, this author would be remiss if he did not describe and discuss those additional security related features in addition to the facilities provided under the Security Setup menu.

7.1.15 Access

You can access both the Security Setup menu as well as other security related pages from the access point Setup page. This page, which is illustrated in

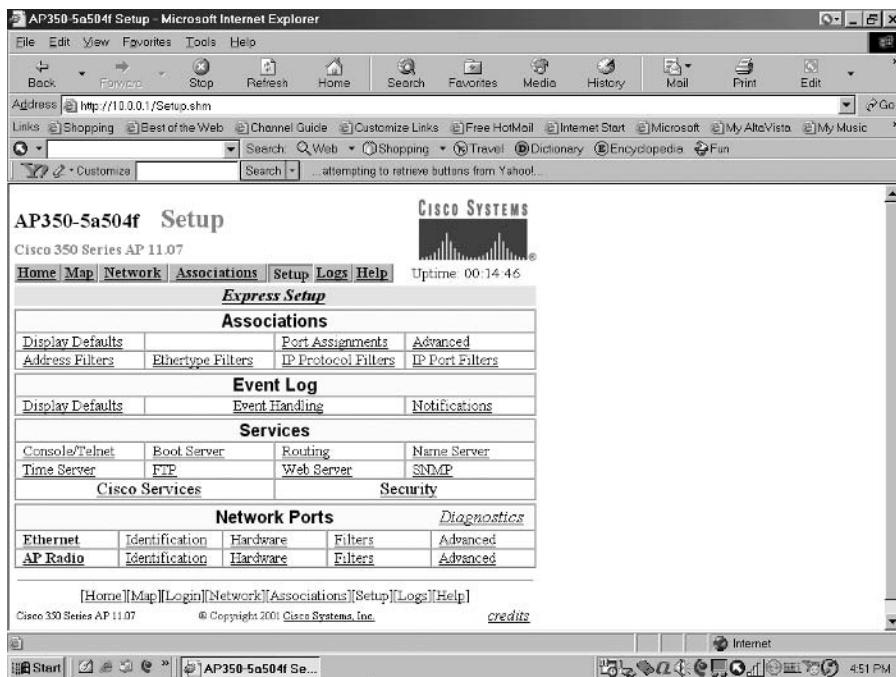


Figure 7.19 Through the Cisco access point setup page you can access both a Security Setup page as well as other pages that can be used to enhance the security of your network.

Figure 7.19, provides you with access to several pages that can be used to enhance the security of your organization's network in addition to the Security Setup page we will shortly discuss. However, prior to doing so a few words about other pages that can be used to enhance security are in order.

7.1.15.1 Filtering Options

If you examine the entries under the 'Associations' heading shown in Figure 7.19 you will note four links to filtering options. Those links include Address Filters, EtherType Filters, IP Protocol Filters and IP Port Filters.

Selecting the Address Filters entry under 'Associations' in Figure 7.19 provides you with the ability to enable MAC-based authentication on the access point. You can also use the Address Filters page to create a list of allowed MAC addresses that will be sent to a server for MAC-based authentication. Although MAC address authentication represents an enhancement to security,

as indicated several times in this book, it is a relatively easy process for an unauthorized third party to discover and spoof MAC addresses. Thus, by itself MAC address filtering is susceptible to being broken.

The other three filters (EtherType, IP Protocol and IP port) provide you with the ability to forward or block (enable or disable) the flow of specific protocols through the access point. For example, if you want to restrict wireless clients to Web access you could set an IP port filter in a field that Cisco refers to as a Special Cases entry to a value of 80. Because you can use the filtering capability of a Cisco access point to filter protocols for wireless client stations and users on the wired LAN, you obtain the capability to control what can flow in either direction through the access point. Although the filtering capability of the Cisco 350 access point is limited in comparison to the capability of that vendor's router access lists, access point filtering provides a mechanism to further secure both your wired and wireless infrastructure which warrants consideration. Now that we have a basic appreciation for the potential role of access point filtering, let's look at the Security Setup page of the AP350. That page is accessed by selecting the Security option under Services on the Setup page shown in Figure 7.19.

7.1.16 Security Setup options

The AP350 Security Setup page is illustrated in Figure 7.20. From this page you can select six security related options. Selecting the Login option provides you with the ability to enter a username and password to obtain access for changing security features associated with the access point. Of course, you must first create a list of one or more authorized management system users who, upon entry of the correct user name and password, will be granted access to the system. To accomplish this action you would select the User Manager entry in the Security Setup page. Figure 7.21 illustrates the display of the resulting User Manager Setup screen.

7.1.16.1 The User Manager

In examining Figure 7.21 you will note that by default the User Manager facility is disabled. This means that to restrict the use of the access point management system you need to enable the User Manager setting. However, prior to doing so you need to define at least one person with full access point capabilities before enabling the user manager. Fortunately, the access point's firmware will not allow you to enable the User Manager until you define a full administrator user, which is a user name and password which

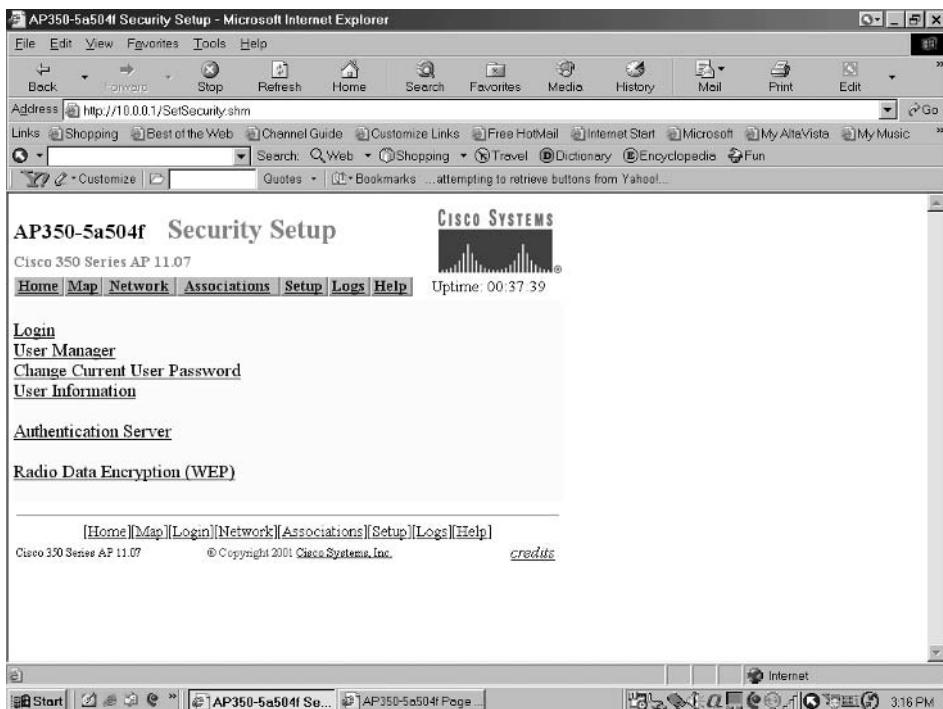


Figure 7.20 The Cisco AP350 Security Setup page provides access to six security related functions.

has full permissions and are referred to by Cisco as capabilities (which we will shortly discuss).

In addition to being able to enable the User Manager, the page with that name includes two additional radio button selectable options. The first, 'Allow Read-Only Browsing without Login' by default is set to 'Yes' and allows any user to view the access point's basic pages. Once you define a full administrator user and optionally define the capabilities of additional users you may wish to consider changing the setting of the browsing option to 'No.' The rational for changing this setting results from the fact that employees often leave their equipment on when going to lunch or taking a break away from their work area. Although visitors should be escorted, why make it easy for a knowledgeable person to use your organization's equipment to view access point settings that could assist them in harming your network? In addition, it is this author's opinion that employees other than network administrators and their staff do not need the capability to view access point pages. Returning to

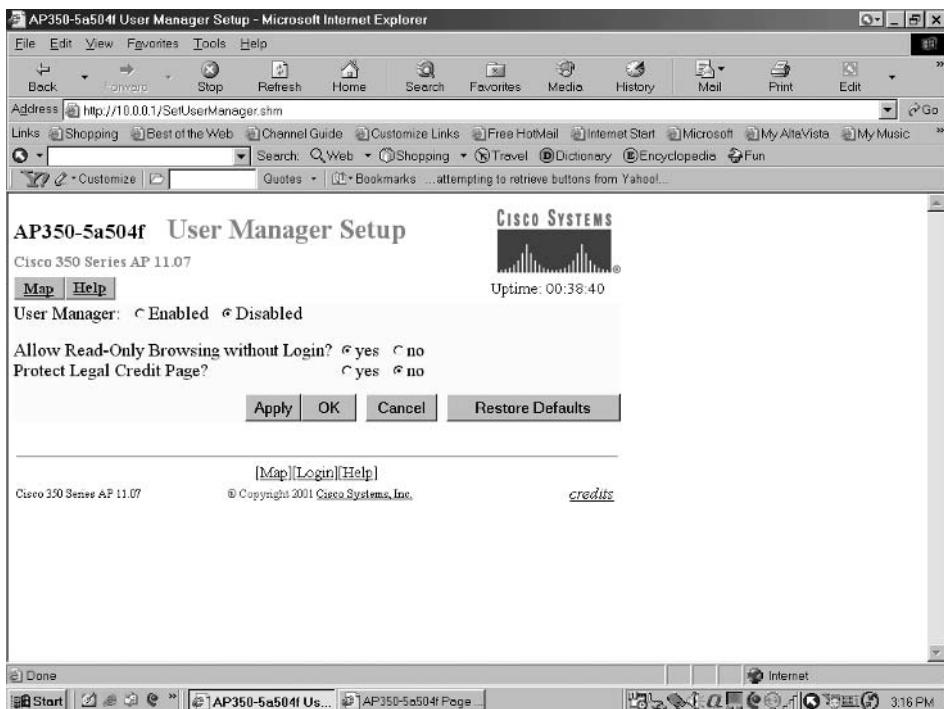


Figure 7.21 The Cisco AP350 User Manager Setup page allows you to enable this facility as well as control browsing to other access point management pages.

the User Manager Setup page illustrated in Figure 7.21, the last radio button on the page controls access to a Legal Credits page. The default setting of 'No' enables any user to view that page while 'Yes' restricts access to users in the user list.

7.1.16.2 User Capabilities

The third option in the Security Setup page shown in Figure 7.20, labeled 'Change Current User Password,' enables a previously configured user to change their password. The fourth option on the Security Setup page, which is labeled 'User Information,' provides the facility to add new users and to display a list of previously assigned users and their user capabilities. Concerning the latter, when you assign a user name and password to establish a management account you also obtain the ability to define

TABLE 7.1 Cisco access point user capability settings

Setting	Description
Write	Allows user to change settings
SNMP	Designates user name as an SNMP community name for SNMP operations
Ident	Permits user to change access point's identity settings (IP address and SSID)
Firmware	Enables user to update access point firmware
Admin	Allows user to view all system screens

the access point capabilities for the user. Those capabilities are listed in Table 7.1.

In examining the entries in Table 7.1, the selection of the firmware capability automatically provides a user with Write and Admin capabilities. However, assigning an Admin capability to a user only allows them to view all system screens. To enable an admin user to make changes to the system both Write and Admin capabilities must be selected.

7.1.16.3 Authentication Configuration

The fifth entry in the Security Setup page provides a mechanism to configure up to four servers as authentication servers. Figure 7.22 illustrates the Cisco AP350 authentication configuration page. Note that when used for EAP you need to specify the version of the 802.1x protocol being used. At the time this book was prepared Draft 10 was the latest version; however, it is possible that either a later draft or a final version will be available for selection at a later date.

The order of configuring the four rows in Figure 7.22 is important. If you set up more than one server for the same service, the server first in the list will be the primary server for the selected service. In comparison, the others are used in their list order if attempted access to the primary server and prior ordered servers time out.

Refocusing on Figure 7.22, the Server Name/IP field enables you to enter the host name or IP address of the authentication server. By default, port 1812 is set for a RADIUS server as this is the port used for Cisco's RADIUS server. Regardless of whether you use port 1812 or have to set a different value to enable access to another vendor's RADIUS server, it is important to consider where the server resides. This results from the fact that when a server is located on a distant network which requires packets to traverse firewalls or routers,

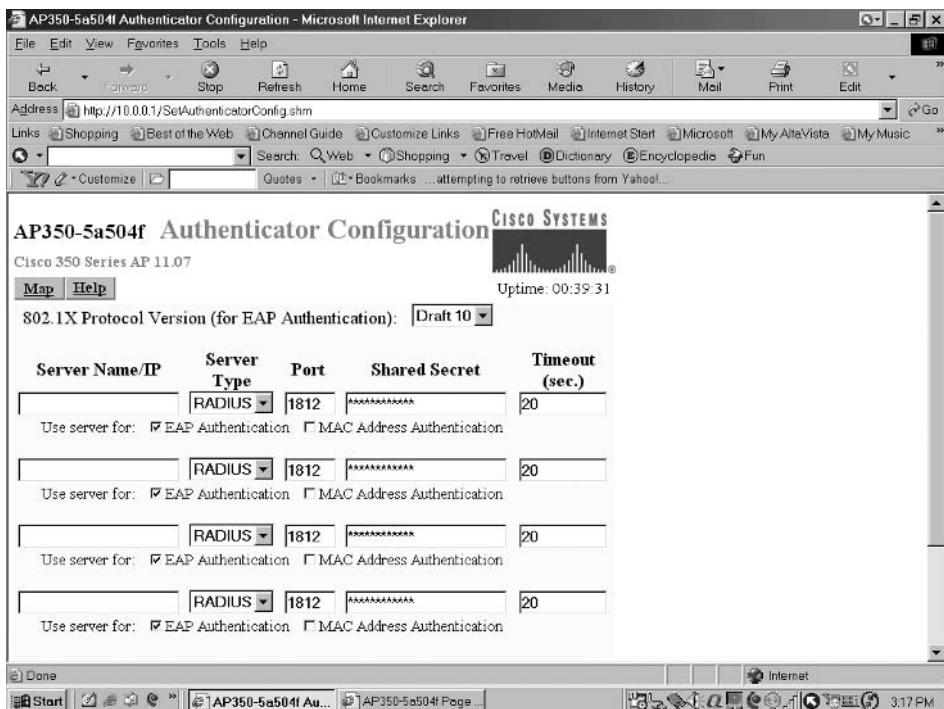


Figure 7.22 The Cisco AP350 Authenticator Configuration page provides support for one primary and up to three backup servers.

those devices must be configured to allow the applicable data to flow to their destination. Thus, you may need to reconfigure your organization's firewalls and routers to allow access from the access point to the RADIUS server. The shared secret entry for each row is matched against the shared secret value, configured on the server the row is pointed at via the specified host name or IP address. The timeout value whose default setting is 20 seconds represents the number of seconds the access point should try contacting the primary authentication server prior to contacting a backup server, assuming one is specified. From a practical standpoint, if your organization has a centralized authentication server on a distant network you may need to increase the timeout value.

At the bottom of the Authentication Configuration page you will note that by default the server is set to be used for EAP authentication. If you previously created a list of allowable MAC addresses for your authentication server you can enable this option to provide this additional method of authentication.

7.1.16.4 WEP Configuration

The sixth and last entry in the Security Setup screen provides you with the ability to configure WEP. Selecting the sixth entry results in the display of the AP Radio Encryption page, which is shown in Figure 7.23. If you focus upon Figure 7.23 you will note that the default setting is open authentication, which enables initial RF access to the access point. Prior to enabling WEP you need to enter at least one key in one of the four encryption key fields. If you are using EAP authentication you need to select key 1 as the transmit key, as the access point will use that key to encrypt multicast data it transmits to EAP-enabled clients.

7.1.16.5 The AP Radio Page

One of the more unusual aspects of the Cisco access point encountered by this author was a new firmware revision that adds several interesting security

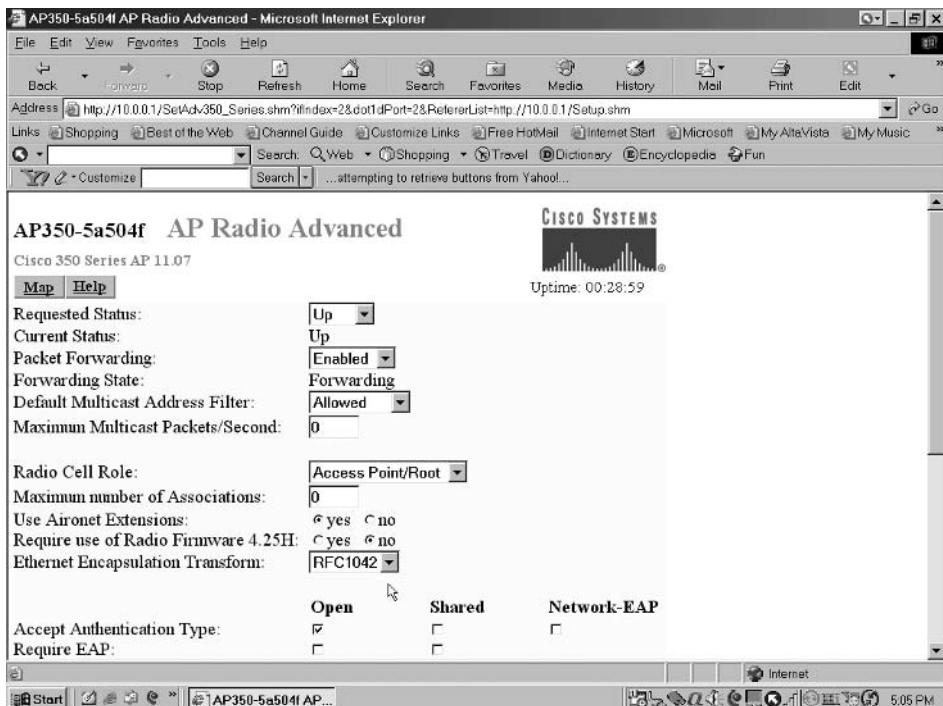


Figure 7.23 The Cisco AP350 Radio Data Encryption page is used to define authentication and WEP key settings.

features to the capability of the AP. If you have firmware release 11.07 or earlier, your AP Advanced Radio page will appear similar to that shown in Figure 7.24.

The AP Radio Advanced page, which is not accessible from the Security Setup page, was originally developed to provide control to a wide range of settings. For example, the first entry, ‘Requested Status,’ turns the radio on and off. The second entry, ‘Packet Forwarding,’ allows you to enable or disable the movement of packets between an Ethernet connection and the radio side of the access point. The third entry, ‘Default Multicast Address Filter,’ enables you to create a filter to either pass traffic to all MAC addresses except those specified or block traffic to those specified addresses. The next entry, ‘Maximum Multicast Packets/Second,’ is used to control the number of multicast packets that can pass through the radio port each second.

To access the AP Radio Advanced page you would select the Advanced column entry under Network Ports for the AP Radio row entry in the Setup page previously shown in Figure 7.19. While this is certainly a strange location

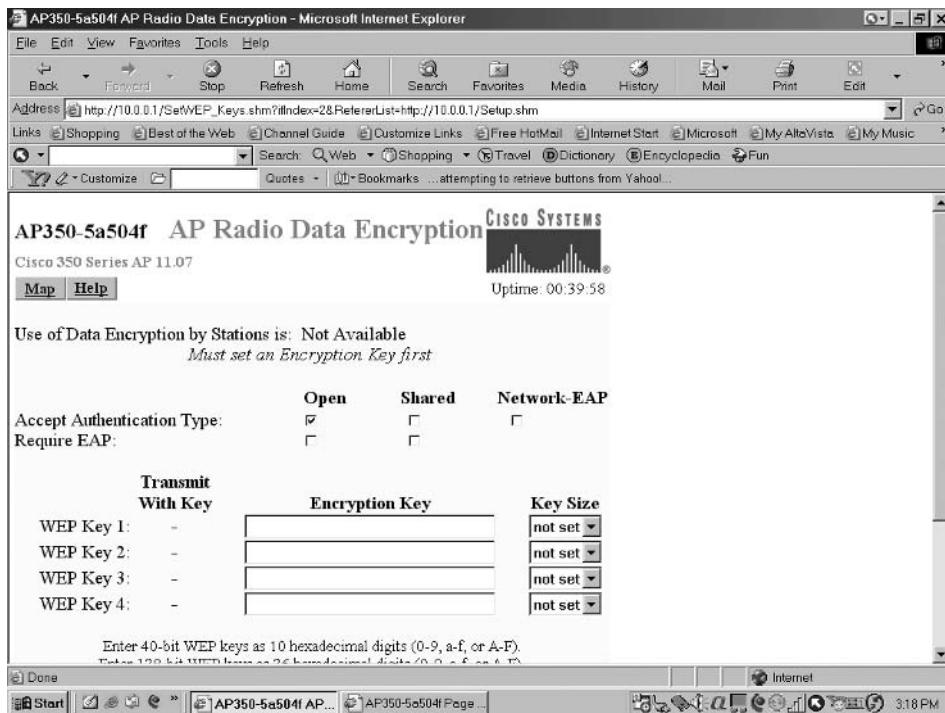


Figure 7.24 The Cisco AP350 AP Radio Advanced Page.

for enabling security options, as we will shortly note, those options are only applicable to recent firmware releases for the AP350 and in this author's opinion, were added to the firmware revision to the page shown in Figure 7.24 as an 'afterthought.'

Returning to our examination of Figure 7.24, the fifth selectable entry shown in that illustration actually represents a repeat of another configuration page as it permits a setting of the role of the radio. As previously discussed, the role of the access point radio can be set to root, repeater or client. The following entry, 'Maximum number of Associations,' permits you to control the maximum number of devices that can be associated with the access point at a particular point in time. Here the default value of 0 means that there is no maximum. The next entry, 'Use Aironet Extensions' when set to 'Yes' enables three extensions to Cisco Aironet 802.11 features that are only available in newer firmware than version 4.25.08 installed on the access point used by this author. Those security related entries and a description of their use are listed in Table 7.2 and are displayed below the Ethernet Encapsulation Transform entry, (shown in Figure 7.24) when a new version of firmware is installed in the access point.

The three security related features listed in Table 7.2, that are applicable to recent Cisco AP350 firmware, are designed to overcome an existing security vulnerability. The use of Message Integrity Check prevents the possibility of undetected bit flipping; however, as previously discussed it adds overhead to each frame that adversely effects throughput. The use of the temporal key integrity protocol (TKIP), which is described in Section 7.2, defends against the WEP key recovery attack previously described. In doing so TKIP removes the predictability that an unauthorized third party relies upon to determine the WEP key in use by constructing a database of packets, IVs and keys and examining the use of IVs and keys to create known sequences within monitored packet fields. When you enable TKIP, all WEP enabled client stations associated with the access point using TKIP must also support WEP

TABLE 7.2 AP Radio Advanced page Security Related Settings (applicable to new firmware)

Setting	Description
Enhanced MIC Verification for WEP	Enabling Message Integrity Check (MIC) prevents bit-flipping attacks on encrypted data
Temporal Key Integrity Protocol	TKIP removes the predictability that allows a third party to passively determine the WEP key in use.
Broadcast WEP Key Rotation Interval	Results in the access point dynamically broadcasting a new WEP key at a defined interval.

key hashing. Otherwise, those clients will not be able to communicate with the access point.

The third security related feature, broadcast WEP key rotation interval, provides you with the ability to specify the period or interval in seconds when the access point will broadcast a new WEP key. In selecting an appropriate interval you only need to consider keeping the number of frames used by a single key to under a million, since most key recovery programs require over five million frames in order to perform their dastardly deed. If your client software does not support TKIP, broadcast key rotation can be considered as a viable alternative to the key hashing performed by TKIP. Some additional comments concerning key rotation in a Cisco access point environment are in order. When you enable this feature only wireless client stations using LEAP or EAP authentication can use the access point. If your clients are configured to use static WEP with either open, shared key or EAP-MD5 authentication, they will not be able to access the AP350 when broadcast key rotation is enabled.

7.1.17 Closing thoughts

In concluding this section we will briefly examine the basic AP Radio Hardware page which is shown in Figure 7.25. Unlike the AP Radio Advanced page, where certain security related features are only applicable to new firmware, the AP Radio Hardware page has one setting that can be used to facilitate security under all versions of firmware. That setting is the transmit power level, which is highlighted in Figure 7.25 at its default setting of 100 mW. Other available settings for the transmit power level include 1, 5, 20 30 and 50 mW. When considering adjusting the power level of the access point you should also consider adjusting the transmit power level of client cards. In a Cisco wireless LAN environment the available transmit power levels for client cards vary by card as indicated in Table 7.3.

By carefully performing a site survey using a lower level of transmit power you may be able to minimize or block RF leakage outside your organization's building or floor. Concerning the latter, as discussed earlier, you can also consider positioning the access point antennas to minimize RF radiation in the vertical plane. One additional setting you can consider when using the AP Radio Hardware page is the transmit antenna setting, which by default is set to 'Diversity.' Upon occasion, configuring the transmit antenna to a single left or right setting and lowering the level of transmit power may minimize RF leakage to a level that precludes any threat to your organization. However, as mentioned several times before, reducing the level of transmit power and antenna positioning does not secure your over-the-air transmissions.

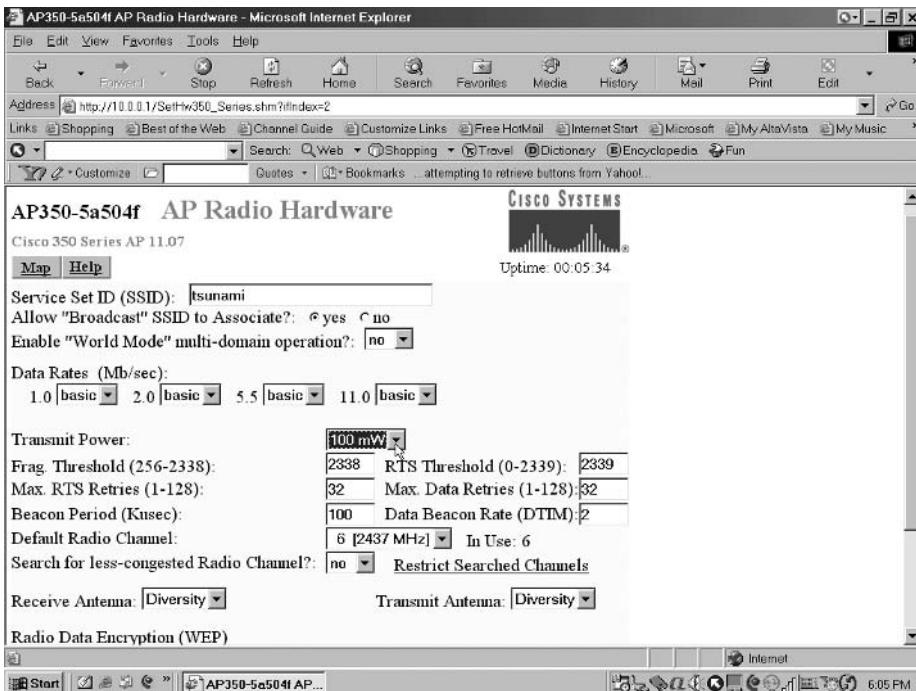


Figure 7.25 The Cisco AP350 AP Radio Hardware page permits you to control the level of transmit power and use of the dual antennas on the access point.

TABLE 7.3 Cisco client adapter power level settings

Client Adapter Type	Power Levels (mW)
350 series PC/LM cards	1, 5, 20, 30, 50, 100
340 series PC cards	1, 30
340 series LM cards	1, 5, 15, 30

Instead, it only makes it harder for an unauthorized third party to observe signal activity and should be used in conjunction with both standardized and non-standardized security techniques as described in this book.

7.2 Evolving encryption

Under the framework of the IEEE 802.11i committee two encryption methods were in the process of being added to wireless LAN standards as a mechanism

to overcome the shortcomings of WEP and its in-the-clear IV. The first method, referred to as the temporal key integrity protocol (TKIP), represents an interim solution developed to fix the most vulnerable aspects of WEP. The second encryption method that is expected to be incorporated into the IEEE 802.11i standard is the Advanced Encryption Standard (AES). While TKIP has recently been incorporated into several vendor products via software, the use of AES requires either a co-processor or a faster processor to operate. This means that companies will need to replace existing client station PC Cards and access points to implement AES when it becomes available for wireless operations. Now that we have a brief overview of the two standards based encryption methods, let's probe a bit deeper into each.

7.2.1 TKIP

The temporal key integrity protocol was developed as an interim solution to overcome some of the security limitations associated with WEP. Those limitations include the ability to bit flip data in frames so that a receiver is non the wiser, the use of weak keys that allow such hacker tools as AirSnort to recover the key in use by constructing a database to analyze, and the reuse of IVs which enables encrypted data to be decrypted without having to discover the encryption key in use. TKIP can be considered as the response to the above-mentioned problems.

7.2.1.1 Components

In actuality, TKIP represents a series of four algorithms that are designed to harden WEP. Those four algorithms and a brief description of the function of each algorithm are listed in Table 7.4.

TABLE 7.4 TKIP algorithms

Algorithm	Description
Message Integrity Code	Adds a tag to each packet to prevent undetected bit flipping
IV sequencing	Associates a packet sequence number with a MIC key to detect a replayed packet.
Per packet key mixing	Prevents weak key attacks by substituting a temporal key for the WEP base key.
Rekeying	Delivery of new keys to prevent a key reuse attack.

As noted earlier, several of the TKIP algorithms are available for individual settings on a Cisco AP350 access point or you can activate TKIP as an entity. Similarly, some other vendor products provide the capability to implement one or more individual TKIP algorithms or the series of algorithms as an entity.

7.2.1.2 Operation

The TKIP process commences with the use of a 128 bit ‘temporal key’ that is shared among client stations and access points. Under the TKIP process the temporal key is combined with the client’s 48 bit MAC address. A 16 byte IV is then added to create an encryption key. Because each client MAC address is unique, this process results in each station using a different key to encrypt and decrypt data. Like WEP, TKIP uses RC4 to perform encryption. However, another difference between the two results from the fact that TKIP changes temporal keys every 10,000 packets. This action ensures that any passive monitoring cannot be used to create a database to discover the key in use.

7.2.1.3 Advantages of Use

Although TKIP represents a suite of algorithms developed as a temporary measure to overcome the security vulnerabilities associated with WEP, it has several advantages over the use of AES that will be covered in the next section. First, TKIP can be added via firmware upgrades to existing hardware. This is no small issue when one considers the ten million WEP compatible wireless LAN PC Cards and access points that will be shipped by the time you read this book. Secondly, the large base of WEP compatible equipment is able to interoperate with many vendor implementations of TKIP products. This means that an organization can gradually migrate to TKIP instead of having to update all devices at one time.

7.2.2 AES

The Advanced Encryption Standard (AES) attacks the WEP security vulnerability by providing a significantly enhanced encryption capability. The proposed use of AES for wireless LANs is in recognition of its selection by the U.S. Department of Commerce National Institute of Standards and Technology (NIST) to replace the aged Data Encryption Standard (DES) that uses a relatively short 56 bit key. In fact, AES is now a Federal Information Processing Standard, specified in FIPS Publication 197, dated November 26, 2001. According to that publication, AES specifies a FIPS approved

symmetric block cipher cryptographic algorithm capable of using cryptographic keys of 128, 192, and 256 bits to encrypt data and to decrypt data in blocks of 128 bits. AES is now defined for use by U.S. Government organizations as a cryptographic algorithm for protecting sensitive, unclassified information.

7.2.2.1 Overview

AES specifies what is referred to as the Rijndael algorithm which can process data blocks of 128 bits using cipher keys whose length can be 128, 192, or 256 bits. The possible use of three key lengths is referred to as AES-128, AES-192 and AES-256. The AES algorithm performs operations on a two-dimensional array of bytes known as the ‘State.’ The State consists of four rows of bytes with the number of bytes per row being divisible by 32. Initially, input bytes to be enciphered are copied into the State array, after which the AES cipher operation is performed on its contents, which are then copied into an output array. Once data is placed into the State array, the AES algorithm performs a round function on the elements of the array which consists of four different byte oriented transformations. Those transformations are listed in Table 7.5.

The transformation process is fully described in the previously referenced FIPS publication and will not be repeated. However, what is worth noting is that the transformation process requires a considerable amount of array element manipulation. In addition, the round function is parameterized via the use of a key scheduler that uses a one dimensional array of four byte words derived from another array element manipulation process. Taken together, the AES encryption process is currently beyond the capability of a firmware addition to existing wireless LAN products. Thus, although AES is considerably stronger than WEP and has no known weak keys, its implementation will require the use of a co-processor or a more intensive processor than is currently embedded in existing products. Due to this, the use of AES in wireless LAN products can be expected to occur in entirely new capability products. Such products will only work with non-AES compatible devices when AES is disabled on the newer products.

TABLE 7.5 AES byte-oriented transformation

-
1. Byte substitution.
 2. Shifting rows of the State array by different offsets.
 3. Mixing the data within each column of the State array.
 4. Adding a Round Key to the State.
-

7.3 VPNs and tunneling protocols

In this concluding section we will focus upon another method that can be used to secure our wireless LAN traffic. That method is the creation of a Virtual Private Network (VPN) through the use of a tunneling protocol that encrypts traffic. First we will briefly review the concept behind the use of VPNs and the major types of virtual private network topologies. Once this is accomplished we will look at two common tunneling protocols, describing their basic operation and utilization as well as their advantages and disadvantages. Because this author is a firm believer in the old adage ‘the proof of the pudding is in the eating,’ we will conclude this section with a discussion of the use of Microsoft Windows built-in VPN capabilities which can be used to secure your wireless communications. However, prior to discussing VPNs a few words about the rationale for not discussing Secure Sockets Layer (SSL) as a mechanism to protect wireless transmission is in order. While SSL is indeed a viable mechanism to secure your wireless transmission, it is only normally applicable for client to Web server applications. This means that client access to other applications, such as email and FTP, would not be secure. The exception to this requires the acquisition of proprietary hardware. Such hardware is installed on the wired network and functions as a conversion device by placing FTP, email and other applications within an SSL protected browser packet for delivery to software on the wireless client. Due to this, we will only mention that you can consider its use if you can restrict your wireless clients to accessing a secure Web server on the wired network or are willing to use proprietary hardware and software.

7.3.1 VPN overview

A VPN represents a temporary connection established over a shared network that interconnects two locations as if they were connected via a private leased line. The original concept behind the use of VPNs was economics. To illustrate why economics was a considerable factor in the use of VPNs, consider Figure 7.26, which shows the interconnection of three geographically separate locations via a private network and via virtual paths over a public network (VPN). Assume each location is 1,000 miles from the other two locations and the cost of a T1 line operating at 1.544 Mbps is \$4/mile per month. Then, the monthly repetitive cost of communication for a private network to interconnect the three locations becomes; $3 \text{ locations} \times \$4,000 \text{ per location, or } \$12,000$. Also note that each router requires two high-speed serial interfaces whose one time cost can be several thousand dollars. Now let’s

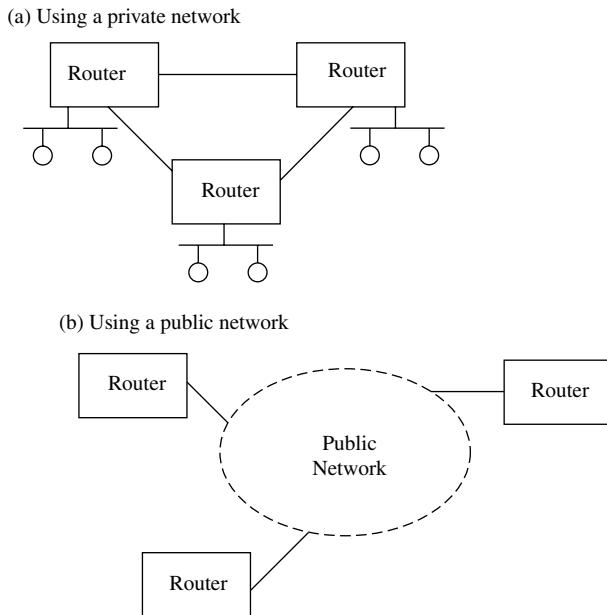


Figure 7.26 Interconnecting three geographically separated networks.

examine the economics associated with the use of a public network as shown in the lower portion of Figure 7.26.

If the public network has high speed access points in each city where your organization has an office, you only need to install an intra-city T1 access line to the public network. Assuming the cost of the T1 circuit and monthly access cost associated with using the public network is \$1,000, then the cost to interconnect the three geographically separated locations via the transport facilities of the public network becomes \$3,000 per month, a significant reduction in comparison to the cost of a private network. In addition, each router now only requires one high speed serial port, reducing the cost of required hardware. Thus, economics can be considered as the driving force behind the use of VPNs as a mechanism to interconnect geographically dispersed locations.

7.3.2 Need for security

Because data flowing over a shared network could be intercepted and either read or modified, security in the form of encryption as well as data integrity is required. In addition, because any user of the shared network could conceivably access one of the locations connected to the network,

authentication represents another security related feature required for secure VPN communications.

7.3.3 Types of VPNs

There are two basic types of VPNs you can construct through the use of a public network's transport facility. Those types of VPNs are referred to as site-to-site and remote access.

7.3.3.1 Site-to-Site VPN

A site-to-site VPN is commonly used to interconnect all clients located at one geographic area that have traffic destined to a second geographic area via the use of a public network transport capability. The site-to-site VPN is bi-directional, enabling data to flow in the opposite direction and is usually implemented via the use of specialized hardware installed at each location connected to the public network. Figure 7.27 illustrates an example of a site-to-site VPN.

In examining Figure 7.27 note that the VPN gateway is commonly a router with VPN capability, the latter typically implemented through software and either a co-processor or accelerator chip that performs processing intensive encryption. The VPN gateway can also be a stand-alone hardware device that encapsulates and encrypts the payload of each client destined for another geographic location of the organization. When fabricated as a stand-alone device without routing capability the gateway resides behind the router. A third hardware option is a firewall with VPN capability, which would also reside behind the router.

As data enters the VPN gateway from the local network its destination is examined against the contents of a state table of IP addresses. If the data is destined to another VPN network address, the payload will be encrypted. Otherwise, if the packet is destined to CNN's Web site or another address that does not reside on your organization's distant network, it is allowed to flow through the gateway without alteration. By performing all VPN operations at one location, client stations do not have to be configured to support VPN operations nor is specialized hardware or software required. Now that we have an appreciation for a site-to-site VPN, let's take a look at the second type of virtual private network.

7.3.3.2 Remote Access VPN

A second type of VPN is referred to as a remote access VPN. A remote access VPN occurs on an individual client basis with each client using

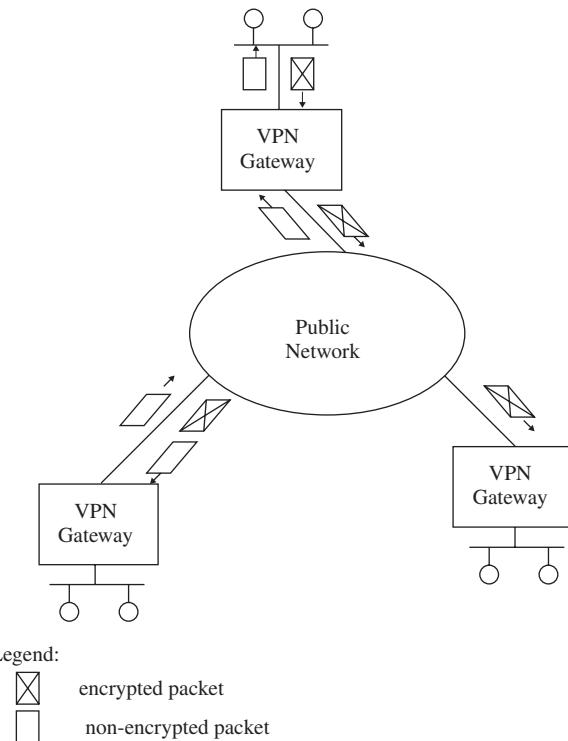


Figure 7.27 Site-to-site VPN.

software to create a secure virtual connection over a public network to a distant location. At the distant location the client will connect to a VPN gateway. That gateway can be a router with specialized software, a separate VPN hardware based gateway or a VPN server. Due to Microsoft's large installed base of Windows client software, the addition of a VPN capability to clients to access a Windows server running VPN software became the most popular method for supporting a remote access VPN connection capability. Figure 7.28 illustrates an example of client stations at different geographical locations using individual remote access VPN connections to a central VPN server. Depending upon the configuration of the server, remote clients may be restricted to accessing data and applications on the server or they may obtain the ability to access other computers located on the network where the VPN server resides.

The development of remote access VPNs dates to the requirement for mobile employees to access corporate data centers securely in an economical

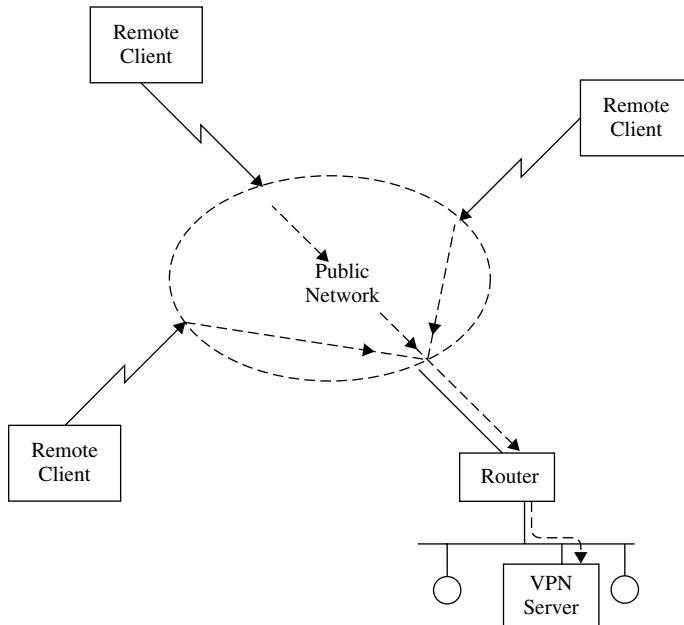


Figure 7.28 Remote Access VPN.

manner. The growth in the Internet made distant access possible through a local telephone call, enabling those traveling to remote locations to access their organization's computational facilities via an Internet connection. Over the past decade several protocols were developed to support remote access VPNs to include PPTP, L2TP and IPSec. Prior to discussing those protocols a few words about the applicability of the two basic types of VPNs to securing wireless transmissions is in order.

7.3.4 Applicability to wireless LANs

In comparing site-to-site and remote access VPN topologies it is important to note the security coverage associated with each method. Under the site-to-site VPN topology data flows encrypted between VPN gateways. In comparison, under the remote access VPN method data flows encrypted from each client to the VPN server. In comparing these two methods it should be obvious that only the remote access VPN method would be applicable to securing wireless transmission. This is because under the remote access VPN method data is protected from the client to the VPN server. Thus, if your wireless clients are configured to support a remote access VPN protocol their transmission

through the air to an access point and over the wired infrastructure to a VPN server would be secure. In comparison, even if a VPN gateway was located next to an access point when a site-to-site VPN is employed, transmission from each client to the gateway would not be protected. Now that we have an understanding as to why we would use remote access VPN connections to protect wireless LANs, let's examine the protocols that can be used.

7.3.5 VPN protocols

There are three common protocols used as a VPN tunneling protocol. Those three protocols are the Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP) and IPSec. In actuality, IPSec actually represents a collection of protocols and is commonly used in conjunction with L2TP. Although vendors other than Microsoft offer IPSec VPN solutions, in this section we will focus upon PPTP and the use of L2TP with IPSec in a Windows environment.

7.3.6 PPTP

The point-to-point tunneling protocol (PPTP) represents an extension to PPP that supports multi-protocol traffic via VPN tunnels, enabling remote users to access corporate networks via the Internet. PPTP dates to the mid-1990s when it was proposed by Ascend and Microsoft Corporation to the IETF. In addition to being enabled on a client station, PPTP can be enabled in an Internet Service Provider (ISP) router, resulting in two methods in which clients can access a Remote Access Services (RAS) facility on a Windows server via an Internet connection. The first method is referred to as an ISP-PPTP connection, while the second method is referred to as a PPTP Client Enabled method.

7.3.6.1 ISP-PPTP Access

The top portion of Figure 7.29 illustrates the data flow for an ISP-PPTP connection via a tunnel through the Internet to a Windows server running RAS. The client will use the PPP to request a connection to the RAS server via the ISP router or an ISP access concentrator. The router or access concentrator will establish the VPN by initiating a PPTP session, tunneling information from the PPP client. This method of tunneling enables the use of any operating system which supports PPP dial-up.

7.3.6.2 PPTP Client Enabled Access

The lower portion of Figure 7.29 illustrates a second and by far the most popular method of PPTP tunneling, referred to as PPTP client enabled access.

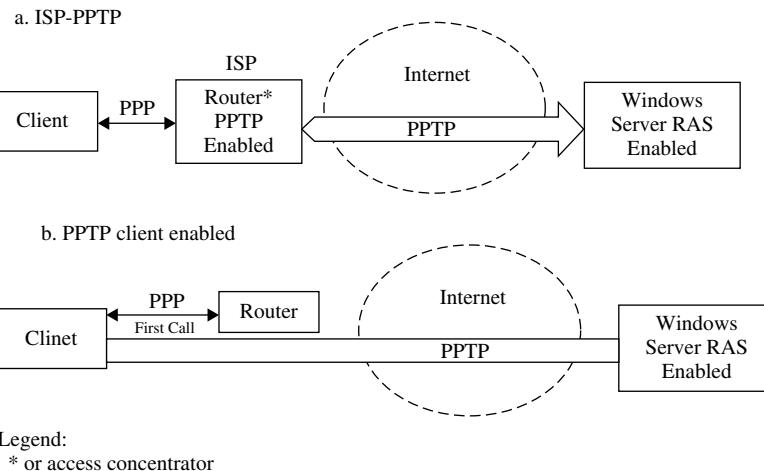


Figure 7.29 PPTP tunneling methods.

Under this method a client dials the ISP and establishes a PPP session. Concurrent with the PPP session the client sets up a PPTP channel to the Windows server running RAS, becoming a virtual node on the corporate LAN. This method of PPTP tunneling is only applicable to PPTP enabled clients.

While the original development of PPTP in association with RAS enabled servers to support mobile users dialing via ISP access nodes, PPTP is now supported via LAN connections. This means you can use PPTP via a hard wired or wireless LAN connection to a Windows server on a wired network.

7.3.6.3 Packet Types

PPTP uses two types of packets, data and control. Data packets are variable in length and encapsulated in IP. Control packets are fixed length sent via a TCP connection.

7.3.6.4 Control Packets

Figure 7.30 illustrates the format of a PPTP control connection packet. This packet will transport call control and management messages used to establish and maintain the PPTP tunnel. Examples of control packets include such periodic queries as PPTP Echo-Request and PPTP Echo-Reply messages used to detect a connectivity failure between the client and server. As indicated in Figure 7.30, PPTP control messages consist of IP and TCP headers and a PPTP control message framed by a data link header and trailer.

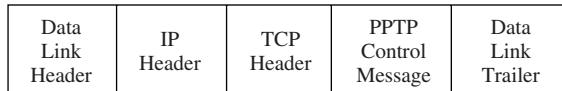


Figure 7.30 PPTP Control Connection Packet Format.

7.3.6.5 Data Packets

In comparison to control packets that are transported in the clear, data packets have their payloads encrypted. Figure 7.31 illustrates the format of PPTP tunneled data. Note that the initial PPP payload is encapsulated with a PPP header, resulting in the creation of an encrypted PPP frame. That frame is then encapsulated using a Generic Routing Encapsulation (GRE) header. GRE, which is described in RFCs 1701 and 1702, represents a client protocol of IP (defined by IP protocol number 47 in the IP header protocol field). The use of GRE provides a streamlined method for encapsulating data transmitted over an IP network. Because PPTP data tunneling begins with the use of a PPP payload, this method permits the transport of IP, IPX and even NETBEUI in a secure manner.

In examining the format of the PPTP control and data frame shown in Figures 7.30 and 7.31, we can observe two limitations. First, control frames are transported in the clear. Secondly, although the PPP payload is encrypted there is no method to authenticate the contents of the packet. Instead, the authentication we will discuss next is only applicable to the PPTP client.

7.3.6.6 Authentication Methods

The authentication methods supported by PPTP are based upon those supported by the device at the opposite end from the client. In a Windows 2000 server environment PPTP based VPN connections support Extensible Authentication Protocol (EAP), Challenge-Handshake Authentication Protocol (CHAP), Microsoft CHAP (MS-CHAP), Shiva Password Authentication Protocol (SPAP) and the Password Authentication Protocol (PAP). Either EAP-Transport Level Security (EAP-TLS) or MS-CHAP must be used for the

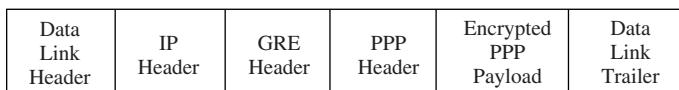


Figure 7.31 PPTP Data Format.

PPP payload to be encrypted through the use of Microsoft Point-to-Point Encryption (MPPE). It should be noted that the use of MPPE provides link encryption and not true end-to-end encryption. If you require encryption from the client to the server hosting the resource or service being accessed by the client application, you should consider the use of IPSec after the PPTP tunnel is established. Now that we have an overview of PPTP let's discuss L2TP and IPSec.

7.3.7 L2TP and IPSec

The Layer 2 Tunneling Protocol (L2TP) represents a combination of PPTP with Cisco Systems Layer 2 Forwarding (L2F) protocol. L2TP was originally developed to support dial-in client VPN access to remote routers or Frame Relay Access Devices (FRADs) via an ISP L2TP compatible router or access concentrator. L2TP is documented in RFC 2661 and operates by encapsulating PPP frames that can be theoretically sent over IP, X.25, Frame Relay and ATM networks. However, at the present time the use of L2TP is only defined for IP. When transmitted over an IP network L2TP frames are encapsulated as UDP messages to include both control and data messages.

Unlike PPTP, for which data packets are encrypted via MPPE, L2TP encapsulated PPP frames in a Microsoft Windows environment are encrypted through the use of IPSec.

7.3.7.1 Packet Types

Like PPTP, there are two types of L2TP packets. Those types of packets are control and data.

7.3.7.2 Control Packets

Figure 7.32 illustrates the format of an L2TP control packet. Note that IPSec encrypts the message, unlike PPTP in which control messages are not encrypted. In a Windows environment both the L2TP client and server

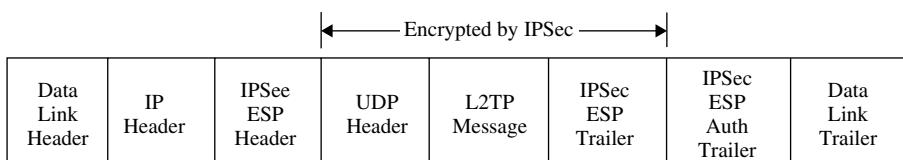


Figure 7.32 L2TP Control Packet Format.

use UDP port 1701. The use of IPSec occurs via the Encapsulated Security Payload (ESP), which represents one of two security related protocols supported by IPSec. The other protocol is the Authentication Header (AH), which is not used by the combination of L2TP with IPSec.

Although L2TP control messages are protected by IPSec and can be considered to flow via a tunnel through a public network, in actuality the mode of operation of IPSec ESP is referred to as an ESP transport mode, one of two nodes of operation supported by ESP. In the transport mode security headers are added before the transport layer header, as previously shown in Figure 7.32.

7.3.7.3 Data Packets

The tunneling of data under L2TP occurs through several levels of encapsulation. First, the initial PPP payload is encapsulated with a PPP header and L2TP header. Next, the resulting L2TP encapsulated packet is again encapsulated with a UDP header, with the source and destination ports each set to a value of 1701. IPSec encapsulation then occurs, with the UDP message encrypted and encapsulated within an IPSec ESP header and trailer, with an IPSec Authentication (Auth) trailer authenticating all data from the IPSec ESP header through the IPSec ESP trailer. This series of encapsulations is indicated by the format of an L2TP data packet shown in Figure 7.33. After the IPSec encapsulation an IP header is added, with the latter containing the source and destination addresses of the VPN client and VPN server. Finally, when transmission occurs the IP datagram is further encapsulated with a data link header and trailer based upon the type of link used, such as a LAN or WAN connection.

7.3.7.4 Authentication

Under L2TP the authentication method used for the creation of tunnels must be the same as the authentication used for the PPP connection. Under Windows

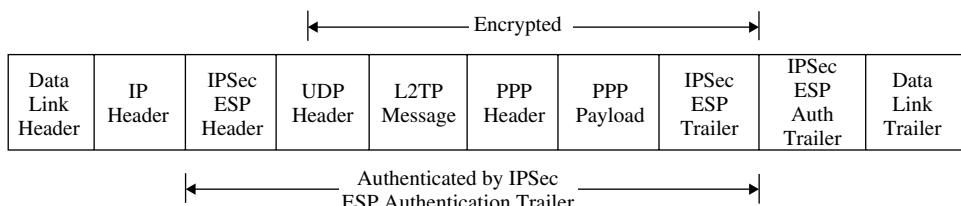


Figure 7.33 L2TP and IPSec Data Packet Format.

2000 available authentication methods include EAP, CHAP, MS-CHAP, SPAP, and PAP, which are also those methods supported by PPTP.

A key difference between the use of PPTP and L2TP over IPSec concerns the need for computer certificates and the method of encryption employed. PPTP uses MPPE encryption, which uses the RC4 cipher. MPPE can use 40, 56, or 128 bit encryption keys. As previously mentioned, under PPTP authentication occurs using PPP based user authentication protocols, such as EAP, CHAP, MS-CHAP, SPAP or PAP. In comparison, under L2TP available encryption algorithms are restricted to the 56 bit key version of the Data Encryption Standard (DES) and Triple DES, with the latter using three 56 bit keys. Concerning authentication, mutual authentication of the VPN client and server occurs when an IPSec ESP security association occurs. This action is accomplished through the use of computer certificates that require a computer certificate to be installed on both the VPN client and server.

In comparing PPTP and L2TP with IPSec, it is obvious that the latter provides a more secure method of VPN communication. This is because both the contents of data and control packets are encrypted and the contents of data packets are verified through the IPSec Authentication trailer. Now that we have an overview of two common tunneling methods used for creating a VPN in a Microsoft environment, let's turn our attention to the use of Windows on a wireless client to create a VPN connection.

7.3.8 VPN operations

On the client station the creation of a VPN connection is facilitated through the use of a ‘network wizard’ in a modern Windows environment, such as Windows XP and Windows 2000.

7.3.8.1 Using the Wizard

To access the wizard you would first open the Network and Dial-up connections icon. You would then double-click on the Make New Connection icon, resulting in the display of the dialog box labeled ‘Network Connection Type,’ which is shown in Figure 7.34. This is the first of a series of easy-to-use dialog boxes displayed by the wizard that allows a minimal amount of user selection. As we will shortly note, under Windows you need to establish a VPN connection using basic defaults prior to being able to change those default settings. Returning to the dialog box shown in Figure 7.34, in this dialog box you would select the radio button to the left of the label ‘Connect to a private network through the Internet’ as indicated by the cursor. Note that if you were configuring a modern version of Windows on a server to accept

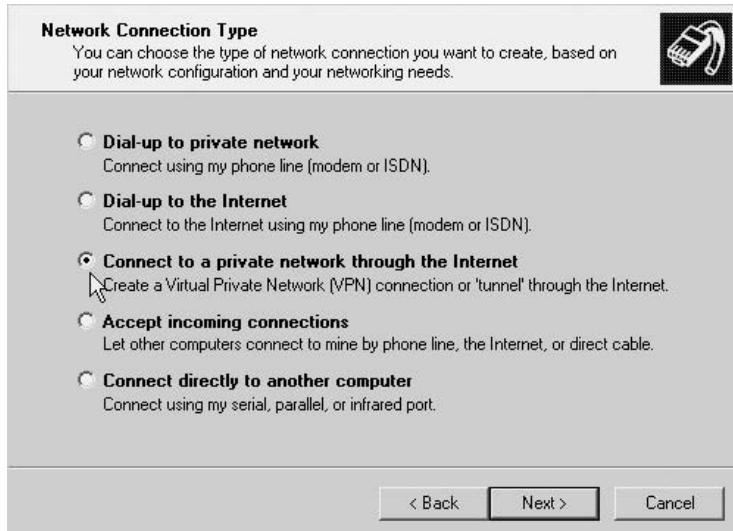


Figure 7.34 On a Windows wireless client you would select the radio button to the left of the label ‘Connect to a private network through the Internet’ to begin the VPN configuration process.

VPN connections you would click on the radio button below the one selected in Figure 7.34.

Once you click on the button labeled ‘Next’ located in the lower right portion of Figure 7.34, a new dialog box will appear. That dialog box, which is shown in Figure 7.35, will prompt you to enter the host name or IP address of the computer or network to which the client will connect. In the example shown in Figure 7.35, it was assumed that the client being configured will connect to a Windows 2000 server whose IP address is 198.78.46.8.

Continuing our client site VPN connection configuration process, the next screen displayed by the wizard will query you concerning connection availability. As indicated in Figure 7.36, you can make the VPN connection available to all users allowed to access your computer or you can restrict the connection for your own exclusive use. As illustrated in Figure 7.36, the radio button to the left of the label ‘For all users’ is shown selected. If you want to restrict the connection for yourself, you would click on the lower radio button to which the cursor is pointing. Once you make your selection you would again click on the button labeled ‘Next,’ resulting in a new dialog box being displayed. That dialog box, shown in Figure 7.37, prompts you for a name for your VPN connection. By default, the name ‘Virtual Private

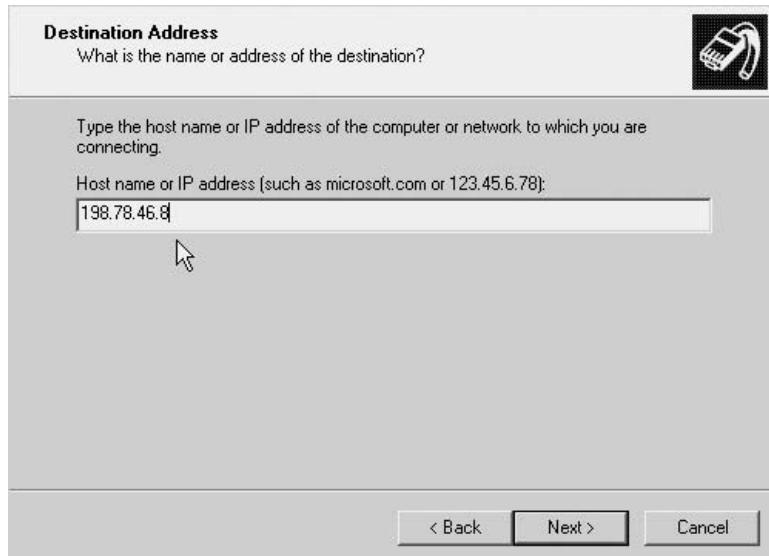


Figure 7.35 Defining the IP address of the host at the end of the tunnel.



Figure 7.36 You can make the VPN connection available to all users that can use your computer or restrict the connection to your use.

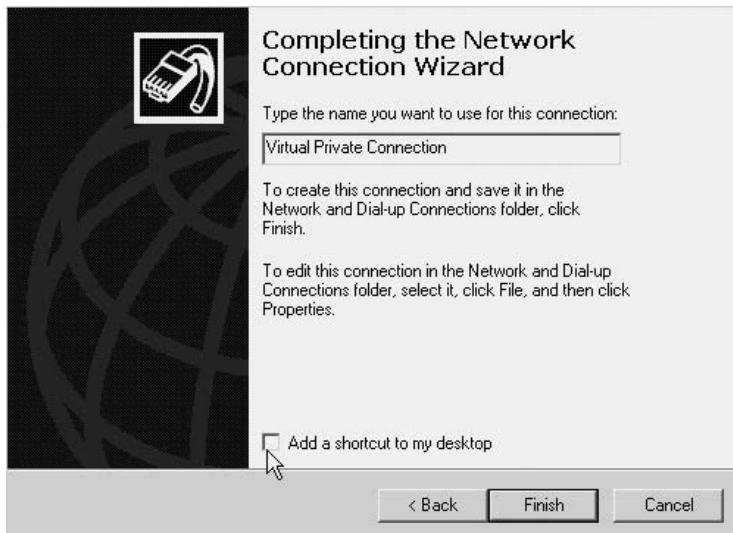


Figure 7.37 Completing the network connection wizard enables you to specify the name for the VPN connection.

'Connection' is used by Windows. If you only plan to have a single VPN connection the default label may be appropriate. However, if you plan to have multiple connections you should use a more descriptive label.

In examining Figure 7.37 it is important to note that in addition to specifying the name for the VPN connection, the dialog box provides a very helpful hint concerning the editing of the connection you have just established. That is, to edit this connection to use settings other than the default which at the present time you are not aware of, you need to select the newly created connection, click on it, and select the button labeled 'Properties.' Thus, to find out more information than that which is provided by the wizard, let's do what it tells us to do. In doing so we will see that in a Microsoft Windows environment the use of the Network Connection Wizard default settings can be easily viewed and, if necessary, modified.

7.3.8.2 Editing the Connection

Because this author likes the philosophy behind the adage 'I'm from Missouri,' let's examine the properties of the VPN connection we have just created. To do so we would open the Network and Dial-up Connections window shown in the left portion of Figure 7.38. We would then open the previously created

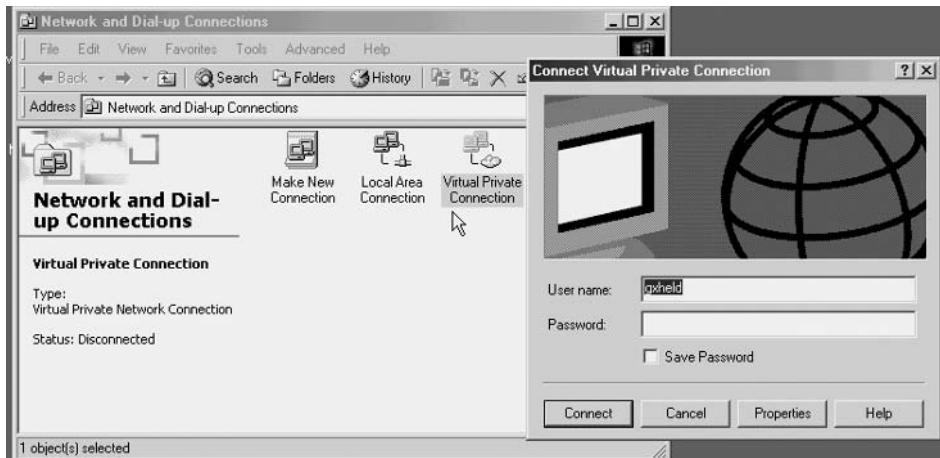


Figure 7.38 To examine or change VPN properties you would click on the VPN connection icon and then select the button labeled Properties from the resulting dialog box.

VPN connection for which we selected the default name of Virtual Private Connection, resulting in the display of the box labeled ‘Connect Virtual Private Connection’ shown in the right portion of Figure 7.38. To examine the default VPN settings under Windows 2000 you would click on the button labeled ‘Properties,’ so let’s do it.

7.3.8.3 VPN Connection Properties

The selection of the Properties box results in the display of a dialog box with five tabs. This dialog box is shown in Figure 7.39, with the tab labeled ‘General’ in the foreground of the box. The primary purpose of the General tab is to define the host name or IP address of the destination. This tab provides you with the ability to change the destination previously entered when you used the wizard to initially configure your VPN connection. Because we did not specify the use of a dial-up connection in the Network Connection Type dialog box, previously illustrated in Figure 7.34, the lower portion of Figure 7.39 is shaded gray.

7.3.8.4 Option Tab

The second tab in the dialog box resulting from the selection of the properties button is labeled ‘Options.’ This tab is shown in Figure 7.40 in the foreground

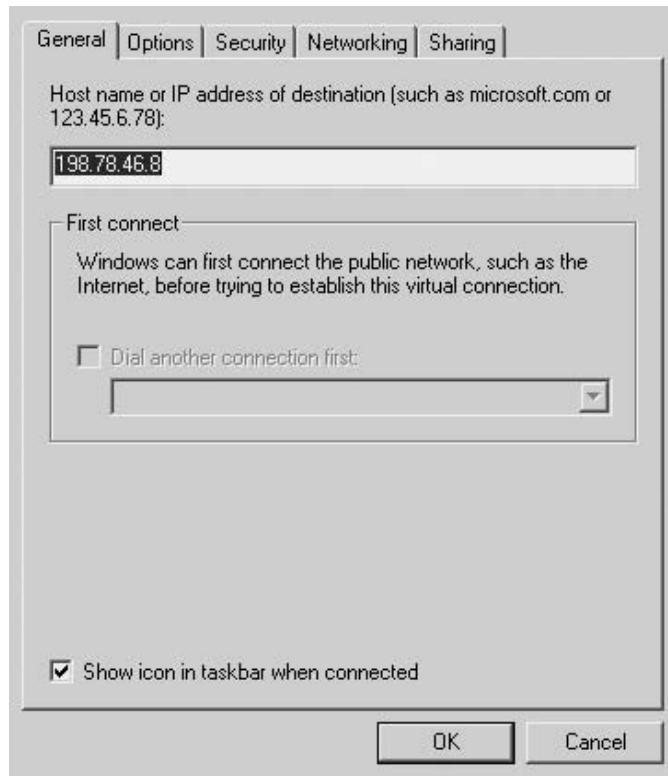


Figure 7.39 The General tab provides the ability to view and change the host name or IP address of the destination.

of the dialog box. There are two areas on the tab, one at the top of the box which is labeled ‘Dialing options,’ while the other, located in the lower portion of the box, is labeled ‘Redialing options.’ Although you will be using a wireless connection instead of a modem dial-up line, the dialing options are also applicable for wireless and wired LAN VPN connections. For example, the first default setting that enables dialing progress while connecting will display a connection progress dialog box if you previously selected the ‘connect to a private network through the Internet’ option shown in Figure 7.34 and are using a LAN connection. Thus, perhaps a better label for the ‘dialing options’ label would be ‘access options.’ Similarly, the next option is applicable for both dial-up and wired and wireless LAN connections. Concerning the second entry under Dialing Options, because we are creating a VPN from the wireless client to a server on the wired LAN and security is an issue, we want to ensure

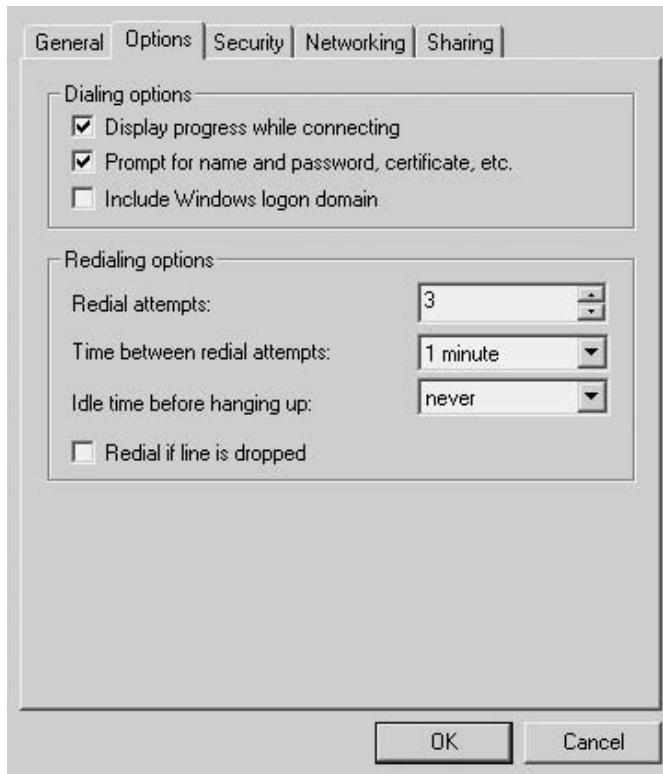


Figure 7.40 The Options tab by default controls prompting for the username and password and results in the display of connection progress information.

that the default setting prompting for name and password in a Windows 2000 client environment remains set.

7.3.8.5 Security Tab

The third tab in the dialog box displayed as a result of selecting the Properties button is the Security tab. An examination of the Security tab will answer some questions you may have about the default settings associated with the use of the wizard to set up a VPN connection, so let's look at its settings. The left portion of Figure 7.41 shows the Security tab in the foreground of the dialog box. In order to show the advanced settings, this author clicked on the radio button associated with 'Advanced' to highlight the button labeled 'Settings.' This action enabled the Advanced Security Settings box to be displayed in the right portion of Figure 7.41. Now that we know the actions that occurred

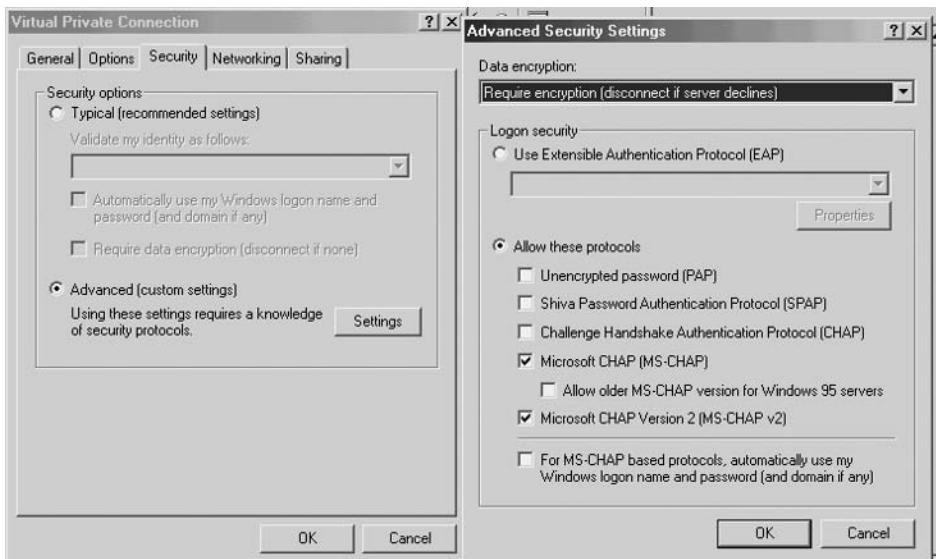


Figure 7.41 The Security tab by default has the radio button to the left of the label ‘Typical’ entry set, precluding the advance settings shown in the right box from being displayed.

to display both boxes, let’s discuss the default settings of the Security tab and the advanced settings available for selection.

When the Security tab is placed in the foreground, the radio button associated with Security options is set to the left of the label ‘Typical’ entry, with validation of your identity set to ‘Require secured password’ in the rectangular box that is currently shown shaded gray. In addition, the box to the left of ‘Require data encryption (disconnect if none)’ is also checked. Thus, by default the VPN connection will require a secure password for authentication and data encryption of packets.

Focusing on the right box in Figure 7.41, by default the Data encryption option is set to ‘Require encryption.’ Other options available for selection include ‘No encryption allowed (server will disconnect if it requires (encryption)’ and ‘Optional encryption (connect even if no encryption).’ Because by default the Security tab is set to ‘require secure password’ for validation of your identity, the Logon Security button to the left of the label ‘Use Extensible Authentication Protocol’ is not set. If you set that button you can select the use of ‘MD5-Challenge’ or ‘Smart Card or other Certificate (encryption enabled)’ while disabling the default protocols allowed in the lower right portion of

Figure 7.41. By default Windows 2000 supports MS-CHAP and MS-CHAPv2 for authentication.

Although the Security tab controls authentication and encryption settings, it does not permit you to define the actual security protocol to be used to create the VPN. In fact, the first three tabs we examined in the Virtual Private Connections dialog box (General, Options and Security) do not provide any capability concerning the selection of the VPN method. Because the VPN method to be used represents a networking protocol its selection occurs under the Networking tab.

7.3.8.6 Networking Tab

In concluding our review of the Virtual Private Connection dialog box we will briefly look at the Networking tab. That tab is shown positioned in

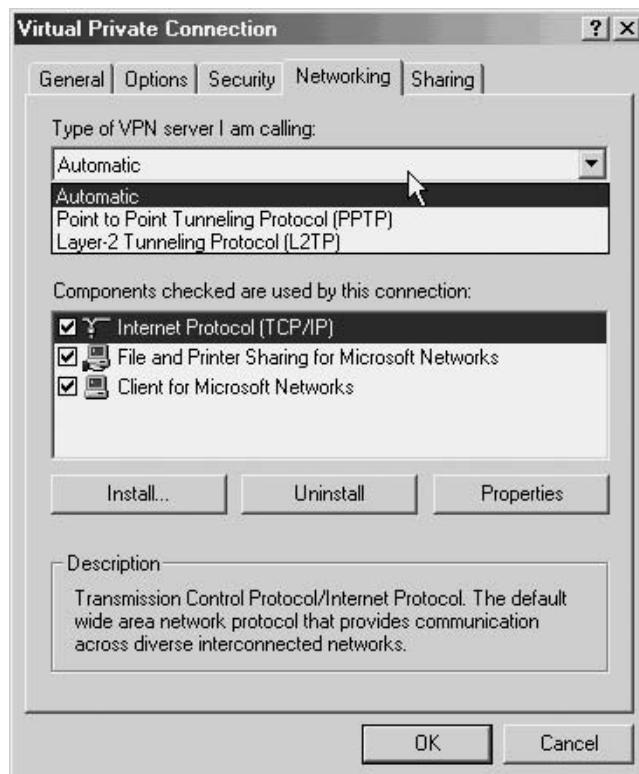


Figure 7.42 The Networking tab provides you with the ability to specify the VPN protocol to be used.

the foreground of the dialog box in Figure 7.42. Note the Networking tab is subdivided into two areas. The top area in the rectangular window permits you to select the type of VPN server you will be establishing a connection with. By default, under Windows 2000, the setting is 'Automatic.' This is because it is assumed you will be accessing a Windows 2000 server, which has the ability to distinguish between the two types of VPN connections it supports. As indicated by the pull-down menu, you can alter the default setting of 'Automatic' by selecting either PPTP or L2TP as the VPN protocol. The lower portion of the Networking tab functions in a similar manner to the normal control panel networking settings selection. That is, you can install and remove components as well as view and assign different properties for a selected component.

If you are operating in a Windows XP or Windows 2000 environment you can usually set up your client VPN connection within a few minutes. By creating a tunnel over your wireless connection through your access point to the server, your over the air communications will be secure regardless of WEP settings. Thus, the creation of a VPN represents another technique in your literal bag of tools you can consider for hardening your organization's wireless transmission.

appendix a

Wireless LAN Security Checklist

As previously noted in this book, there are a range of hardware and software products we can collectively refer to as tools and also many techniques you can consider to harden your organization's wireless LAN. In this appendix those tools and techniques are listed within broad categories in the form of a checklist. You can consider each of the entries in the checklist based upon the current infrastructure of your network, the type of data transmitted over your wireless network, economics, and the potential threat to your organization. Doing so will result in some items being of more value than others to different readers or more accurately, reader organizations.

In the table that follows we grouped the tools and techniques discussed in this book into the collective area of 'category/features.' While the categories are listed alphabetically, their listing does not indicate their relative importance. Thus, both potentially trivial as well as key techniques and tools are simply listed within defined categories, placed in alphabetical order as a mechanism to structure the contents of the table. When using this checklist you can either indicate your specific requirement for a particular security feature or place a notation concerning its use. In fact, you can also use this checklist to compare vendor products by adding two or more columns to compare and contrast vendor features against your requirements.

Category/Feature	Requirement
Access Control	
Authentication of Hardware	_____

Category/Feature	Requirement
Open System	
Shared Key	
MAC Address	
Port based access (802.1x)	
Access Point	
Change access point location	
Change default SSID setting	
Disable SSID broadcasting	
Change default management password	
Enable WEP or another encryption method	
Disable DHCP and assign static IP addresses to clients	
Change default IP address of access point and, if possible, use a different subnet	
Antenna operation	
Orient antenna	
Lower transmit power	
Shield antenna	
Authentication	
Enable user authentication	
CHAP	
Extensible Authentication Protocol (EAP)	
MS CHAP	
Kerberos	
MAC address	
Digital certificates	
Encryption	
Enable WEP	
Use automatic key exchange	
Use Temporal Key Integrity Protocol	
Use software to avoid weak keys	
Use separate uplink/downlink keys	
Firewall	
Install firewall between access point and wired network	
Configure firewall to restrict data traffic from wireless clients based on organizational policy	
Network scan	
Measure signal strength	

Category/Feature	Requirement
On other floors in building	
Outside building	
Use tool like NetStumbler to locate rogue access points	
Use tool like AiroSnort to attempt to recover encryption key in use	
Physical Security	
Establish mechanism for reporting loss of hardware	
Server-based authentication	
Use Cisco's proprietary LEAP	
Use Extensible Authentication Protocol (EAP)	
SNMP	
Verify ASN1 problem fixed	
Obtain latest software patch, if available	
Enable/disable capability	
Restrict access via IP address	
Restrict use via alphanumeric community string	
VPN	
Use tunnel to server on wired LAN	
Use PPTP	
Use L2TP with IPSec	

index

A

access lists 159–161
access point 2, 10–13, 19–20,
 22–23, 39, 46–48, 88–89,
 91–93, 96, 105–106, 114–116,
 142–148, 150–155, 158–159,
 183–192, 201–220
accounting 2, 4, 122–123
ACK frame 26, 45–46
active scanning 47–48
address fields 41
address spoofing 152–153,
 191–192
Advanced Encryption System (see
 AES)
AeroPeek 93–97
AES 32, 221–223
Agere System’s Orinoco PC Card
 14, 88–90, 137–138,
Air Defense 172
AirSnort 109–110, 139, 221
American National Standards
 Institute (see ANSI)
An Initial Analysis of the IEEE
 802.1x Standard paper
 189–190
ANSI 27
antenna 64, 71–84, 118
antenna diversity 118–119
antenna gain 73–74, 76–78

antenna positioning 5–6, 81–83,
 118, 166–172
antenna sensitivity 78–79
antenna shielding 5–6, 118,
 166–172
AP Manager 137–142
Arbaugh, William 189–190
associate request frame 47, 51
associate response frame 48, 51
association process 46–52
authentication 2–3, 21–23, 32,
 52–53, 122–124, 150–153,
 173–174, 183–193, 198, 210,
 214–215, 231–232, 242
awake power state 168

B

bandwidth 64
Basic Service Set (see BSS)
beacon 5, 40, 46, 49, 96, 168
beam width 74
Bel 66–67
BOOTP 208
Bootstrap Protocol (see BOOTP)
Borisov, Nikita 103–107
bridge 10, 13
broadcast monitoring 141–145
BSS 18–21, 94, 114
buffer overflow 136

C

Carrier Sense Multiple Access with Collision Avoidance (see CSMA/CA)
Carrier Sense Multiple Access with Collision Detection (see CSMA/CD)
Challenge Handshake Authentication Protocol (see CHAP)
CHAP 6, 153–154, 187, 231
Cisco Aironet 114, 118–120, 121–123, 170–171, 173–177, 193–200, 203–220
Cisco access lists 159–161
Client Encryption Manager 177–181, 199
closed system option 154–155
collision 43
Community Settings 136–138, 209
Contention Free-End frame 46
Contention Free-End plus contention Free-ACK frame 46
Controlled Port 189
CRC 56
CSMA/CA 24, 45
CSMA/CD 24
CTS frame 26–27, 44–45, 132–133
Cyclic Redundancy Check (see CRC)

D

Data Encryption Standard (see DES)
data modification 124
dB 67–68
dBd 74
dbi 73–74, 77
dBm 68–69, 77
DCF 24

deauthentication 23
Decibel (see dB)
Decibel above 1 mw (see dBm)
Decibel dipole (see dBd)
Decibel isotropic (see dBi)
DES 222
DFS 31
DHCP 6, 14–15
dictionary attack 106, 122, 146
diffused infrared transmission 7
dipole antenna 72, 76–77
directional antenna 79–80
Direct Sequence Spread Spectrum (see DSSS)
disassociate frame 51, 192
Distributed Coordination Function (see DCF)
Distributed Wireless Security Auditor 147
Distribution System (see DS)
doze power state 168
DS 20–21, 37–39
DSSS 7, 13, 28–29
dual-port model 189
Duration/ID subfield 41
dwell time 28
Dynamic Frequency Selection (see DFS)
Dynamic Host Configuration Protocol (see DHCP)
dynamic key exchange 109, 135, 156–157

E

EAP 173, 183–184, 187–189, 193, 198–199, 215–216, 231
EAPOL 185–187
EAP over LAN (see EAPOL)

EAP-TLS 191, 231
 eavesdropping 117–121
 effective Isotropic Radiated Power (see EIRP)
 EIRP 74–75, 77
 Encapsulated Security Payload (see ESP)
 encryption 2–4, 232, 234, 241
 encryption attacks 133–135
 ESP 233
 ESS 20
 exception report 123
 Extended Service Set (see ESS)
 Extensible Authentication Protocol (see EAP)

F

FCS field 42–43
 FHSS 7, 13, 28
 file sharing 124–130
 filtering 12–13, 141–144, 210–211
 firewall 7
 flooding 11–12, 141–144
 folder sharing 6
 forwarding 12, 141–144
 fragment 39, 42
 Frame Body Field 42
 Frame Check Sequence field (see FCS field)
 Frame Control Field 36–41
 Frame Formats 35–59
 Free Space Loss (see FSL)
 frequency 62–64
 frequency analysis 58, 135
 Frequency Hopping Spread Spectrum (see FHSS)
 frequency spectrum 64–66
 FSL 75–76

G

Generic Routing Encapsulation (see GRE)
 Goldberg, Ian 103–107
 GRE 231

H

hardware theft 146
 hidden node problem 26–27, 43–46, 132
 hot zone 85

I

IBSS 19–20, 39
 ICV 56, 87, 105–106, 124, 190–191
 IEEE standards
 802.1x 173, 183–187, 200–203
 802.11 7, 13, 28–30, 81, 150–153
 802.11a 13, 30, 81
 802.11b 7, 13, 30, 81
 802.11c 30
 802.11d 31
 802.11e 31
 802.11f 31
 802.11g 31
 802.11h 31–32
 802.11i 32
 impulse noise 69
 infrared 29
 Infrastructure Basic Service Set (see IBSS)
 Infrastructure networking 12, 19
 Institute of Electrical and Electronics Engineers standards (see IEEE standards)
 Integrity Check Value (see ICV)

- Intercepting Mobile Communications
paper 103–107
- interframe spaces 25–26
- Initialization Vector (see IV)
- IPSec 4, 6, 232–235
- IPSU program 204–205
- intrusion detection 172
- Iouannidas, John 108–109
- ITU 62
- IV 42, 55–56, 58, 86–87, 103–104, 106, 135, 221
- IV collisions 86, 103, 105, 135
- J**
- jamming 59, 131–133
- K**
- KarlNet 155–156
- Key ID field 86, 90
- key recovery attack 59
- key rollover 157, 219, 221
- L**
- Layer 2 Tunneling Protocol (see L2TP)
- LEAP 122, 173–177, 193, 198–199
- Lightweight Extensible Authentication Protocol (see LEAP)
- lockout 4
- L2TP 232–234
- M**
- MAC address 5
- MAC address authentication 150–153
- management frame 48–49
- man in the middle attack 87, 106, 189–191
- masquerade 121–123
- MD5 153, 200
- Media Access Control address (see MAC address)
- Message Integrity Check (see MIC)
- MIC 191, 218, 221
- Mishra, Arunesh 189–190
- monitoring equipment 83–84
- monopole antenna 72
- More Data subfield 40
- More Fragments subfield 39
- MS-CHAP 153–154, 231
- N**
- NAT 15–17
- NAV 26, 45
- Net Allocation Vector (see NAV)
- Network Address Translation (see NAT)
- Network Interface Card (see NIC)
- network name 5, 88, 90, 94, 113–117, 139
- network name broadcast 5
- Network Stumbler 91–93, 139
- NIC 8–10
- null authentication 53, 122
- O**
- OFDM 30
- omni-directional antenna 9, 73–74
- Open System Authentication 22, 53, 122, 150, 198
- order subfield 41
- Orinoco Client Manager Link Test 83–84

Orthogonal Frequency Division Multiplexing (see OFDM)
out-of-band 22

P

PAP 153
passive scanning 46, 48
passphrase 57, 90, 108, 155–156
password 21, 47, 145–146, 162
Password Authentication Protocol (see PAP)
PCF 49
PEAP 173
peer-to-peer networking 19
PIFA 72, 75
Planar Inverted ‘F’ Antenna (see PIFA)
Point Coordination Function (see PCF)
Point-to-point tunneling protocol (see PPTP)
port/address table 11–13, 141–144
port-based access control 183–198
power level 69, 74–75
power management 40, 168
power management subfield 40
power measurements 66–69
Power Save-Poll frame 46
PPTP 229–232
private network addresses 15
propagation loss 75–76
Probe Request frame 50, 132
Probe Response frame 50, 132

Q

QoS 31
Quality of Service (see QoS)

R

RADIUS server 151–153, 175, 184–185, 214–215
RC4 97–103, 107–108, 134
reassociation frames 52
remote access VPN 226–229
Remote Dial-In User Service (see RADIUS)
repeater access point 209
retransmission 39
retry subfield 39
RFC 1918 15, 17, 145
Rijndael algorithm 223
Rivest, Ronald 97
rogue access points 147–148, 173
Root Access Point 209
RTS frame 26, 44–45, 132–133
Rubin, Aviel 108–109

S

Secure ID 185–186
Secure Sockets Layer (see SSL)
security checklist 245–247
sequence control field 42
session hijack 189–192
shared key authentication 22–23, 53, 122, 150
shared key cryptology 2
shielding 80–81
Short Interframe Spaces (see SIFS)
SIFS 25
signal-to-noise ratio 69–71
Simple Network Monitoring Protocol (see SNMP)
Site Survey Client 209
site-to-site VPN 226–230
slot time 24

slotted waveguide antenna 79
SMC Networks bus-based adapter card 9–10
SMC Networks 802.11a Wireless Access Point 10
SMC Networks 802.11a Wireless Card Bus Adapter 8–9
SMC Networks Barricade Wireless router 17–18, 114–115, 145, 161–165
SNMP 135–141
space diversity 10
SSID 21, 47, 59, 113–117, 147, 196–197
SSL 6, 97, 163, 191
Station Set ID (see SSID)
stream cipher 97–102
Stubblefield, Adam 108–109
supplicant 184–185
symmetrical key 54

T

Temporal Key Integrity Protocol (see TKIP)
thermal noise 69–70
TIM 40, 49–50
TLS 163, 187, 191
TKIP 32, 124, 218–219, 221–222
TPC 31–32, 119, 168–170, 219–220
traffic injection 105
Traffic Indication Map (see TIM)
Transmit Power Control (see TPC)
Transport Layer Security (see TLS)
TurboCell 155–156

U

uncontrolled port 185, 189
uni-directional antenna 9, 73–74
Unsafe at Any Key Size paper 102–103
Using the Fluhrer, Mantin and Shamir Attack to Break WEP paper 108–109

V

VCS 26–27, 43
Virtual carrier sensing (see VCS)
Virtual private network (see VPN)
VPN 4, 124, 224–243

W

Wagner, David 103–107
Walker, Jesse R. 102–103
wavelength 63–64
Weakness in the Key Scheduling Algorithm of RC4 paper 107
weak key 102, 158
WEP 2–5, 23–24, 29–30, 40–41, 53–59, 85–111
WEPCrack 110–111
WEP subfield 40–41
white noise 69
wildcard mask 159–160
Windows XP 200–203
Wired Equivalent Privacy (see WEP)
wireless bridge 13
wireless LAN station 8–9
wireless router 13–18