Sniffer® Technologies

FOR USE WITH SNIFFER PORTABLE 4.8

NETWORK GENERAL™

Contents

Preface ix

Audience ix
Getting More Information ix
Contacting Network General xii
. xiii

1 Introducing Wireless Functionality 3

Overview 3
Supported Wireless Adapters 3
Overview of Installing the Wireless Adapters and Drivers 5
Notes on Upgrading from Sniffer Portable 4.7 or 4.7.5 5

2 Installing the 802.11a/b/g Adapter / Driver 7

Overview 7
Installing the 802.11a/b/g Adapter 7
Windows XP 7
Windows 2000 9
First Time Installation (Windows 2000) 9
Using the 802.11a/b/g Adapter as a Normal Network Adapter 10
802.11a/b/g Adapter Installation Notes and Issues 11

3 Installing the ORiNOCO Gold Adapter / Driver 13

Overview 13
Installing the ORiNOCO Gold Adapter 13
Windows NT 4.0 13
Windows XP 17
Windows 2000 19
First Time Installation 19
Updating Existing Drivers 20
Using the ORiNOCO Gold as a Normal Network Adapter 22
ORiNOCO Gold Installation Notes and Issues 23

4 Installing the Enterasys Adapter / Driver 25

Overview 25
Installing the Enterasys RoamAbout Adapter 25
Windows NT 4.0 25
Windows XP 30
Windows 2000 31
First Time Installation 32
Updating Existing Drivers 33
Using the Enterasys RoamAbout as a Normal Network Adapter 35
Enterasys RoamAbout Installation Notes and Issues 36

5 Installing the Spectrum 24 Adapter / Driver 37

Overview 37
Installing the Spectrum 24 Model 4121 in Windows NT 4.0 37
Troubleshooting Spectrum 24 Installation Issues in Windows NT 42
Installing the Spectrum 24 Model 4121 Adapter in Windows XP 43
Installing the Spectrum 24 Model 4121 in Windows 2000 45
First Time Installation 45
Updating Existing Drivers 47
Using the Spectrum 24 as a Normal Network Adapter 50
Spectrum 24 Installation Notes and Issues 51

6 Installing the Cisco Aironet Adapter / Driver 53

Overview 53
Installing the Cisco Aironet in Windows NT 4.0 53
Installing the Cisco Aironet in Windows XP 58
Installing the Cisco Aironet in Windows 2000 60
First Time Installation 61
Updating Existing Drivers 62
Using the Cisco Aironet as a Normal Network Adapter 64
Cisco Aironet Installation Notes and Issues 66

7 Installing the Proxim 802.11a Adapters / Drivers 67

Overview 67
Installing the Proxim 802.11a Adapter in Windows XP 67
Installing the Proxim 802.11a Adapter in Windows 2000 69
First Time Installation 69

Updating Existing Drivers 70
Using the Proxim 802.11a Adapter as a Normal Network Adapter 72
Proxim 802.11a Adapter Installation Notes and Issues 74
Using the Proxim 802.11a Harmony to Monitor “2X” Networks 75

8 Creating Local Agents for Wireless LAN Adapters 79

Overview 79
Creating a Local Agent to Use the Wireless LAN Adapter 79

9 Configuring Wireless LANs to Capture 81

Overview 81
Monitoring Wireless Networks 81
Setting Wireless Options 82
Setting Configuration Options 83
Channel Surfing Mode and Capture Triggers 84
Setting Encryption Options 85
40-Bit Encryption 85
128-Bit Encryption 86
Configuring Encryption Options 86
Entering Encryption Keys in Hex Format 86
Entering Encryption Keys in ASCII Format 88
Setting the Security Options 89
Setting Expert Wireless Options 90
Adding Known Addresses to the Expert’s List 92
Adding Known Addresses from the Host Table 92
Adding Known Addresses from the Postcapture Display 93
Autodiscovering and Adding Addresses from the Address Book 95
Adding Known Addresses Manually in the 802.11 Options Tab 95
Determining a Wireless Unit’s Full Hexadecimal Address 97
Importing and Exporting Known Addresses 97

10 Advanced Features for Wireless Analysis 99

Overview 99
Differences Between Wireless Network Displays 100
Notes on Proprietary Implementations of the 802.11a Standard 101
Dashboard Counters for Wireless Networks 101
How Utilization is Calculated 103
The Dashboard’s Gauge Tab 104

The Dashboard's Detail Tab 104
The Dashboard's 802.11 Tab 106
Statistics Counters in the 802.11 Tab 106
Management Frame Type Counters in the 802.11 Tab 108
Control Frame Type Counters in the 802.11 Tab 110
Dashboard Graphs for Wireless Networks 111
Working with the Dashboard Graphs 112
Setting Thresholds for the Dashboard Statistics 113
Host Table Counters for Wireless Networks 114
Global Statistics Counters for Wireless Networks 118
Post-Analysis Views for Wireless Networks 121
802.11 View in the Post-Analysis Matrix Tab 121
802.11 View in the Post-Analysis Host Table Tab 123
802.11 View in the Post-Analysis Protocol Distribution Tab 125
802.11 Information in the Post-Analysis Statistics Tab 127
Define Filter Options for Wireless Networks 130
Filters for 802.11 Packet Types 131
Filters for Wireless LAN Error Packet Types 133
Protocol Decodes for Wireless Networks 133
Postcapture WEP Decryption 134
Expert Objects and Alarms for Wireless Networks 136
Expert Object Detail Displays for Wireless LANs 137
DLC Layer Expert Detail Display with 802.11 Information 138
Wireless Layer Expert Detail Display for a Wireless Station 142
Expert Alarms for Wireless Networks 146
Global Layer Expert Alarms for Wireless Networks 146
Channel Mismatch 146
PLCP Error 147
Wireless Layer Expert Alarms for Wireless Networks 147
ACK Frame Timeout 147
Association Failure 148
Authentication Failure 148
CTS Frame Timeout 149
Deauthentication 150
Disassociation 150
Mcast/Bcast Fragmentation 151
Missing Fragment Number 151
Oversized WLAN Frame 152

Reassociation Failure 152
Rogue Access Point 153
Rogue Mobile Unit 154
Runt WLAN Frame 155
Same Transmitter and Receiver Address 155
Transmitter Address Is Broadcast 155
Transmitter Address Is Multicast 155
WEP-ICV Error 156

Index 157

Preface

This guide describes how to install wireless adapters and drivers to run Sniffer® Portable network analyzer on wireless networks, as well as Sniffer software features for wireless networks.

Audience

This guide is intended for wireless network IT Professionals who are working with Sniffer Portable network analyzer software.

Getting More Information

Source	Contents
Sniffer Portable Installation Guide	Provides the system requirements and installation instructions for Sniffer Portable and Sniffer Portable enhanced drivers.
Sniffer Portable User's Guide	Provides a comprehensive overview of all Sniffer Portable features.
Sniffer Portable Expert Alarms Reference Guide	Describes each of the alarms generated by Sniffer Portable's Expert analyzer, along with their related thresholds.
Switch Expert Guide	Describes how to connect and configure Sniffer Portable to use Switch Expert features.
Sniffer Mobile Operations Guide	Provides information specific to configuring, and operating Sniffer Mobile. Sniffer Mobile provides decodes and Expert Analysis for Mobile IP protocols.
Sniffer Reporter	Describes how to install and configure Sniffer Reporter to generate a wide variety of reports based on data collected by Sniffer network analysis and monitoring products.
Sniffer Tool Collection's Sniffer Focused Analysis Guide	Describes how to use Sniffer Focused Analysis to leverage existing Sniffer trace files for additional analysis and troubleshooting.

Source	Contents
Sniffer Tool Collection's Sniffer Capture Format Converter	Describes how to use Sniffer Capture Format Converter to convert existing third-party trace files to .cap format.
Sniffer Wireless Guide	Describes how to install, configure, and operate Sniffer Portable with a supported wireless network adapter.
Sniffer Voice Operations Guide	Provides information specific to configuring and operating Sniffer Voice. Sniffer Voice provides decodes and Expert analysis for Voice over IP (VoIP) protocols.
ATM Adapter Reference Guide	Describes how to install, connect, and configure Sniffer Portable when using ATM hardware. Describes ATM interface pods.
ATMbook Reference Guide	Describes how to install, connect, and configure the ATMbook to capture and generate packets using Sniffer Portable.
Full Duplex 10/100 Ethernet Reference Guide	Describes how to install, connect, and configure Sniffer Portable when using the Full Duplex Ethernet PCI adapter.
Upgrading the Full Duplex 10/100 Ethernet PCI Adapter Guide	Describes how to use the FlashUpd utility provided with Sniffer Portable to upgrade the FPGA firmware used on the FDX 10/100 Ethernet PCI adapter.
Gigabit Ethernet Reference Guide	Describes how to install, connect, and configure Sniffer Portable when using the Gigabit Ethernet PCI adapter.
WAN Adapter Cards Reference Guide	Describes how to install, connect, and configure Sniffer Portable when using the LM2000 or HSSI adapter.
Snifferbook Ultra Reference Guide	Describes how to install and configure the Snifferbook Ultra unit and optional Phys.
Snifferbook Reference Guide	Describes how to install, connect, and configure Sniffer Portable when using the Snifferbook.

Source	Contents
Help	Product information that is accessed from within the application. • The Help system provides high-level and detailed information. Access from either the Help menu option or the Help button in the application. • Context-sensitive (also called What's *This?*) Help provides brief descriptions of the selections in the application. Access by right-clicking an option, pressing the [F1] control key, or dragging the question icon to an option.
Release Notes	*README file.* Product information, system requirements, resolved issues, any known issues, and last-minute additions or changes to the product or its documentation.

Contacting Network General

Customer Service

Get help with license entitlement, registrations, grant number inquiries, tech support validation and more by contacting the Network General Customer Service department at:

North America phone: 1-800-764-3337 (1-800-SNIFFER)

Email:

support@networkgeneral.com

Web:

http://www.networkgeneral.com/ContactUs.aspx

The department's hours of operation are 7:00 AM to 7:00 PM Central time, Monday through Friday.

International phone numbers:

http://www.networkgeneral.com/ContactUs.aspx

Latin America: +55 (11) 5180-6643

Europe: +44 (0) 1753 217500

Australia/New Zealand: +61 (2) 9761 4200

Asia: +65 6222 7555

Japan: +81 3-5219-1221

Mail:

Network General Corporation (North America)

Customer Service Department

Mail Stop 2S362

5000 Headquarters Drive

Plano, TX 75024

USA

Customer Service International Address

Network General International BV (EMEA)

Customer Service Department

PO Box 58326

1040 HH Amsterdam

The Netherlands

Technical Support

Visit Network General Technical Support at:

- http://www.networkgeneral.com/TechnicalSupport.aspx

Sniffer University

Sniffer University is a comprehensive educational resource for building and enhancing all network professionals' skills in fault and performance management. Sniffer University has trained over 70,000 network professionals worldwide. The Sniffer Certified Professional Program provides network professionals industry-recognized accreditation as experts in their field.

For more information:

- Toll-free: 866-764-3337
- Email: education@networkgeneral.com
- Web: http://www.networkgeneral.com/SnifferUniversity.aspx

Consulting Services

Our consultants provide an expert supplemental resource and independent perspective to resolve your problems. They are ready to assist you during all stages of network growth, from planning and design, through implementation, and with ongoing management. They will help integrate our products into your environment and troubleshoot or baseline network performance. Our consultants also develop and deliver custom solutions to help accomplish your project goals. Currently, custom and product consulting are available.

For more information:

- http://www.networkgeneral.com/Consulting.aspx

SECTION 1

Installing Wireless Adapters and Drivers

Introducing Wireless Functionality

Installing the 802.11a/b/g Adapter / Driver

Installing the ORiNOCO Gold Adapter / Driver

Installing the Enterasys Adapter / Driver

Installing the Spectrum 24 Adapter / Driver

Installing the Cisco Aironet Adapter / Driver

Installing the Proxim 802.11a Adapters / Drivers

Introducing Wireless Functionality 1

Overview

Wireless analysis consists of the Sniffer Portable software and a supported wireless adapter and driver. This section provides a brief overview of wireless analysis functionality, including:

- *Supported Wireless Adapters* on page 3
- *Overview of Installing the Wireless Adapters and Drivers* on page 5

The following chapters in this section describe how to install each wireless adapter supported by the software with its corresponding enhanced driver. Please note, you must successfully install Sniffer Portable before installing your specific wireless adapter.

- *Installing the 802.11a/b/g Adapter / Driver* on page 7
- *Installing the ORiNOCO Gold Adapter / Driver* on page 13
- *Installing the Enterasys Adapter / Driver* on page 25
- *Installing the Spectrum 24 Adapter / Driver* on page 37
- *Installing the Cisco Aironet Adapter / Driver* on page 53
- *Installing the Proxim 802.11a Adapters / Drivers* on page 67

Supported Wireless Adapters

Sniffer Portable has been tested with the wireless LAN adapters listed in Table 1-1.

NOTE: Although the Sniffer software may work with other versions of these adapters, these are the only versions explicitly tested and supported. See the Sniffer software readme file that accompanied your product shipment for the latest information on supported adapters.

Table 1-1. Supported Wireless Adapters

Supported Adapter	Notes
Atheros AR5001X+ and AR5002X Chipset Wireless	Supports 802.11a/b/g.
Cisco Aironet 340 (product number PCM-34x)	To use the Cisco Aironet with the Sniffer software, you must also have the following: • Version 4.23 or higher of the Aironet firmware This item is available for download from the Cisco web site. This manual describes how to use the Aironet Client Utility to upgrade the Aironet firmware to a version supported by the Sniffer software.
Cisco Aironet 350 (product number PCM-35x)	To use the Cisco Aironet with the Sniffer software, you must also have the following: • Version 4.23 or higher of the Aironet firmware This item is available for download from the Cisco web site. This manual describes how to use the Aironet Client Utility to upgrade the Aironet firmware to a version supported by the Sniffer software.
Cisco Aironet 802.11a/b/g AIR-CB21AG-x-K9 CardBus based on AR5002X Chipset	Where x can be A (America), J (Japan), E (Europe) or W (World).
8660WD 802.11a/b/g Cardbus Card World Gold 8480WD 802.11a/b/g Cardbus Card World Gold based on AR5001X+ Chipset	Manufactured by Proxim Corporation. **Note:** A Sniffer Enhanced driver is not provided for the 8660WD 802.11a/b/g Cardbus Card World Gold.
Proxim Harmony 802.11a CardBus Card	Manufactured by Proxim Corporation.
Proxim Orinoco 11 a/b/g/ Combo Card	Manufactured by Agere Systems, formerly the Microelectronics Group of Lucent Technologies.
ORiNOCO Gold PC card manufactured by Agere Systems	Manufactured by Agere Systems, formerly the Microelectronics Group of Lucent Technologies.
RoamAbout 802.11b PC Card	Manufactured by Enterasys Networks.
Spectrum 24 802.11b Model 4121	Manufactured by Symbol Technologies.

Overview of Installing the Wireless Adapters and Drivers

The wireless analysis software is included as part of the general Sniffer Portable release. Installing the Sniffer software will install the wireless functionality.

After installing the Sniffer software, install one of the wireless LAN adapter cards supported by the Sniffer software along with its corresponding Network General driver. This step is performed differently depending on your adapter and operating system. Separate procedures are provided for the Atheros a/b/g chip-based cards on Windows 2000 and Windows XP, as well as for the ORiNOCO Gold, Spectrum 24, Cisco Aironet, and Proxim Harmony on Windows NT, Windows XP and Windows 2000.

After installing the Sniffer software, the wireless adapter card, and the supported driver, start the Sniffer software and create a new “local agent” for the wireless LAN adapter. See *Creating a Local Agent to Use the Wireless LAN Adapter* on page 79.

IMPORTANT: You ***must*** reinstall any existing installed Sniffer Technologies drivers to receive the benefits of the updated software!

Notes on Upgrading from Sniffer Portable 4.7 or 4.7.5

If you are upgrading your Sniffer Portable installation to 4.8, after upgrading from 4.7 or 4.7.5, the miniport driver for all existing WLAN adapters needs to be updated.

Installing the 802.11a/b/g Adapter / Driver 2

Overview

This chapter describes how to install the adapters and drivers for supported 802.11a/b/g wireless cards.

Supported 802.11a/b/g cards include the Atheros AR5001X+ and AR5002X Chipset Wireless cards, the 8660WD 802.11a/b/g Cardbus Card World Gold, the 8480WD 802.11a/b/g Cardbus Card World Gold, and the Proxim Orinoco 11 a/b/g/ Combo Card.

- *Installing the 802.11a/b/g Adapter* for:
  - *Windows XP* on page 7
  - *Windows 2000* on page 9
- *Using the 802.11a/b/g Adapter as a Normal Network Adapter* on page 10
- *802.11a/b/g Adapter Installation Notes and Issues* on page 11

Installing the 802.11a/b/g Adapter

The following sections provide operating system-specific information for installing supported 802.11a/b/g adapters and drivers.

Windows XP

This section describes how to install a supported 802.11a/b/g adapter and driver on a Windows XP system.

To install the 802.11a/b/g adapter and driver in Windows XP:

1. After installing the Sniffer software, log into Windows XP as an Administrator.
2. Insert the 802.11a/b/g based wireless card in an available card slot or PCMCIA slot on the target machine. Windows XP will automatically detect the new card and install its native device driver.

   NOTE: If Windows XP does not install the device driver for the wireless card, then install the original driver from the CD provided by the vendor of the wireless card.

3. Open the Network Connections folder through **Start > Control Panel > Network Connections**.
4. Right-click the Wireless Network Connection entry associated with the 802.11a/b/g adapter and select **Properties**.
5. Click **Configure** in the Wireless Network Connections Properties dialog box to open the Adapter Properties dialog box for the 802.11a/b/g adapter.
6. Click the **Driver** tab.
7. Click **Update Driver** to open the Hardware Update Wizard.
8. Select **Install from a list or specific location (Advanced)** and click **Next**.
9. Select the **Don't search** option and click **Next**.
10. Click **Have Disk**.
11. In the Install from Disk dialog box, click **Browse** and navigate to the Atheros.ABG\ WinXP subdirectory where the driver files for the 802.11a/b/g adapter are installed.

    NOTE: The location for Sniffer Portable drivers is C:\Program Files\NAI\SnifferNT\Driver\en\Atheros.ABG\WinXP.

12. Click **OK** in the Install from Disk dialog box.
13. If the operating system is configured to alert you to unsigned drivers, a dialog box will appear warning you that you are about to install a driver that has not been verified by Microsoft Corporation. Click **Continue Anyway** to continue the installation.

14 Click **Finish** to complete the installation.

15 Click **OK** in the Adapter Properties dialog box.

16 After the enhanced driver for the Cisco Atheros a/b/g card is installed, the Atheros Client Utility (ACU) is disabled.

17 For Sniffer Portable users: If you did not uninstall the QoS Packet Scheduler Service during the installation of the Sniffer Portable software, you should disable it for this adapter now. See the *Sniffer Portable Installation Guide* .

18 Create a new local agent in to use the adapter. See *Creating a Local Agent to Use the Wireless LAN Adapter* on page 79.

Windows 2000

This section describes how to install the 802.11a/b/g adapter and driver on a Windows 2000 system. The procedure is somewhat different whether you are updating an existing driver for the wireless adapter (either a previous version of the Sniffer driver or another vendor's driver) or installing the adapter and driver for the first time. Use the appropriate procedure below.

- *First Time Installation (Windows 2000)* on page 9
- *Using the 802.11a/b/g Adapter as a Normal Network Adapter* on page 10

First Time Installation (Windows 2000)

For Windows 2000, install the adapter for the first time by inserting the card in the PC and using the Found New Hardware Wizard.

To install the 802.11a/b/g adapter and driver in Windows 2000 for the first time:

1 After installing the Sniffer software, log into Windows 2000 as an Administrator.

2 Insert the 802.11a/b/g wireless adapter in an available Type II PC card slot on the target machine.

3 Windows 2000 presents a Wizard to help you install a new driver for the 802.11a/b/g adapter. Click **Next**.

NOTE: If Windows 2000's plug-and-play feature automatically installs a driver for the adapter instead of starting the Found New Hardware Wizard, turn to *Using the 802.11a/b/g Adapter as a Normal Network Adapter* on page 10 to update the existing driver.

---

4 In the Install Hardware Device Drivers window, select the **Search for a suitable driver for my device** option and click **Next**.

5 In the Locate Driver Files window, check only the **Specify a location** option and click **Next**.

6 When prompted, click **Browse**, navigate to the Atheros.ABG\WinXP subdirectory where the driver files are installed, and click **Open**.

NOTE: The location for Sniffer Portable drivers is C:\Program Files\NAI\SnifferNT\Driver\en\Atheros.ABG\Win2K.

---

7 Click **OK**.

8 Windows 2000 scans for the driver and presents the Driver Files Search Results window. Click **Next** in the Driver Files Search Results window when the specified driver is found.

9 Click **Yes** on the Digital Signature Not Found warning to continue the installation.

10 When the Add/Edit Configuration Profile dialog box appears, the installation procedure is the same as the *Using the 802.11a/b/g Adapter as a Normal Network Adapter* procedure.

Using the 802.11a/b/g Adapter as a Normal Network Adapter

When the Sniffer software is connected to the 802.11a/b/g wireless adapter, the card operates in promiscuous mode and cannot participate as an active member of the wireless LAN. However, when the Sniffer software is not connected to the 802.11a/b/g adapter, you can use the adapter to participate actively in a wireless network.

During a normal installation of the 802.11a/b/g wireless adapter, you are given the option of configuring a profile for normal wireless network participation (including configuring the ESSID, WEP keys, and so on). If you did not configure these settings during the initial installation of the adapter (or if you want to change the current settings), you can configure them later in either of the following ways. However, do **not** make changes to the 802.11a/b/g adapter's configuration while the Sniffer software is running.

- Using the **Wireless Network** option in the Control Panel.
- Using the wireless adapter's vendor-supplied configuration utility.

See the 802.11a/b/g card vendor documentation for details.

NOTE: For Windows XP, use the **Wireless Network** tab in the Wireless Network Connection Properties dialog box to set wireless network participation parameters.

802.11a/b/g Adapter Installation Notes and Issues

Keep the following notes and tips in mind when working with the 802.11a/b/g wireless adapter:

- After exiting the Sniffer software, it may take up to a minute for the wireless adapter to transition to normal wireless network participation.
- The client utility will not function while the Sniffer software is running. However, the client utility can be used once the user exits from the Sniffer software.
- If the machine has multiple card slots, you can prevent potential problems by always using the wireless adapter in the same slot.
- While configuring the 802.11a/b/g adapter, you may see the following warning: *Can not access your wireless card. Please remove and reinsert PC card to activate settings*.

  This warning can safely be ignored.
- After the enhanced driver for the Cisco Atheros a/b/g card is installed, the Atheros Client Utility (ACU) is disabled.
- Use the **Safely Remove Hardware** option when removing the cardbus card. Make sure the Sniffer software is properly shut down before the card is removed.
- Aegis Protocol (IEEE802.1x) should not be bound to the driver of the adapter as shown in Figure 2-1.

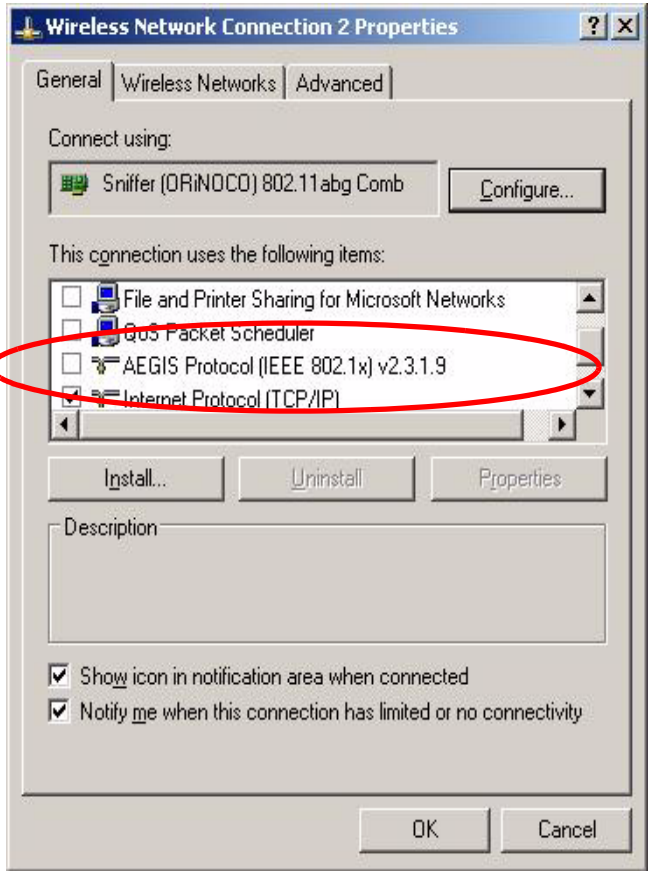


Figure 2-1. 802.11a/b/g Wireless Adapter Properties Dialog Box

Installing the ORiNOCO Gold Adapter / Driver 3

Overview

This chapter describes how to install the ORiNOCO Gold Card and drivers:

- *Installing the ORiNOCO Gold Adapter* for:
  - *Windows NT 4.0* on page 13
  - *Windows XP* on page 17
  - *Windows 2000* on page 19
- *Using the ORiNOCO Gold as a Normal Network Adapter* on page 22
- *ORiNOCO Gold Installation Notes and Issues* on page 23

Installing the ORiNOCO Gold Adapter

The following sections provide operating system-specific information for installing ORiNOCO Gold adapters and drivers.

Windows NT 4.0

This section describes how to install the ORiNOCO Gold adapter on a Windows NT 4.0 system.

To install the ORiNOCO Gold adapter and driver in Windows NT 4.0:

1. After installing the Sniffer software, remove any installed adapter drivers (either a previous version of the Sniffer driver or another vendor's driver) for the ORiNOCO Gold adapter from the **Adapters** tab of the **Network** control panel.
2. Restart the computer.
3. Log into Windows NT as an Administrator.
4. Insert the ORiNOCO Gold wireless adapter in an available Type II PC card slot on the target machine.
5. Locate an available I/O Port and interrupt number.

NOTE: In most cases, the default resources found by the driver will work. However, in some cases, you may need to identify free resources as described in the following steps.

a Select the **Windows NT Diagnostics** program from the **Administrative Tools (Common)** program group under the **Start** menu.

b In the dialog box that appears, click the **Resources** tab. The IRQs currently in use on the PC are listed by number.

c The ORiNOCO Gold adapter card can use IRQ 3 through 12 and 15. Determine if one of these IRQs is available and write down its number for later use.

NOTE: If IRQ 3 through 12 and 15 are already in use, make one available for the ORiNOCO Gold adapter by uninstalling a conflicting device.

d Click **I/O Port** at the bottom of the Windows NT Diagnostics window. The I/O Port windows currently in use on the PC are listed.

e The ORiNOCO Gold adapter card can use I/O base addresses from 0180 to F000. Determine if one of these I/O base addresses is available and write down its number for later use.

NOTE: If I/O base addresses from 0180 to F000 are already in use, make one available for the ORiNOCO Gold adapter by uninstalling a conflicting device.

6 Install the driver provided by Network General for the ORiNOCO Gold adapter:

a Start the Windows **Network** control panel by right-clicking **Network Neighborhood** and selecting **Properties**.

b Click the **Adapters** tab of the **Network** control panel.

c In the **Adapters** tab, click **Add**.

d Click **Have Disk** in the Select Network Adapter dialog box.

e In the Insert Disk dialog box, supply the path to the AgereOrinoco\WinNT subdirectory where the driver files are installed and click **OK**.

NOTE: The location for Sniffer Portable drivers is *C:\Program Files\NAI\SnifferNT\Driver\en\AgereOrinoco\WinNT.*

f The Select OEM Option dialog box appears with the **ORiNOCO PC Card** entry highlighted. Click **OK**.

The Add/Edit Configuration Profile dialog box appears (Figure 3-1).

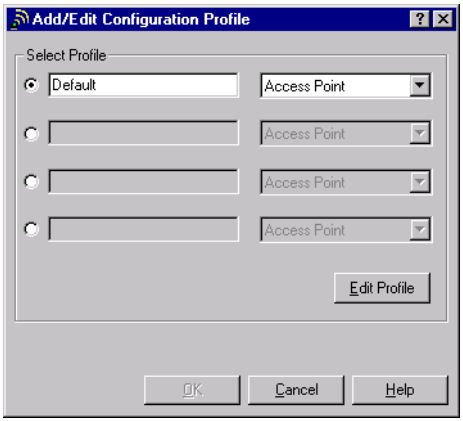


Figure 3-1. The Add/Edit Configuration Profile Dialog Box

g Make sure the Default profile is selected, leave the adjacent drop-down field set to its default value of **Access Point** (as in Figure 3-1), and click **Edit Profile**.

NOTE: The **OK** button in the Add/Edit Configuration Profile dialog box is not available until you click **Edit Profile**.

h In the Edit Configuration dialog box, click the **Adapter** tab and set the **I/O Base Address** and **Interrupt** options to the same values you recorded for the ORiNOCO Gold adapter in Step 5 on page 13.

NOTE: Occasionally, Windows NT may have some difficulty installing the wireless adapter's driver even after allocating free resources. If this happens, try changing some of the resource settings for the card (I/O Base Address or Interrupt) to other free resources.

i After configuring the **Default** profile for the ORiNOCO Gold adapter, click **OK**.

j At this point, you can add or edit other profiles to use the ORiNOCO Gold adapter. For example, if you want to use the ORiNOCO Gold adapter for normal wireless LAN operations (in addition to its default role for network analysis with the Sniffer software), you could create another profile here with configuration information to match your wireless network (ESSID, WEP keys, and so on; see your ORiNOCO Gold documentation for details).

k When you have finished adding and editing profile information, click **OK** in the Add/Edit Configuration Profile dialog box.

The Wizard installs the selected driver. You may see the error message shown in Figure 3-2 if the ORiNOCO Client Manager software is not installed. You can safely ignore this message. The Client Manager can be installed later.

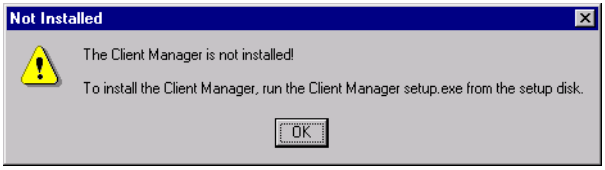


Figure 3-2. ORiNOCO Client Manager Warning

l Click **Close** on the Network Control Panel. The system installs the card according to your settings and updates the bindings.

m When installation finishes, the system will prompt you to configure the TCP/IP properties for the ORiNOCO Gold adapter (if TCP/IP is bound to it).

Binding TCP/IP to the ORiNOCO Gold adapter is not required for the Sniffer software. However, to use the ORiNOCO Gold adapter for normal wireless LAN operations, you must set the TCP/IP properties to match your network. Click **OK** when you have finished.

n Click **Yes** to restart the computer when prompted.

7 Verify that the updated driver is installed correctly by examining its entry in the **Adapters** tab of the Network control panel:

a Start the Windows **Network** control panel by right-clicking **Network Neighborhood** and selecting **Properties**.

b Click the **Adapters** tab of the **Network** control panel.

c In the **Adapters** tab, verify that the driver for the wireless adapter appears in the following format:.

Sniffer (*vendor name*) - *card description*

If the driver for the wireless adapter does not appear in this format, repeat the driver installation.

8 At this point, the ORiNOCO Gold wireless adapter should be installed with the Network General driver in Windows NT. Turn to *Creating Local Agents for Wireless LAN Adapters* on page 79 to create a new local agent in the Sniffer software to use the adapter.

Windows XP

This section describes how to install the ORiNOCO Gold adapter and driver on a Windows XP system.

To install the ORiNOCO Gold adapter and driver in Windows XP:

1 After installing the Sniffer software, log into Windows XP as an Administrator.

2 Insert the ORiNOCO Gold adapter in an available Type II PC card slot on the target machine. Windows XP will automatically detect the new card and install its native device driver.

3 Open the Network Connections folder through **Start > Control Panel > Network Connections**.

4 Right-click the Wireless Network Connection entry associated with the ORiNOCO Gold adapter and select **Properties**.

5 Click **Configure** in the Wireless Network Connections Properties dialog box to open the Adapter Properties dialog box for the ORiNOCO Gold adapter.

6 Click the **Driver** tab (Figure 3-3).

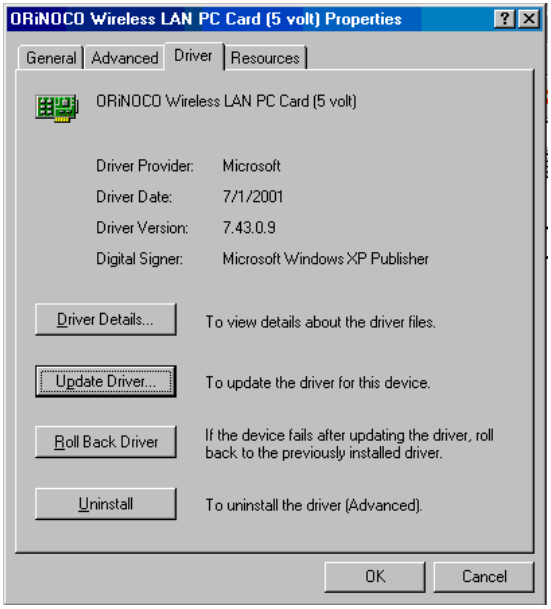


Figure 3-3. Wireless Network Connection Properties Dialog Box

7 Click **Update Driver** to open the Hardware Update Wizard.

8 Select **Install from a list or specific location (Advanced)** and click **Next**.

9 Select the **Don't search** option and click **Next**.

10 Click **Have Disk**.

11 In the Install from Disk dialog box, click **Browse** and navigate to the AgereOrinoco\ WinXP subdirectory where the driver files for the ORiNOCO Gold adapter are installed.

NOTE: The location for Sniffer Portable drivers is *C:\Program Files\NAI\SnifferNT\Driver\en\AgereOrinoco\WinXP.*

---

12 Click **OK** back in the Install from Disk dialog box.

13 If the operating system is configured to alert you to unsigned drivers, a dialog box will appear warning you that you are about to install a driver that has not been verified by Microsoft Corporation. Click **Continue Anyway** to continue the installation.

14 Click **Finish** to complete the installation.

15 Click **OK** in the Adapter Properties dialog box.

16 For Sniffer Portable users: If you did not uninstall the QoS Packet Scheduler Service during the installation of the Sniffer Portable software, you should disable it for this adapter now. See the *Sniffer Portable Installation Guide* for detailed information.

17 Create a new local agent in to use the adapter. See *Creating a Local Agent to Use the Wireless LAN Adapter* on page 79.

Windows 2000

This section describes how to install the ORiNOCO Gold adapter and driver on a Windows 2000 system. The procedure is somewhat different whether you are updating an existing driver for the wireless adapter (either a previous version of the Sniffer driver or another vendor's driver) or installing the adapter and driver for the first time. Use the appropriate procedure below.

- *First Time Installation* on page 19
- *Updating Existing Drivers* on page 20

First Time Installation

For Windows 2000, install the adapter for the first time by inserting the card in the PC and using the Found New Hardware Wizard.

To install the ORiNOCO Gold adapter and driver in Windows 2000 for the first time:

1 After installing the Sniffer software, log into Windows 2000 as an Administrator.

2 Insert the ORiNOCO Gold wireless adapter in an available Type II PC card slot on the target machine.

3 Windows 2000 presents a Wizard to help you install a new driver for the ORiNOCO Gold adapter. Click **Next**.

NOTE: If Windows 2000's plug-and-play feature automatically installs a driver for the adapter instead of starting the Found New Hardware Wizard, turn to *Updating Existing Drivers* on page 20 to update the existing driver.

4 In the Install Hardware Device Drivers window, select the **Search for a suitable driver for my device** option and click **Next**.

5 In the Locate Driver Files window, check only the **Specify a location** option and click **Next**.

6 When prompted, click **Browse**, navigate to the AgereOrinoco\WinXP subdirectory where the driver files are installed, and click **Open**.

NOTE: The location for Sniffer Portable drivers is *C:\Program Files\NAI\SnifferNT\Driver\en\AgereOrinoco\Win2K.*

---

7 Click **OK**.

8 Windows 2000 scans for the driver and presents the Driver Files Search Results window. Click **Next** in the Driver Files Search Results window when the specified driver is found.

9 Click **Yes** on the Digital Signature Not Found warning to continue the installation.

10 When the Add/Edit Configuration Profile dialog box appears, the installation procedure is the same as the *Updating Existing Drivers* procedure. Continue with Step 14 on page 21.

Updating Existing Drivers

For Windows 2000, update existing drivers using the Device Manager. The procedure is the same regardless of whether you are updating the vendor's existing driver or a previous version of the Sniffer driver.

To update existing drivers for the ORiNOCO Gold adapter in Windows 2000:

1 After installing the Sniffer software, log into Windows 2000 as an Administrator.

2 Start the Device Manager:

- **a** Right-click the **My Computer** icon and select **Properties**.
- **b** Click the **Hardware** tab, then click **Device Manager**.
- **c** Expand the **Network Adapters** entry by clicking the **+** sign.

3 Right-click the entry for the ORiNOCO Gold adapter and select **Properties**.

4 Click the **Driver** tab, then click **Update Driver**.

5 Click **Next** when the Welcome to the Upgrade Device Driver Wizard appears.

6 Select the **Display a list of the known drivers for this device so that I can choose a specific driver** option and click **Next**.

7 In the dialog box that appears, click **Have Disk**.

8 When prompted, click **Browse** and navigate to the AgereOrinoco\Win2k subdirectory where the driver files are installed.

NOTE: The default Sniffer Portable location for all drivers: *C:\Program Files\NAI\SnifferNT\Driver\en*

---

9 Click **Open** in the Locate File dialog box.

10 Click **OK** in the Install from Disk dialog box.

11 Windows scans for the driver and presents a dialog box listing different cards supported by the specified driver. Select the entry corresponding to your card and click **Next**. For the ORiNOCO Gold adapter, select the **5V** option if not selected automatically.

12 Click **Next** to begin installing the driver.

13 Click **Yes** on the Digital Signature Not Found warning to continue the installation.

14 In the Add/Edit Configuration Profile dialog box, specify settings for the ORiNOCO Gold adapter when used as a normal wireless LAN adapter (ESSID, WEP keys, and so on; see your ORiNOCO Gold documentation for details). The settings in this dialog box do not affect the adapter when used in promiscuous mode by the Sniffer software.

- If you will only use the ORiNOCO Gold adapter for the Sniffer software, simply leave the **Default** profile selected and the adjacent drop-down box set to **Access Point**.
- If you will use the ORiNOCO Gold adapter as a normal wireless LAN adapter in addition to its network analysis role with the Sniffer software, click **Edit Profile** to open a dialog box in which you can add or edit other profiles to use the ORiNOCO Gold adapter.

15 After adding and editing profile information, click **OK**.

The Wizard installs the selected driver. During installation, you may see the error message shown in Figure 3-4 if the ORiNOCO Client Manager software is not installed. You can safely ignore this message and install the Client Manager later.

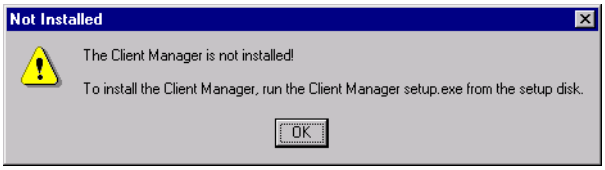


Figure 3-4. ORiNOCO Client Manager Warning

16 Click **Finish** to finish the driver installation and restart the computer.

17 Verify that the correct driver is installed by examining its **Device Name** entry in the Network and Dial-Up Connections window:

   a Right-click **My Network Places** and select **Properties**.

   b Select the entry in the Network and Dial-Up Connections window for the wireless adapter and verify that the entry in the Device Name column appears in the following format:

   Sniffer (*vendor name*) - *card description*

   If the driver for the wireless adapter does not appear in this format, you will need to repeat the installation procedure to install the driver.

18 At this point, the ORiNOCO Gold wireless adapter should be installed with the Network General driver in Windows 2000. Turn to *Creating Local Agents for Wireless LAN Adapters* on page 79 to create a new local agent in the Sniffer software to use the adapter.

Using the ORiNOCO Gold as a Normal Network Adapter

When the Sniffer software is connected to the ORiNOCO Gold wireless adapter, the card operates in promiscuous mode and cannot participate as an active member of the wireless LAN. However, when the Sniffer software is not connected to the ORiNOCO Gold adapter, you can use the adapter to participate actively in a wireless network.

During a normal installation of the ORiNOCO Gold wireless adapter, you are given the option of configuring a profile for normal wireless network participation (including configuring the ESSID, WEP keys, and so on). If you did not configure these settings during the initial installation of the adapter (or if you want to change the current settings), you can configure them later in either of the following ways. However, do **not** make changes to the ORiNOCO Gold adapter's configuration while the Sniffer software is running.

- Using the **Wireless Network** option in the Control Panel.

- Using the wireless adapter's vendor-supplied configuration utility.

See the ORiNOCO Gold documentation for details.

NOTE: For Windows XP, use the **Wireless Network** tab in the Wireless Network Connection Properties dialog box to set wireless network participation parameters.

ORiNOCO Gold Installation Notes and Issues

Keep the following notes and tips in mind when working with the ORiNOCO Gold wireless adapter:

- After exiting the Sniffer software, it may take up to a minute for the wireless adapter to transition to normal wireless network participation.
- Do not use the client utility provided with the ORiNOCO Gold adapter while the Sniffer software is running.
- If the machine has multiple card slots, you can prevent potential problems by always using the wireless adapter in the same slot.
- While configuring the ORiNOCO Gold adapter, you may see the following warning: *Can not access your wireless card. Please remove and reinsert PC card to activate settings.*

  This warning can safely be ignored.

Installing the Enterasys Adapter / Driver 4

Overview

This chapter describes how to install the Enterasys RoamAbout adapter card and driver for the Sniffer software. This chapter includes the following sections:

- *Installing the Enterasys RoamAbout Adapter* for:
  - *Windows NT 4.0* on page 25
  - *Windows XP* on page 30
  - *Windows 2000* on page 31
- *Using the Enterasys RoamAbout as a Normal Network Adapter* on page 35
- *Enterasys RoamAbout Installation Notes and Issues* on page 36

Installing the Enterasys RoamAbout Adapter

The following sections provide operating system-specific information for installing Enterasys RoamAbout Adapters and drivers.

Windows NT 4.0

This section describes how to install the Enterasys RoamAbout adapter on a Windows NT 4.0 system.

To install the Enterasys RoamAbout adapter and driver in Windows NT 4.0:

1. Ensure the Sniffer software is properly installed.
2. Remove any installed adapter drivers (either a previous version of the Sniffer driver or another vendor's driver) for the Enterasys RoamAbout adapter. Remove drivers in Windows NT from the **Adapters** tab of the **Network** control panel.
3. Restart the computer.
4. Log in to Windows NT as an Administrator.

5 Insert the Enterasys RoamAbout wireless adapter in an available Type II PC card slot on the target machine.

6 Locate an available I/O Port and interrupt number:

NOTE: In most cases, the default resources found by the driver will work. However, in some cases, you may need to identify free resources as described in this step.

a Go to **Start** > **Administrative Tools (Common)** > **Windows NT Diagnostics**.

b Click the **Resources** tab. The IRQs currently in use on the PC are listed by number (Figure 4-1).

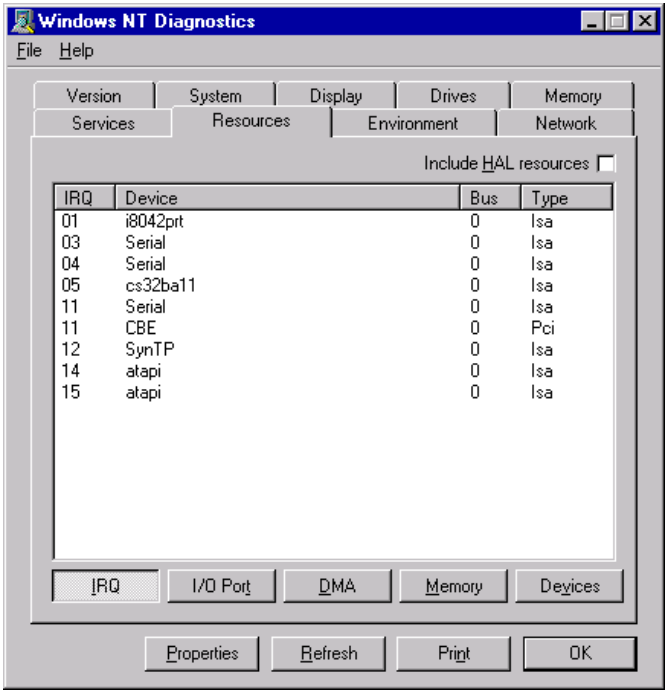


Figure 4-1. Finding Available Resources for the Enterasys RoamAbout Wireless LAN Adapter

c The Enterasys RoamAbout adapter card can use IRQ 3 through 12 and 15. Determine if one of these IRQs is available and write down its number for later use.

NOTE: If the IRQs are already in use, make one available for the

Enterasys RoamAbout adapter by uninstalling a conflicting device.

d Click **I/O Port**.

e The I/O Port windows currently in use on the PC are listed. The Enterasys RoamAbout adapter card can use I/O base addresses from 0180 to F000. Determine if one of these I/O base addresses is available and write down its number for later use.

NOTE: If the I/O base addresses are already in use, make one available for the Enterasys RoamAbout adapter by uninstalling a conflicting device.

7 Install the driver provided by Network General for the Enterasys RoamAbout adapter:

a Start the Windows **Network** control panel by right-clicking **Network Neighborhood** and selecting **Properties**.

b Click the **Adapters** tab.

c Click **Add**.

d The Select Network Adapter dialog box appears. Click **Have Disk**.

e Supply the path to the EnterasysRoamAbout\WinNT subdirectory where the driver files are installed and click **OK**.

NOTE: *The location for Sniffer Portable drivers is C:\Program Files\NAI\SnifferNT\Driver\en\EnterasysRoamAbout\WinNT.*

f The Select OEM Option dialog box appears with the **Sniffer (RoamAbout) 802.11 PC Card** entry highlighted. Click **OK**.

g Make sure the Default profile is selected, then click **Edit Profile** in the Add/Edit Configuration Profile dialog box.

NOTE: Leave the adjacent drop-down field set to its default value of **Access Point** (as shown in Figure 4-2).

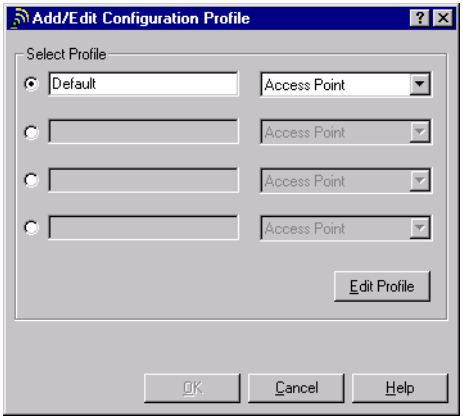


Figure 4-2. The Add/Edit Configuration Profile Dialog Box

NOTE: Click **Edit Profile** to enable the **OK** button in the Add/Edit Configuration Profile dialog box.

h Select the **Adapter** tab in the Edit Configuration dialog box and set the **I/O Base Address** and **Interrupt** options to the same values you recorded for the Enterasys RoamAbout adapter in Step 6 on page 26.

NOTE: Occasionally, Windows NT may have some difficulty installing the wireless adapter's driver even after allocating free resources. If this happens, try changing some of the resource settings for the card (I/O Base Address or Interrupt) to other free resources.

i When you have finished configuring the **Default** profile for the Enterasys RoamAbout adapter in the Edit Configuration dialog box, click **OK** to return to the Add/Edit Configuration dialog box.

j At this point, you can add or edit other profiles to use the Enterasys RoamAbout adapter. For example, if you want to use the Enterasys RoamAbout adapter for normal wireless LAN operations (in addition to its default role for network analysis with the Sniffer software), you could create another profile here with configuration information to match your wireless network (ESSID, WEP keys, and so on; see your Enterasys RoamAbout documentation for details).

k When you have finished adding and editing profile information, click **OK** in the Add/Edit Configuration Profile dialog box.

The Wizard installs the selected driver. During installation, you may see the error message shown in Figure 4-3 if the Client Manager software is not installed. You can safely ignore this message. The Client Manager can be installed later.

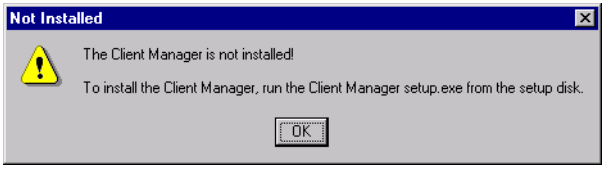


Figure 4-3. Client Manager Warning

l Click **Close** on the Network control panel.

The system installs the card according to your settings and updates the bindings.

m When installation finishes, the system prompts you to configure the TCP/IP properties for the Enterasys RoamAbout adapter (if TCP/IP is bound to it).

Binding TCP/IP to the Enterasys RoamAbout adapter is not required for the Sniffer software. However, to use the Enterasys RoamAbout adapter for normal wireless LAN operations, you must set the TCP/IP properties to match your network. Click **OK** when you have finished.

n Click **Yes** to restart the computer when prompted.

8 Verify that the correct driver is installed by examining its entry in the **Adapters** tab of the Network control panel:

a Start the Windows **Network** control panel by right-clicking **Network Neighborhood** and selecting **Properties**.

b Click the **Adapters** tab.

c In the **Adapters** tab, verify that the driver for the wireless adapter appears in the following format:.

Sniffer (*vendor name*) - *card description*

If the driver for the wireless adapter does not appear in this format, you will need to repeat the installation procedure to install the driver.

9 At this point, the Enterasys RoamAbout wireless adapter should be installed with the Network General driver in Windows NT. Turn to *Creating Local Agents for Wireless LAN Adapters* on page 79 to create a new local agent in the Sniffer software to use the adapter.

Windows XP

This section describes how to install the Enterasys RoamAbout adapter and driver on a Windows XP system.

To install the Enterasys RoamAbout adapter and driver in Windows XP:

1. Ensure the Sniffer software is properly installed.
2. Log into Windows XP as an Administrator.
3. Insert the Enterasys RoamAbout adapter in an available Type II PC card slot on the target machine.

   Windows XP automatically detects the new card and installs its native device driver.
4. Open the Network Connections folder by selecting the **Start > Control Panel > Network Connections** option.
5. Right-click the Wireless Network Connection entry associated with the Enterasys RoamAbout adapter and select **Properties**.

   The Wireless Network Connections Properties dialog box appears.
6. Click **Configure**.

   The Adapter Properties dialog box for the Enterasys RoamAbout adapter appears.
7. Click the **Driver** tab.
8. Click **Update Driver**.

   The Hardware Update Wizard starts.
9. Select the **Install from a list or specific location (Advanced)** option. and click **Next**.
10. Select the **Don't search** option and click **Next.**
11. Click **Have Disk**.

    The Install from Disk dialog box appears prompting you to supply the path to the driver to install.
12. Click **Browse** and navigate to the EnterasysRoamAbout\WinXP subdirectory where the driver files are installed.

NOTE: *The location for Sniffer Portable drivers is C:\Program Files\NAI\SnifferNT\Driver\en\EnterasysRoamAbout\WinXP.*

13 Click **Open** in the Browse dialog box.

You are returned to the Install from Disk dialog box.

14 Click **OK** in the Install from Disk dialog box.

If the operating system is configured to alert you to unsigned drivers, a dialog box will appear warning you that you are about to install a driver that has not been verified by Microsoft Corporation.

15 Click **Continue Anyway** to continue the installation.

The wizard installs the driver. When it has finished, it displays a screen indicating that the driver is installed.

16 Click **Finish** to complete the installation.

17 Click **OK** to clear the Adapter Properties dialog box.

18 For Sniffer Portable users: If you did not uninstall the QoS Packet Scheduler Service during the Sniffer Portable installation, you should disable it for this adapter now. See the *Sniffer Portable Installation Guide* for details.

19 Then, turn to *Creating Local Agents for Wireless LAN Adapters* on page 79 to create a new local agent in the Sniffer software to use the adapter.

Windows 2000

This section describes how to install the Enterasys RoamAbout adapter and driver on a Windows 2000 system. The procedure is somewhat different depending on whether you are updating an existing driver for the wireless adapter (either a previous version of the Sniffer driver or another vendor's driver) or installing the adapter and driver for the first time. Use the appropriate procedure below.

- *First Time Installation* on page 32
- *Updating Existing Drivers* on page 33

First Time Installation

For Windows 2000, you install an adapter for the first time by inserting the card in the PC and using the Found New Hardware Wizard.

To install the Enterasys RoamAbout adapter and driver in Windows 2000 for the first time:

1. Ensure the Sniffer software is properly installed.
2. Log into Windows 2000 as an Administrator.
3. Insert the Enterasys RoamAbout wireless adapter in an available Type II PC card slot on the target machine.

   Windows 2000 presents a Wizard to help you install a new driver for the Enterasys RoamAbout adapter.

   NOTE: If Windows 2000's plug-and-play feature automatically installs a driver for the adapter instead of starting the Found New Hardware Wizard, turn to *Updating Existing Drivers* on page 33 to update the existing driver.

4. Click **Next**.

   The Install Hardware Device Drivers window appears.

5. Select the **Search for a suitable driver for my device** option and click **Next**.

   The Locate Driver Files window appears.

6. Check only the **Specify a location** option and click **Next**.
7. Click **Browse**, navigate to the EnterasysRoamAbout\Win2K subdirectory where the driver files are installed, and click **Open**:

   NOTE: The default Sniffer Portable location for all drivers: *C:\Program Files\NAI\SnifferNT\Driver\en*

8. Click **OK**.
9. Click **OK** in the Install from Disk dialog box.

   Windows 2000 scans for the driver and presents the Driver Files Search Results window indicating that it has found the driver you specified in the previous step.

10. Click **Next** on the Driver Files Search Results window.

The Digital Signature Not Found warning appears asking you if you want to continue the installation.

11 At this point, the rest of the installation procedure is the same as the **Update** procedure. Continue with Step 15 on page 34.

Updating Existing Drivers

For Windows 2000, you update an existing driver using the Device Manager. The procedure is the same regardless of whether you are updating the vendor's existing driver or a previous version of the Sniffer driver.

To update an existing driver for the Enterasys RoamAbout adapter in Windows 2000:

1 Ensure the Sniffer software is properly installed.

2 Log into Windows 2000 as an Administrator.

3 Start the Device Manager:

- **a** Right-click **My Computer** and select **Properties**.
- **b** Click the **Hardware** tab.
- **c** Click **Device Manager**.
- **d** Expand the **Network Adapters** entry by clicking the **+** sign adjacent to its entry.

4 Right-click the entry for the Enterasys RoamAbout adapter and select **Properties**.

5 Click the **Driver** tab.

6 Click **Update Driver**.

7 Click **Next**.

8 Select **Display a list of the known drivers for this device so that I can choose a specific driver** and click **Next**.

9 Click **Have Disk**.

10 Click **Browse** and navigate to the EnterasysRoamAbout\Win2K subdirectory where the driver files are installed.

NOTE: *The location for Sniffer Portable drivers is C:\Program Files\NAI\SnifferNT\Driver\en\EnterasysRoamAbout\Win2K.*

---

11 Click **Open** in the Locate File dialog box.

12 Click **OK** in the Install from Disk dialog box.

Windows scans for the driver and presents a dialog box listing different cards supported by the specified driver.

13 Select the entry corresponding to your card and click **Next**.

14 The Upgrade Device Wizard indicates that it is ready to install the selected driver. Click **Next** to begin installing the driver.

The Digital Signature Not Found warning appears asking you if you want to continue the installation.

15 Click **Yes** on the Digital Signature Not Found warning to continue the installation.

When driver installation has finished, the Wizard presents the Completing the Found New Hardware Wizard window.

16 Click **Finish** to finish the installation.

17 Restart the computer.

18 Verify that the correct driver is installed by examining its **Device Name** entry in the Network and Dial-Up Connections window:

a Right-click **My Network Places** and select **Properties**.

b Select the entry in the Network and Dial-Up Connections window for the wireless adapter and verify that the entry in the Device Name column appears in the following format:

Sniffer (*vendor name*) - *card description*

If the driver for the wireless adapter does not appear in this format, you will need to repeat the installation procedure to install the driver.

19 At this point, the Enterasys RoamAbout wireless adapter should be installed with the Network General driver in Windows 2000. Turn to *Creating Local Agents for Wireless LAN Adapters* on page 79 to create a new local agent in the Sniffer software to use the adapter.

Using the Enterasys RoamAbout as a Normal Network Adapter

When the Sniffer software is connected to the Enterasys RoamAbout wireless adapter, the card operates in promiscuous mode and cannot participate as an active member of the wireless LAN. However, when the Sniffer software is not connected to the Enterasys RoamAbout, you can use the adapter to participate actively in a wireless network.

During a normal installation of the Enterasys RoamAbout wireless adapter, you are given the option of configuring a profile for normal wireless network participation (including configuring the ESSID, WEP keys, and so on). If you did not configure these settings during the initial installation of the adapter (or if you are a Windows 2000 user), you can configure them later in either of the following ways. However, do not make changes to the Enterasys RoamAbout's configuration while the Sniffer software is running.

- Using the **Wireless Network** option in the Control Panel.
- Using the wireless adapter's vendor-supplied configuration utility.

See the Enterasys RoamAbout documentation for details.

NOTE: For Windows XP, use the **Wireless Network** tab in the Wireless Network Connection Properties dialog box to set wireless network participation parameters.

Enterasys RoamAbout Installation Notes and Issues

Keep the following notes and tips in mind when working with the Enterasys RoamAbout wireless adapter:

- After exiting the Sniffer software, it may take up to a minute for the wireless adapter to transition to normal wireless network participation.
- Do not use the client utility provided with the Enterasys RoamAbout while the Sniffer software is running.
- If the machine in which the Sniffer software is installed has multiple card slots, you can prevent potential problems by always using the wireless adapter in the same slot.
- While configuring the Enterasys RoamAbout adapter, you may see the following warning: *Can not access your wireless card. Please remove and reinsert PC card to activate settings.*

  This warning can safely be ignored.

Installing the Spectrum 24 Adapter / Driver 5

Overview

This chapter describes how to install the Spectrum 24 Model 4121 adapter card and driver for the Sniffer software:

- *Installing the Spectrum 24 Model 4121 in Windows NT 4.0* on page 37
- *Installing the Spectrum 24 Model 4121 Adapter in Windows XP* on page 43
- *Installing the Spectrum 24 Model 4121 in Windows 2000* on page 45
- *Using the Spectrum 24 as a Normal Network Adapter* on page 50
- *Spectrum 24 Installation Notes and Issues* on page 51

Installing the Spectrum 24 Model 4121 in Windows NT 4.0

This section describes how to install the Spectrum 24 adapter and driver on a Windows NT 4.0 system.

To install the Spectrum 24 adapter and driver in Windows NT 4.0:

1. After installing the Sniffer software, remove any installed adapter drivers (either a previous version of the Sniffer driver or another vendor's driver) for the Spectrum 24 adapter. Remove drivers in Windows NT from the **Adapters** tab of the **Network** control panel.
2. Restart the computer.
3. Log in to Windows NT as an Administrator.
4. Insert the Spectrum 24 wireless adapter in an available Type II PC card slot on the target machine.
5. Locate an available IRQ and IO Base Address:
    a. Select the **Windows NT Diagnostics** program from the **Administrative Tools (Common)** program group under the **Start** menu.

b In the dialog box that appears, click the **Resources** tab. The IRQs currently in use on the PC are listed by number.

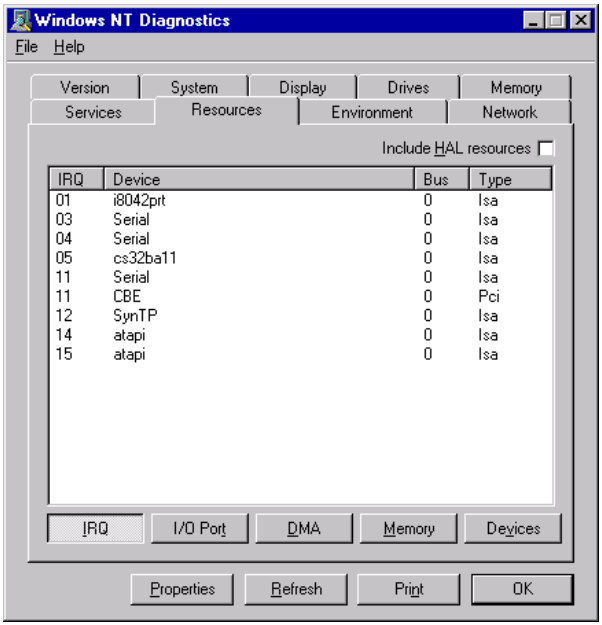


Figure 5-1. Finding Available Resources for the Spectrum 24 Wireless LAN Adapter

c The Spectrum 24 card can use IRQs 2 through 15. Determine if one of these IRQs is available and write down its number for later use.

NOTE: If all of these IRQs are already in use, you will need to make one of them available for the Spectrum 24 adapter by uninstalling a conflicting device.

---

d Click **I/O Port** at the bottom of the **Windows NT Diagnostics** window (Figure 5-1). The I/O Port windows currently in use on the PC are listed.

e Find an available I/O Port and write down its number for later use.

f Click **Memory** at the bottom of the Windows NT Diagnostics window (Figure 5-1). The Memory Base Addresses currently in use on the PC are listed.

g Find an available Memory Base Address and write down its number for later use.

6 Next, install the driver provided by Network General for the Spectrum 24 adapter:

a Start the MS-Windows **Network** control panel by right-clicking on the Network Neighborhood icon on the desktop and selecting the **Properties** command from the menu that appears.

b Click the **Adapters** tab of the **Network** control panel.

c In the **Adapters** tab, click **Add**.

d The Select Network Adapter dialog box appears. Click **Have Disk**.

e In the Insert Disk dialog box, supply the path to the SymbolSpectrum24HR\WinNT subdirectory where the driver files are installed and click **OK**.

NOTE: *The location for Sniffer Portable drivers is C:\Program Files\NAI\SnifferNT\Driver\en\SymbolSpectrum24HR\WinNT.*

---

f In the Select OEM Option dialog box, select the **Symbol LA-41x1 Spectrum24 Wireless LAN PC Card** option and click **OK**.

The Symbol Spectrum24 WLAN Easy Setup dialog box appears (Figure 5-2).

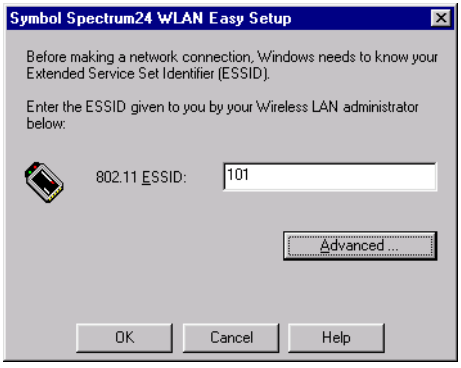


Figure 5-2. The Symbol Spectrum24 WLAN Easy Setup Dialog Box

g Click **Advanced**.

The Symbol Spectrum24 WLAN Advanced Properties dialog box appears.

h Click the **WLAN Adapter** tab.

The Symbol Spectrum24 WLAN Advanced Properties dialog box appears as in Figure 5-3.

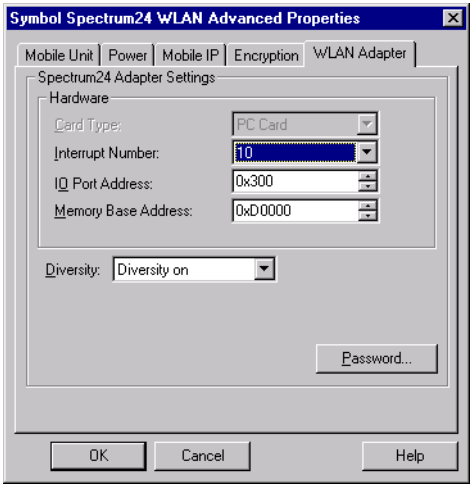


Figure 5-3. The WLAN Adapter Tab

i Set the **Interrupt Number**, **IO Port Address**, and **Memory Base Address** options to the same values you recorded for the Spectrum 24 adapter in Step 5 on page 37 and click **OK**.

NOTE: Occasionally, Windows NT may have some difficulty installing the wireless adapter's driver even after allocating free resources. If this happens, try changing some of the resource settings for the card (IRQ, I/O Port, or Memory address) to other free resources.

---

j The other tabs in the Symbol Spectrum24 WLAN Advanced Properties dialog box let you specify settings for the Spectrum 24 adapter when used as a normal wireless LAN adapter (ESSID, WEP keys, and so on; see your Symbol Spectrum documentation for details). The settings in this dialog box do not affect the adapter when used in promiscuous mode by the Sniffer software.

- If you will only use the Spectrum 24 adapter for the Sniffer software, you do not need to make any other changes in this dialog box.

- If you will use the Spectrum 24 adapter as a normal wireless LAN adapter (in addition to its network analysis role), use the provided tabs to specify configuration information for the Spectrum 24 adapter when used as a normal wireless adapter (see your Symbol Spectrum documentation for details).

k When you have finished configuring the options in the Symbol Spectrum24 WLAN Advanced Properties dialog box, click **OK**.

l Click **OK** in the Symbol Spectrum24 WLAN Easy Setup dialog box.

m Click **Close** on the **Network** control panel.

The system installs the card according to your settings and updates the bindings.

n When installation finishes, the system prompts you to configure the TCP/IP properties for the Spectrum 24 adapter (if TCP/IP is bound to it).

Binding TCP/IP to the Spectrum 24 adapter is not required for the Sniffer software. However, to use the Spectrum 24 adapter for normal wireless LAN operations, you must set the TCP/IP properties to match your network. Click **OK** when you have finished.

o The system prompts you to restart the computer. Click **Yes** to restart the computer.

7 Verify that the correct driver is installed correctly by examining its entry in the **Adapters** tab of the Network control panel:

a Start the MS-Windows **Network** control panel by right-clicking on the Network Neighborhood icon on the desktop and selecting the **Properties** command from the menu that appears.

b Click the **Adapters** tab of the **Network** control panel.

c In the **Adapters** tab, verify that the driver for the wireless adapter appears in the following format:.

Sniffer (*vendor name*) - *card description*

If the driver for the wireless adapter does not appear in this format, you will need to repeat the installation procedure to install the driver.

8 At this point, the Symbol Technologies Spectrum 24 wireless adapter should be installed with the Network General driver in Windows NT. See *Creating a Local Agent to Use the Wireless LAN Adapter* on page 79 to create a new local agent in the Sniffer software to use the adapter.

NOTE: If you are having difficulties installing the Spectrum 24 adapter, see *Troubleshooting Spectrum 24 Installation Issues in Windows NT* on page 42.

Troubleshooting Spectrum 24 Installation Issues in Windows NT

If you have performed the installation procedures in the previous section and are having difficulties getting the system to recognize the adapter because of IRQ, I/O Port, or Memory Base Address conflicts, you can try installing the Spectrum 24 with its native driver provided by Symbol Technologies to locate available hardware resources.

To install the Spectrum 24 with the native driver:

1. The Spectrum 24 wireless LAN adapter is provided by Symbol Technologies with its own driver and documentation. Install the Spectrum 24 adapter and driver in according to the Symbol Technologies documentation. Ensure that the card is working correctly before proceeding to the next step.
2. Once you have successfully installed the Spectrum 24 adapter with the native Symbol Technologies driver, write down the Memory Address, I/O Port, and Interrupt used by the Spectrum 24:
   a. Start the MS-Windows **Network** control panel by right-clicking on the Network Neighborhood icon on the desktop and selecting the **Properties** command from the menu that appears.
   b. Click the **Adapters** tab of the **Network** control panel.
   c. In the **Adapters** tab, select the entry for the Spectrum 24 adapter in the **Network Adapters** list and click **Properties**.

      A Properties window appears listing various properties for the Spectrum 24.
   d. Write down the values listed for **Memory Address**, **I/O Port**, and **Interrupt** in the Properties window.
   e. Click **Cancel** to close the Properties window, but leave the **Network** control panel open.
3. Remove the Symbol Technologies driver from the PC:
   a. The **Adapters** tab of the **Network** control panel should be open from the previous step. In the **Adapters** tab, select the entry for the Spectrum 24 adapter in the **Network Adapters** list and click **Remove**.
   b. The system prompts you to confirm your intention to remove the selected adapter. Click **Yes** to remove the Spectrum 24 adapter. Once the system has removed the adapter, it prompts you to restart the computer. Restart the computer.

4 Next, reinstall the Network General driver for the Spectrum 24 adapter as described in Step 6 on page 39. When you reach the step where you need to specify the IRQ, I/O Port, and Memory Base Address values in the **Spectrum 24 Adapter Properties** dialog box, specify the values you recorded in Step 2, above.

Installing the Spectrum 24 Model 4121 Adapter in Windows XP

This section describes how to install the Spectrum 24 adapter and driver on a Windows XP system.

To install the Spectrum 24 adapter and driver in Windows XP:

1 After installing the Sniffer software, log in to Windows XP as an Administrator.

2 Insert the Spectrum 24 adapter in an available Type II PC card slot on the target machine.

Windows XP automatically detects the new card and installs its native device driver.

3 Open the Network Connections folder by selecting the **Start > Control Panel > Network Connections** option.

4 Right-click the Wireless Network Connection entry associated with the Spectrum 24 adapter and select the **Properties** command from the menu that appears.

The Wireless Network Connections Properties dialog box appears.

5 Click **Configure**.

The Adapter Properties dialog box for the Spectrum 24 adapter appears.

6 Click the **Driver** tab.

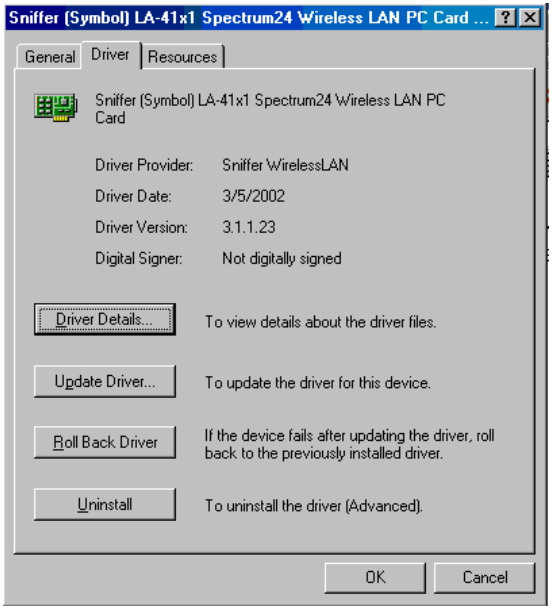


Figure 5-4. Wireless Network Connection Properties Dialog Box

7 Click **Update Driver**.

The Hardware Update Wizard starts.

8 Select the **Install from a list or specific location (Advanced)** option. and click **Next**.

9 Select the **Don't search** option and click **Next.**

10 Click **Have Disk**.

The Install from Disk dialog box appears prompting you to supply the path to the driver to install.

11 Click **Browse** and navigate to the SymbolSpectrum24HR\WinXP subdirectory where the driver files are installed.

NOTE: *The location for Sniffer Portable drivers is C:\Program Files\NAI\SnifferNT\Driver\en\SymbolSpectrum24HR\WinXP.*

---

12 Click **Open** on the Browse dialog box.

You are returned to the Install from Disk dialog box.

13 Click **OK** on the Install from Disk dialog box.

If the operating system is configured to alert you to unsigned drivers, a dialog box will appear warning you that you are about to install a driver that has not been verified by Microsoft Corporation.

14 Click **Continue Anyway** to continue the installation.

The wizard installs the driver. When it has finished, it displays a screen indicating that the driver is installed.

15 Click **Finish** to complete the installation.

You are returned to the Adapter Properties dialog box.

16 Click **OK** to clear the Adapter Properties dialog box.

17 For Sniffer Portable users: If you did not uninstall the QoS Packet Scheduler Service during the installation of the Sniffer Portable software, you should disable it for this adapter now. See the *Sniffer Portable Installation Guide* for more information.

18 See *Creating a Local Agent to Use the Wireless LAN Adapter* on page 79 to create a new local agent in the Sniffer software to use the adapter.

Installing the Spectrum 24 Model 4121 in Windows 2000

This section describes how to install the Spectrum 24 adapter and driver on a Windows 2000 system. The procedure is somewhat different depending on whether you are updating an existing driver for the wireless adapter (either a previous version of the Sniffer driver or another vendor's driver) or installing the adapter and driver for the first time. Use the appropriate procedure below.

- *First Time Installation* on page 45
- *Updating Existing Drivers* on page 47

First Time Installation

For Windows 2000, you install an adapter for the first time by inserting the card in the PC and using the Found New Hardware Wizard.

To install the Spectrum 24 adapter and driver in Windows 2000 for the first time:

1 After installing the Sniffer software, log in to Windows 2000 as an Administrator.

2 Insert the Spectrum 24 wireless adapter in an available Type II PC card slot on the target machine.

Windows 2000 presents a Wizard to help you install a new driver for the Spectrum 24 adapter.

NOTE: If Windows 2000's plug-and-play feature automatically installs a driver for the adapter instead of starting the Found New Hardware Wizard, turn to *Updating Existing Drivers* on page 47 to update the existing driver.

---

3 Click **Next** in the Wizard window.

The Install Hardware Device Drivers window appears.

4 Select the **Search for a suitable driver for my device** option and click **Next**.

The Locate Driver Files window appears.

5 Check only the **Specify a location** option and click **Next**.

The Found New Hardware Wizard prompts you to supply a path to the device driver.

6 Click **Browse**, navigate to the SymbolSpectrum24HR\Win2K subdirectory where the driver files are installed, and click **Open**.

NOTE: *The location for Sniffer Portable drivers is C:\Program Files\NAI\SnifferNT\Driver\en\SymbolSpectrum24HR\Win2K.*

---

7 Click **OK**.

Windows 2000 scans for the driver and presents the Driver Files Search Results window indicating that it has found the driver you specified in the previous step.

8 Click **Next** in the Driver Files Search Results window.

The Digital Signature Not Found warning appears asking you if you want to continue the installation.

9 Click **Yes** on the Digital Signature Not Found warning to continue the installation.

The Symbol Spectrum24 WLAN Easy Setup dialog box appears (Figure 5-5 on page 48).

10 At this point, the rest of the installation procedure is the same as the **Update** procedure. Continue with Step 15 on page 48.

Updating Existing Drivers

For Windows 2000, you update an existing driver using the Device Manager. The procedure is the same regardless of whether you are updating the vendor's existing driver or a previous version of the Sniffer driver.

To update an existing driver for the Spectrum 24 adapter in Windows 2000:

1. After installing the Sniffer software, log in to Windows 2000 as an Administrator.
2. Start the Device Manager:
   a. Right-click the **My Computer** icon and select the **Properties** command from the menu that appears.
   b. In the dialog box that appears, click the **Hardware** tab.
   c. Click **Device Manager**.
   d. Expand the **Network Adapters** entry by clicking the **+** sign adjacent to its entry.
3. Right-click the entry for the Spectrum 24 adapter and select the **Properties** command from the menu that appears.
4. Click the **Driver** tab in the dialog box that appears
5. Click **Update Driver**.

   The Upgrade Device Driver Wizard starts.
6. Click **Next** in the Welcome to the Upgrade Device Driver Wizard window.
7. Select the **Display a list of the known drivers for this device so that I can choose a specific driver** option and click **Next**.
8. In the dialog box that appears, click **Have Disk**.

   The Upgrade Device Driver Wizard prompts you to supply a path to the device driver.
9. Click **Browse** and navigate to the SymbolSpectrum24HR\Win2k subdirectory where the drivers are installed.

NOTE: The default Sniffer Portable location for all drivers: *C:\Program Files\NAI\SnifferNT\Driver\en*

10 Click **Open** in the Locate File dialog box.

11 Click **OK** in the Install from Disk dialog box.

Windows scans for the driver and presents a dialog box listing different cards supported by the specified driver.

12 Select the entry corresponding to your card and click **Next**.

13 The Upgrade Device Wizard indicates that it is ready to install the selected driver. Click **Next** to begin installing the driver.

The Digital Signature Not Found warning appears asking you if you want to continue the installation.

14 Click **Yes** on the Digital Signature Not Found warning to continue the installation.

The Symbol Spectrum24 WLAN Easy Setup dialog box opens.

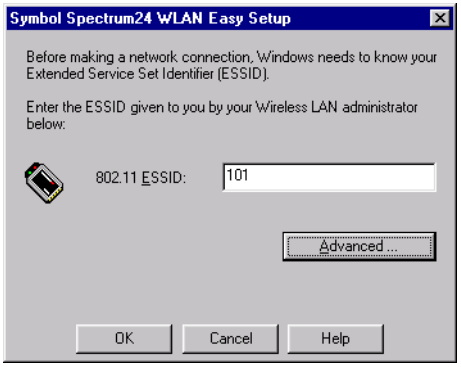


Figure 5-5. The Symbol Spectrum24 WLAN Easy Setup Dialog Box

15 The Symbol Spectrum24 WLAN Easy Setup dialog box lets you specify settings for the Spectrum 24 adapter when used as a normal wireless LAN adapter (ESSID, WEP keys, and so on; see your Symbol Spectrum documentation for details). The settings in this dialog box do not affect the adapter when used in promiscuous mode by the Sniffer software.

- If you will only use the Spectrum 24 adapter for the Sniffer software, you do not need to make any changes in this dialog box.

- If you will use the Spectrum 24 adapter as a normal wireless LAN adapter, click **Advanced** to open a dialog box in which you can specify configuration information for the Spectrum 24 adapter when used as a normal wireless adapter.

16 When you have finished configuring the options in the Symbol Spectrum24 WLAN Easy Setup dialog box, click **OK**.

The Wizard installs the selected driver. When it has finished, it presents the **Completing the Found New Wizard** window.

17 Click **Finish** to finish the installation.

18 Restart the computer.

19 Verify that the correct driver is installed correctly by examining its **Device Name** entry in the Network and Dial-Up Connections window:

a Right-click the **My Network Places** icon on the desktop and select **Properties**.

b Select the entry in the Network and Dial-Up Connections window for the wireless adapter and verify that the entry in the Device Name column appears in the following format:

Sniffer (*vendor name*) - *card description*

If the driver for the wireless adapter does not appear in this format, you will need to repeat the installation procedure to install the driver.

20 At this point, the Symbol Technologies Spectrum 24 wireless adapter should be installed with the Network General driver in Windows 2000. See *Creating a Local Agent to Use the Wireless LAN Adapter* on page 79 to create a new local agent in the Sniffer software to use the adapter.

Using the Spectrum 24 as a Normal Network Adapter

When the Sniffer software is connected to the Spectrum 24 wireless adapter, the card operates in promiscuous mode and cannot participate as an active member of the wireless LAN. However, when the Sniffer software is not connected to the Spectrum 24, you can use the adapter to participate actively in a wireless network.

During a normal installation of the Spectrum 24 wireless adapter on Windows NT, 2000, and 98 SE, you are given the option of configuring settings for normal wireless network participation (including configuring the ESSID, WEP keys, and so on). If you did not configure these settings during the initial installation of the adapter (or if you want to change the current settings), you can do so as described below:

NOTE: In addition to the methods described below, you can also change these settings using the wireless adapter's vendor-supplied configuration utility.

NOTE: Do not make changes to the Spectrum 24 configuration while the Sniffer software is running.

Windows NT

1. Start the MS-Windows **Network** control panel by right-clicking on the Network Neighborhood icon on the desktop and selecting the **Properties** command from the menu that appears.
2. Click the **Adapters** tab of the **Network** control panel.
3. In the **Adapters** tab, select the entry for the Symbol Spectrum 24 adapter and click **Properties**.
4. Use the dialog box that appears to set parameters for normal wireless network participation for the Spectrum 24.

Windows XP

1. Open the Network Connections folder by selecting the **Start > Control Panel > Network Connections** option.
2. Right-click the Wireless Network Connection entry associated with the Symbol Spectrum 24 adapter and select the **Properties** command from the menu that appears.

   The Wireless Network Connections Properties dialog box appears.
3. Click the **Wireless Networks** tab and use the options that appear to set parameters for normal wireless network participation.

Windows 2000

1. Start the Device Manager:
   a. Right-click the **My Computer** icon and select **Properties**.
   b. In the dialog box that appears, click the **Hardware** tab.
   c. Click **Device Manager**.
2. Right-click the entry for the Symbol Spectrum 24 adapter and select the **Properties** command from the menu that appears.
3. Click the **Spectrum24** tab in the dialog box that appears
4. Use the options in the **Spectrum24** tab to set parameters for normal wireless network participation for the Spectrum 24.

See the Symbol Spectrum 24 documentation for details on working with these configuration options.

Spectrum 24 Installation Notes and Issues

Keep the following notes and tips in mind when working with the Spectrum 24 wireless adapter:

- After exiting the Sniffer software, it may take up to a minute for the wireless adapter to transition to normal wireless network participation.
- Do not use the client utility provided with the Spectrum 24 while the Sniffer software is running.
- If the machine in which the Sniffer software is installed has multiple card slots, you can prevent potential problems by always using the wireless adapter in the same slot.

Installing the Cisco Aironet Adapter / Driver 6

Overview

This chapter describes how to install the Cisco Aironet 340/350 adapter card and driver for the Sniffer software.

- *Installing the Cisco Aironet in Windows NT 4.0* on page 53
- *Installing the Cisco Aironet in Windows XP* on page 58
- *Installing the Cisco Aironet in Windows 2000* on page 60
- *Using the Cisco Aironet as a Normal Network Adapter* on page 64
- *Cisco Aironet Installation Notes and Issues* on page 66

Installing the Cisco Aironet in Windows NT 4.0

This section describes how to install the Cisco Aironet 340 adapter and driver on a Windows NT 4.0 system.

NOTE: The Cisco Aironet 350 adapter is not supported on Windows NT, and therefore no driver is provided.

To install the Cisco Aironet 340 adapter and driver in Windows NT 4.0:

1. After installing the Sniffer software, remove any installed copies of the Aironet Client Utility.
2. Remove any installed adapter drivers (either a previous version of the Sniffer driver or another vendor's driver) for the Cisco Aironet adapter. You remove drivers in Windows NT from the **Adapters** tab of the **Network** control panel.
3. Restart the computer and log in to Windows NT as an Administrator.
4. Install Version 4.15 or later of Cisco's Aironet Client Utility:
    a. Download Version 4.15 or later of Cisco's Aironet Client Utility from the Cisco web site (http://www.cisco.com).

b Install the Aironet Client Utility according to the instructions on the Cisco web site. Install with the following settings:

- When the installation program prompts you to select the preferred server-based authentication method, select None.

- When the installation program asks you which components you would like to install, select all components.

5 Restart the computer and log in to Windows NT as an Administrator.

6 Insert the Aironet 340 adapter in an available Type II PC card slot on the target machine.

7 Locate an available IRQ and IO Base Address.

NOTE: In most cases, the default resources found by the driver will work. However, in some cases, you may need to identify free resources as described in this step.

---

a Select the **Windows NT Diagnostics** program from the **Administrative Tools (Common)** program group under the **Start** menu.

b In the dialog box that appears, click the **Resources** tab. The IRQs currently in use on the PC are listed by number.

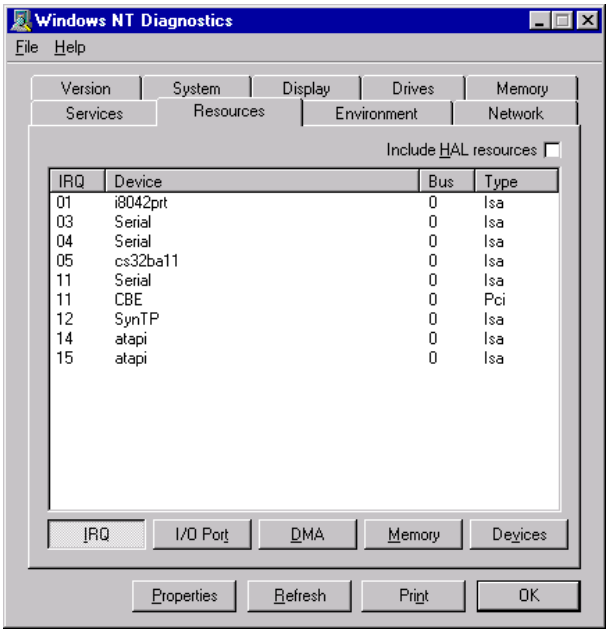


Figure 6-1. Selecting an IRQ for the Cisco Aironet Wireless LAN Adapter

c The Cisco Aironet card can use IRQs 3 through 15. Determine if one of these IRQs is available and write down its number for later use.

NOTE: If all of these IRQs are already in use, you will need to make one of them available for the Cisco Aironet adapter by uninstalling a conflicting device.

---

d Click **I/O Port** at the bottom of the **Windows NT Diagnostics** window (Figure 6-1). The I/O Port windows currently in use on the PC are listed.

e The Cisco Aironet card can use I/O Ports from 0-7F0. Determine if one of these I/O Ports is available and write down its number for later use.

NOTE: If all of these I/O Ports are already in use, you will need to make one of them available for the Cisco Aironet adapter by uninstalling a conflicting device.

---

8 Install the driver provided by Network General for the Aironet 340 adapter:

a Start the MS-Windows **Network** control panel by right-clicking on the Network Neighborhood icon on the desktop and selecting the **Properties** command from the menu that appears.

b Click the **Adapters** tab of the **Network** control panel.

c In the **Adapters** tab, click **Add**.

d The Select Network Adapter dialog box appears. Click **Have Disk**.

e In the Insert Disk dialog box, supply the path to the Cisco340\WinNT subdirectory, and click **OK**.

NOTE: The location for Sniffer Portable drivers is *C:\Program Files\NAI\SnifferNT\Driver\en\Cisco340\WinNT or C:\Program Files\NAI\SnifferNT\Driver\en\Cisco350\WinNT.*

---

f In the Select OEM Options dialog box, select the driver corresponding to the type of Cisco Aironet card you installed (for example, Cisco 340 Series PCMCIA Wireless LAN Adapter) and click **OK**.

The Aironet Wireless Communications, Inc. Adapter Setup dialog box appears.

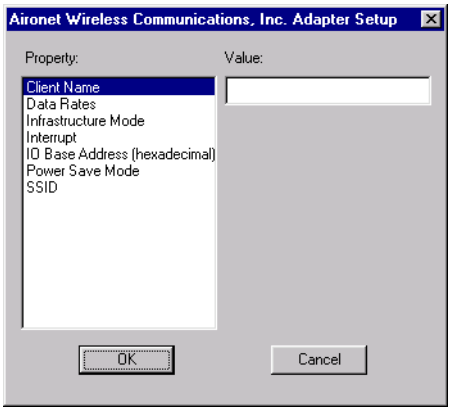


Figure 6-2. The Aironet Wireless Communications Adapter Setup Dialog Box

g Set the options in the Aironet Wireless Communications, Inc. Adapter Setup dialog box:

Client Name	Not necessary for the Sniffer software.
Data Rates	Set to Auto.
Infrastructure Mode	Set to Yes.
Interrupt	Set to the same value you recorded in Step 7 on page 54.
IO Base Address	Set to the same value you recorded in Step 7 on page 54.
Power Save Mode	Set to CAM.
SSID	Not necessary for the Sniffer software. However, if you want to use the Aironet 340/350 adapter for normal wireless LAN activities, you will need to set both this option (either here or in the Aironet Client Utility) and the **WEP Encryption** option (which can only be set in the Aironet Client Utility).

NOTE: Occasionally, Windows NT may have some difficulty installing the wireless adapter's driver even after allocating free resources. If this happens, try changing some of the resource settings for the card (I/O Base Address or Interrupt) to other free resources.

h When you have finished configuring the Cisco Aironet adapter in the Aironet Wireless Communications, Inc. Adapter Setup dialog box, click **OK**.

i Click **Close** in the **Network** control panel.

The system installs the card according to your settings and updates the bindings.

j When installation finishes, the system prompts you to configure the TCP/IP properties for the Aironet 340 adapter (if TCP/IP is bound to it).

Binding TCP/IP to the Aironet 340 adapter is not required for the Sniffer software. However, to use the Aironet 340 adapter for normal wireless LAN operations, you must set the TCP/IP properties to match your network. Click **OK** when you have finished.

k When installation has finished, the system prompts you to restart the computer. Click **Yes** to restart the computer.

9 If you will also use this adapter for normal wireless LAN activities, use the Aironet Client Utility to configure the card's SSID, WEP keys, and so on. See your Aironet documentation for details.

10 Verify that the correct driver is installed correctly by examining its entry in the **Adapters** tab of the Network control panel:

   a Start the MS-Windows **Network** control panel by right-clicking on the Network Neighborhood icon on the desktop and selecting the **Properties** command from the menu that appears.

   b Click the **Adapters** tab of the **Network** control panel.

   c In the **Adapters** tab, verify that the driver for the wireless adapter appears in the following format:.

   Sniffer (*vendor name*) - *card description*

   If the driver for the wireless adapter does not appear in this format, you will need to repeat the installation procedure to install the driver.

11 At this point, the Cisco Aironet wireless adapter should be installed with the Network General driver in Windows NT. See *Creating a Local Agent to Use the Wireless LAN Adapter* on page 79 to create a new local agent in the Sniffer software to use the adapter.

Installing the Cisco Aironet in Windows XP

This section describes how to install the Cisco Aironet 340/350 adapter and driver on a Windows XP system.

To install the Cisco Aironet 340/350 adapter and driver in Windows XP:

1 After installing the Sniffer software, log in to Windows XP as an Administrator.

2 Insert the Aironet 340/350 adapter in an available Type II PC card slot on the target machine.

   Windows XP automatically detects the new card and installs its native device driver.

3 Open the Network Connections folder by selecting the **Start > Control Panel > Network Connections** option.

4 Right-click the Wireless Network Connection entry associated with the Cisco Aironet 340/350 adapter and select **Properties**.

   The Wireless Network Connections Properties dialog box appears.

5 Click **Configure**.

The Adapter Properties dialog box for the Cisco Aironet 340/350 adapter appears.

6 Click the **Driver** tab.

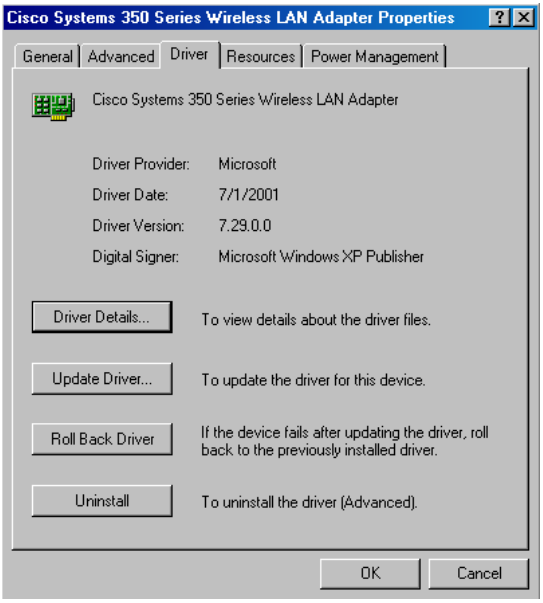


Figure 6-3. Wireless Network Connection Properties Dialog Box

7 Click **Update Driver**.

The Hardware Update Wizard starts.

8 Select the **Install from a list or specific location (Advanced)** option. and click **Next**.

9 Select the **Don't search** option and click **Next.**

10 Click **Have Disk**.

The Install from Disk dialog box appears prompting you to supply the path to the driver to install.

11 Click **Browse** and navigate to the path where the driver for the Cisco Aironet 340/350 adapter is installed.

NOTE: The location for Sniffer Portable drivers is *C:\Program Files\NAI\SnifferNT\Driver\en\Cisco340\XP or C:\Program Files\NAI\SnifferNT\Driver\en\Cisco350\XP.*

12 Click **Open** on the Browse dialog box.

You are returned to the Install from Disk dialog box.

13 Click **OK** in the Install from Disk dialog box.

If the operating system is configured to alert you to unsigned drivers, a dialog box will appear warning you that you are about to install a driver that has not been verified by Microsoft Corporation.

14 Click **Continue Anyway** to continue the installation.

The wizard installs the driver. When it has finished, it displays a screen indicating that the driver is installed.

15 Click **Finish** to complete the installation.

You are returned to the Adapter Properties dialog box.

16 Click **OK** to clear the Adapter Properties dialog box.

17 For Sniffer Portable users: If you did not uninstall the QoS Packet Scheduler Service during the Sniffer Portable software installation, you should disable it for this adapter now. See the *Sniffer Portable Installation Guide* for more information.

18 See *Creating a Local Agent to Use the Wireless LAN Adapter* on page 79 to create a new local agent in the Sniffer software to use the adapter.

Installing the Cisco Aironet in Windows 2000

This section describes how to install the Cisco Aironet adapter and driver on a Windows 2000 system. The procedure is somewhat different depending on whether you are updating an existing driver for the wireless adapter (either a previous version of the Sniffer driver or another vendor's driver) or installing the adapter and driver for the first time. Use the appropriate procedure below.

- *First Time Installation* on page 61
- *Updating Existing Drivers* on page 62

First Time Installation

For Windows 2000, you install an adapter for the first time by inserting the card in the PC and using the Found New Hardware Wizard.

To install the Aironet 340/350 adapter and driver in Windows 2000 for the first time:

1. Remove any installed copies of the Aironet Client Utility.
2. Reboot the computer.
3. After installing the Sniffer software, log in to Windows 2000 as an Administrator.
4. Insert the Aironet 340/350 wireless adapter in an available Type II PC card slot on the target machine.

   Windows 2000 presents a Wizard to help you install a new driver for the Aironet 340/350 adapter.

   NOTE: If Windows 2000's plug-and-play feature automatically installs a driver for the adapter instead of starting the Found New Hardware Wizard, turn to *Updating Existing Drivers* on page 62 to update the existing driver

5. Click **Next**.

   The **Install Hardware Device Drivers** window appears.
6. Select the **Search for a suitable driver for my device** option and click **Next**.

   The **Locate Driver Files** window appears.
7. Check only the **Specify a location** option and click **Next**.

   The Found New Hardware Wizard prompts you to supply a path to the device driver.
8. Click **Browse**, navigate to the Cisco340\Win2K or Cisco350\Win2K subdirectory where the driver files are installed, and click **Open**. Specify the Cisco340\Win2K driver directory for either the Cisco 340 or the Cisco 345 adapter.

   NOTE: The location for Sniffer Portable drivers is *C:\Program Files\NAI\SnifferNT\Driver\en\Cisco340\Win2K or C:\Program Files\NAI\SnifferNT\Driver\en\Cisco350\Win2K.*

9 Click **OK**.

Windows 2000 scans for the appropriate driver and presents the **Driver Files Search Results** window indicating that it has found the driver you specified in the previous step.

10 Click **Next** in the Driver Files Search Results window.

11 The **Digital Signature Not Found** warning appears asking you if you want to continue the installation. Click **Yes** to continue the installation.

The Wizard installs the selected driver. When it has finished, it presents the **Completing the Found New Hardware Wizard** window.

12 Click **Finish** to finish the installation.

13 Restart the computer.

14 Verify that the correct driver is installed correctly by examining its **Device Name** entry in the Network and Dial-Up Connections window:

a Right-click the My Network Places icon on the desktop and select **Properties**.

b Select the entry in the Network and Dial-Up Connections window for the wireless adapter and verify that the entry in the Device Name column appears in the following format:

Sniffer (*vendor name*) - *card description*

If the driver for the wireless adapter does not appear in this format, you will need to repeat the installation procedure to install the driver.

15 At this point, the Aironet 340/350 wireless adapter should be installed with the Network General driver in Windows 2000. See *Creating a Local Agent to Use the Wireless LAN Adapter* on page 79 to create a new local agent in the Sniffer software to use the adapter.

Updating Existing Drivers

For Windows 2000, you update an existing driver using the Device Manager. The procedure is the same regardless of whether you are updating the vendor's existing driver or a previous version of the Sniffer driver.

To update an existing driver for the Cisco Aironet adapter in Windows 2000:

1 If the currently installed driver is the native Cisco driver:

a Remove any installed copies of the Aironet Client Utility.

b. Remove any installed adapter drivers for the Aironet 340/350.

   Cisco Systems describes how to do this in the **Cisco Aironet Drivers and Utilities** web page on their web site at http://www.cisco.com.

c. Reboot the computer.

2. Start the Device Manager:

   a. Right-click the **My Computer** icon and select **Properties**.

   b. In the dialog box that appears, click the **Hardware** tab.

   c. Click **Device Manager**.

   d. Expand the **Network Adapters** entry by clicking the **+** sign adjacent to its entry.

3. Right-click the entry for the Cisco Aironet adapter and select **Properties**.

4. Click the **Driver** tab in the dialog box that appears

5. Click **Update Driver**.

   The Upgrade Device Driver Wizard starts.

6. Click **Next**.

7. Select the **Display a list of the known drivers for this device so that I can choose a specific driver** option and click **Next**.

8. In the dialog box that appears, click **Have Disk**.

   The Upgrade Device Driver Wizard prompts you to supply a path to the device driver.

9. Click **Browse** and navigate to the Cisco340\Win2K or Cisco350\Win2K subdirectory where the driver files are installed.

NOTE: The default Sniffer Portable location for all drivers: *C:\Program Files\NAI\SnifferNT\Driver\en\Cisco340\Win2K or C:\Program Files\NAI\SnifferNT\Driver\en\Cisco350\Win2K*

---

10. Click **Open** in the Locate File dialog box.

11. Click **OK** in the Install from Disk dialog box.

    Windows scans for the driver and presents a dialog box listing different cards supported by the specified driver.

12. Select the entry corresponding to your card and click **Next**.

13 The Upgrade Device Wizard indicates that it is ready to install the selected driver. Click **Next** to begin installing the driver.

   The Digital Signature Not Found warning appears asking you if you want to continue the installation.

14 Click **Yes** in the Digital Signature Not Found warning to continue the installation.

   The Wizard installs the selected driver. When it has finished, it presents the **Completing the Upgrade Device Driver Wizard** window.

15 Click **Finish** to finish the installation.

16 Restart the computer.

17 Verify that the correct driver is installed correctly by examining its **Device Name** entry in the Network and Dial-Up Connections window:

   a Right-click the **My Network Places** icon and select **Properties**.

   b Select the entry in the Network and Dial-Up Connections window for the wireless adapter and verify that the entry in the Device Name column appears in the following format:

      Sniffer (*vendor name*) - *card description*

      If the driver for the wireless adapter does not appear in this format, you will need to repeat the installation procedure to install the driver.

18 At this point, the Aironet 340/350 wireless adapter should be installed with the Network General driver in Windows 2000. See*Creating a Local Agent to Use the Wireless LAN Adapter* on page 79 to create a new local agent in the Sniffer software to use the adapter.

Using the Cisco Aironet as a Normal Network Adapter

When the Sniffer software is connected to the Cisco Aironet 340/350, the card operates in promiscuous mode and cannot participate as an active member of the wireless LAN. However, when the Sniffer software is not connected to the Cisco Aironet 340/350, you can use the adapter to participate actively in a wireless network. For Windows NT, 2000, and 98 SE, use the Aironet Client Utility to set up the Aironet 340/350's operating parameters (ESSID, WEP keys, and so on) for normal network participation. For Windows XP, use the **Wireless Network** tab in the Wireless Network Connection Properties dialog box to set the same parameters. See the Aironet 340/350 documentation for details.

NOTE: Do not make changes to the Cisco Aironet's configuration while the Sniffer software is running.

Cisco Aironet Installation Notes and Issues

Keep the following notes and tips in mind when working with the Cisco Aironet wireless adapter:

- After exiting the Sniffer software, it may take up to a minute for the wireless adapter to transition to normal wireless network participation.
- Do not use the client utility provided with the Cisco Aironet while the Sniffer software is running.
- If the machine with the Sniffer software installed has multiple card slots, you can prevent potential problems by always using the wireless adapter in the same slot.

Installing the Proxim 802.11a Adapters / Drivers 7

Overview

This chapter describes how to install the Proxim Harmony 802.11a CardBus adapter and driver for the Sniffer software.

- *Installing the Proxim 802.11a Adapter in Windows XP* on page 67
- *Installing the Proxim 802.11a Adapter in Windows 2000* on page 69
- *Using the Proxim 802.11a Adapter as a Normal Network Adapter* on page 72
- *Proxim 802.11a Adapter Installation Notes and Issues* on page 74

Installing the Proxim 802.11a Adapter in Windows XP

This section describes how to install the Proxim 802.11a adapter and driver on a Windows XP system.

To install the Proxim 802.11a adapter and driver in Windows XP:

1. After installing the Sniffer software, log in to Windows XP as an Administrator.
2. Insert the Proxim 802.11a adapter in an available Type II PC card slot on the target machine.

   Windows XP detects the new card and displays a wizard to help you install the driver.
3. Select the **Install from a list or specific location (Advanced)** option and click **Next**.
4. Select the **Don't search** option and click **Next.**
5. Click **Have Disk**.

   The Install from Disk dialog box appears prompting you to supply the path to the driver to install.

6 Click **Browse** and navigate to the Proxim\WinXP subdirectory where the driver files are installed.

NOTE: The location for Sniffer Portable drivers is *:\Program Files\NAI\SnifferNT\Driver\en\Proxim\WinXP.*

---

7 Click **Open** in the Browse dialog box.

You are returned to the Install from Disk dialog box.

8 Click **OK** in the Install from Disk dialog box.

If the operating system is configured to alert you to unsigned drivers, a dialog box will appear warning you that you are about to install a driver that has not been verified by Microsoft Corporation.

9 Click **Continue Anyway** to continue the installation.

The wizard installs the driver. When it has finished, it displays a screen indicating that the driver is installed.

10 Click **Finish** to complete the installation.

You are returned to the Adapter Properties dialog box.

11 Click **OK** to clear the Adapter Properties dialog box.

12 For Sniffer Portable users: If you did not uninstall the QoS Packet Scheduler Service during the installation of the Sniffer Portable software, you should disable it for this adapter now. See the *Sniffer Portable Installation Guide* for details.

13 See *Creating a Local Agent to Use the Wireless LAN Adapter* on page 79 to create a new local agent in the Sniffer software to use the adapter.

Installing the Proxim 802.11a Adapter in Windows 2000

This section describes how to install the Proxim 802.11a adapter and driver on a Windows 2000 system. The procedure is somewhat different depending on whether you are updating an existing driver for the wireless adapter (either a previous version of the Sniffer driver or another vendor's driver) or installing the adapter and driver for the first time. Use the appropriate procedure below.

- *First Time Installation* on page 69
- *Updating Existing Drivers* on page 70

First Time Installation

For Windows 2000, you install an adapter for the first time by inserting the card in the PC and using the Found New Hardware Wizard.

To install the Proxim 802.11a adapter and driver in Windows 2000 for the first time:

1. After installing the Sniffer software, log in to Windows 2000 as an Administrator.
2. Insert the Proxim 802.11a wireless adapter in an available Type II PC card slot on the target machine.

   Windows 2000 presents a Wizard to help you install a new driver for the Proxim 802.11a adapter.

   NOTE: If Windows 2000's plug-and-play feature automatically installs a driver for the adapter instead of starting the Found New Hardware Wizard, turn to *Updating Existing Drivers* on page 70 to update the existing driver.

3. Click **Next**.

   The Install Hardware Device Drivers window appears.
4. Select the **Search for a suitable driver for my device** option and click **Next**.

   The Locate Driver Files window appears.
5. Check only the **Specify a location** option and click **Next**.
6. Click **Browse**, navigate to the Proxim\Win2K subdirectory where the driver files are installed, and click **Open**:

NOTE: The location for Sniffer Portable drivers is *:\Program Files\NAI\SnifferNT\Driver\en\Proxim\Win2K.*

7 Click **OK**.

Windows 2000 scans for the driver and presents the Driver Files Search Results window indicating that it has found the driver you specified in the previous step.

8 Click **Next** on the Driver Files Search Results window.

The Digital Signature Not Found warning appears asking you if you want to continue the installation.

9 At this point, the rest of the installation procedure is the same as the **Update** procedure. Continue with Step 14 on page 71.

Updating Existing Drivers

For Windows 2000, you update an existing driver using the Device Manager. The procedure is the same regardless of whether you are updating the vendor's existing driver or a previous version of the Sniffer driver.

To update an existing driver for the Proxim 802.11a adapter in Windows 2000:

1 After installing the Sniffer software, log in to Windows 2000 as an Administrator.

2 Start the Device Manager:

- **a** Right-click the **My Computer** icon and select the **Properties** command from the menu that appears.
- **b** In the dialog box that appears, click the **Hardware** tab.
- **c** Click **Device Manager**.
- **d** Expand the **Network Adapters** entry by clicking the **+** sign adjacent to its entry.

3 Right-click the entry for the Proxim 802.11a adapter and select **Properties**.

4 Click the **Driver** tab.

5 Click **Update Driver**.

The Upgrade Device Driver Wizard starts.

6 Click **Next**.

7 Select the **Display a list of the known drivers for this device so that I can choose a specific driver** option and click **Next**.

8 In the dialog box that appears, click **Have Disk**.

The Upgrade Device Driver Wizard prompts you to supply a path to the device driver.

9 Click **Browse** and navigate to the following Proxim\Win2K subdirectory for the driver.

NOTE: The default Sniffer Portable location for all drivers: *C:\Program Files\NAI\SnifferNT\Driver\en*

---

10 Click **Open** in the Locate File dialog box.

11 Click **OK** in the Install from Disk dialog box.

Windows scans for the driver and presents a dialog box listing different cards supported by the specified driver.

12 Select the entry corresponding to your card and click **Next**.

13 The Upgrade Device Wizard indicates that it is ready to install the selected driver. Click **Next** to begin installing the driver.

The Digital Signature Not Found warning appears asking you if you want to continue the installation.

14 Click **Yes** on the Digital Signature Not Found warning to continue the installation.

When driver installation has finished, the Wizard presents the Completing the Found New Hardware Wizard window.

15 Click **Finish** to finish the installation.

16 Restart the computer.

17 Verify that the correct driver is installed correctly by examining its **Device Name** entry in the Network and Dial-Up Connections window:

a Right-click the **My Network Places** desktop icon and select **Properties**.

b Select the entry in the Network and Dial-Up Connections window for the wireless adapter and verify that the entry in the Device Name column appears in the following format:

Sniffer (*vendor name*) - *card description*

If the driver for the wireless adapter does not appear in this format, you will need to repeat the installation procedure to install the driver.

18 At this point, the Proxim 802.11a wireless adapter should be installed with the Network General driver in Windows 2000. See *Creating a Local Agent to Use the Wireless LAN Adapter* on page 79 to create a new local agent in the Sniffer software to use the adapter.

Using the Proxim 802.11a Adapter as a Normal Network Adapter

When the Sniffer software is connected to a Proxim 802.11a wireless adapter, the card operates in promiscuous mode and cannot participate as an active member of the wireless LAN. However, when the Sniffer software is not connected to a Proxim 802.11a card, you can use the adapter to participate actively in a wireless network.

You can configure a Proxim 802.11a card for normal wireless network participation (including configuring the ESSID, WEP keys, and so on).

Windows XP

For Windows XP, you can configure a Proxim 802.11a adapter for normal wireless network participation in three different ways:

- Using Windows XP's built-in tools for automatic wireless network management on the **Wireless Networks** tab of the Connection Properties dialog box (if the **Use Windows to configure my wireless network settings** option found there is enabled).

  This is the easiest way to configure client settings for the Proxim 802.11a adapter.

- Using the manual options on the **Advanced** tab of the Connection Properties dialog box (if the **Use Windows to configure my wireless network settings** option on the Wireless Networks tab is disabled).

- Using Proxim's supplied configuration utility. For the Proxim Harmony card, the **Enabled Harmony Configuration (Disable Windows XP Settings)** option on the Harmony Utility's **Configuration** tab is checked.

The following procedure explains how to use either Windows XP's automatic or manual configuration capabilities. For information on Proxim's utility, see the Proxim documentation for your specific adapter.

To configure the Proxim 802.11a adapter for normal client operations (Windows XP):

1. Open the Network Connections folder by selecting the **Start > Control Panel > Network Connections** option.
2. Right-click the Wireless Network Connection entry associated with the Proxim 802.11a adapter and select the **Properties** command from the menu that appears.

   The Wireless Network Connection Properties dialog box appears.
3. Click the **Wireless Networks** tab.
4. Do you want to set wireless network options automatically or manually?

   - For automatic configuration, enable the **Use Windows to configure my wireless network settings** option, click **Configure**, and check the Windows-supplied settings found there for suitability. Change settings to match your wireless network, if necessary.

   NOTE: If you enable either the **Internet Connection Firewall** or **Internet Sharing** options on a client connection, it is a good idea to unbind the Sniffer driver from the connection before proceeding. Remember to rebind the Sniffer driver before using the connection with the Sniffer software.

   - For manual configuration, deselect the **Use Windows to configure my wireless network settings** option. Then, click the **General** tab and click **Configure**. Click the **Advanced** tab and set the options found there to match your wireless network.

Windows 2000

For Windows 2000, you can configure a Proxim 802.11a adapter for normal wireless network participation using either the options on the **Advanced** tab of the Connection Properties dialog box or by using Proxim's vendor-supplied configuration utility.

The following procedure explains how to access the options on the **Advanced** tab. For information on Proxim's utility, see the Proxim documentation for your Proxim adapter.

To configure the Proxim 802.11a for normal client operations (Windows 2000):

1. Open the Network and Dial-Up Connections folder by selecting the **Start > Settings > Network and Dial-Up Connections** option.

2 Right-click the Wireless Network Connection entry associated with the Proxim 802.11a adapter and select **Properties**.

The Connection Properties dialog box appears.

3 Click **Configure**.

The Network Adapter Properties dialog box appears.

4 Click the **Advanced** tab and use the options that appear to set parameters for normal wireless network participation.

NOTE: For Windows 2000, you must leave the **Authentication** option on the **Advanced** tab enabled for successful operation.

NOTE: Do not make changes to the Proxim 802.11a adapter's configuration while the Sniffer software is running.

Proxim 802.11a Adapter Installation Notes and Issues

Keep the following notes and tips in mind when working with Proxim 802.11a wireless adapters:

- After exiting the Sniffer software, it may take up to a minute for the wireless adapter to transition to normal wireless network participation.
- If the PC with the Sniffer software installed has multiple card slots, you can prevent potential problems by always using the wireless adapter in the same slot.
- Stop the Microsoft Windows service, Wireless Zero Configuration, when using the Proxim Harmony 802.11a adapter.

Using the Proxim 802.11a Harmony to Monitor "2X" Networks

The Proxim Harmony 802.11a adapter card used by the Sniffer software supports a proprietary extension of the 802.11a standard called **2X** (or, occasionally, **Turbo**). Essentially, this extension allows 802.11a networks to operate at twice the rates stated by the 802.11a specification (for example, instead of the upper limit of 54 Mbps stated for the 802.11a specification, the 2X extension theoretically allows for an upper limit of 108 Mbps).

If you want to use the Proxim Harmony to monitor a network which has implemented the 2X extension, be sure to enable the 2X/Turbo mode for the adapter before starting the Sniffer software. Enable the 2X/Turbo mode in either the **Advanced** tab of the Connection Properties dialog box, or in the vendor-supplied configuration utility for the Proxim Harmony. See the procedures in *Using the Proxim 802.11a Adapter as a Normal Network Adapter* on page 72 for information on how to access this tab (as well as other ways to set configuration options for the Proxim Harmony).

SECTION 2

Getting Started with Wireless Functionality

Creating Local Agents for Wireless LAN Adapters

Configuring Wireless LANs to Capture

Advanced Features for Wireless Analysis

Creating Local Agents for Wireless LAN Adapters 8

Overview

This chapter describes how to create a local agent in the Sniffer software to use the wireless LAN adapter installed in the previous chapters.

Creating a Local Agent to Use the Wireless LAN Adapter

Before you can use the Sniffer software to capture from a wireless network, you need to define a local agent that will use the wireless LAN adapter you installed in the previous chapters. The following procedure explains how.

To define a new local agent to work with the wireless LAN adapter:

1. Start the Sniffer software.
2. Go to **Files** > **Select Settings** to open the **Settings** dialog box opens. It lists the local agents that have already been defined for machine with the Sniffer software installed.
3. Click **New** to define a new local agent to work with the wireless LAN adapter.
4. In the **New Settings** dialog box, use the **Description** field to supply a descriptive name for this local agent. Your description will appear in future instances of the **Settings** dialog box. For example, you may want to choose something like **Wireless LAN Analyzer**.
5. Select the wireless adapter to use for this local agent from the **Network Adapter** drop-down list. The list includes all NDIS 3.1 compliant adapters currently installed.

NOTE: If the wireless adapter does not appear in the drop-down list, ensure that the **Sniffer Driver** is bound to the network card you installed in the previous chapters.

For Windows XP and NT, you can do this on the **Bindings** tab of the Network control panel.

For Windows 2000, you can do this by starting the Network control

panel, right-clicking the entry for the adapter you installed in the previous chapters, and selecting **Properties**. Then make sure that the checkbox next to the **Sniffer Driver** entry under **Components checked are used by this connection** is checked.

6 The **Netpod Configuration** fields do not apply for the wireless LAN adapter. Specify **No Pod**.

7 If at some point you want to define an additional local agent using the same settings you have specified here, you can use the **Copy settings from** field to use these settings as a template. The drop-down list includes all previously defined local agents.

The following example shows the **New Settings** dialog box as configured to use a wireless LAN adapter.

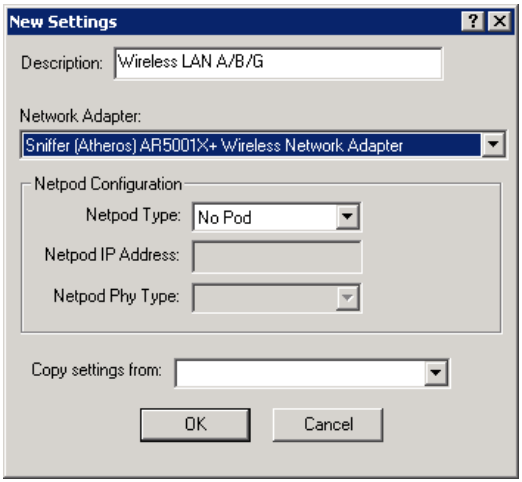


Figure 8-1. Creating a Local Agent

8 Click **OK**.

9 A new entry appears in the **Settings** dialog box for the local agent you just defined. Make sure this local agent is selected by clicking it.

10 Click **OK** again.

The new local agent using the wireless LAN adapter is now selected for capturing and monitoring the network. At this point, you are ready to configure the Sniffer software to monitor and capture from your wireless network. See *Configuring Wireless LANs to Capture* on page 81 for additional information.

Configuring Wireless LANs to Capture 9

Overview

This chapter describes how to configure the Sniffer software to monitor and capture traffic on your wireless network. This chapter describes how to set options specific to analyzing wireless networks. For information on standard Sniffer software features (such as how to set triggers, filters, and so on), see the software *User's Guide*.

Options specific to wireless adapters are found in the following areas:

- Set standard Sniffer software options in the **802.11** tab of the Options dialog box (accessed by selecting **Options** from the **Tools** menu). *Setting Wireless Options* on page 82.
- Set Expert options in the **802.11 Options** tab of the Sniffer software's Expert Properties dialog box (accessed by selecting **Expert Options** from the **Tools** menu). *Setting Expert Wireless Options* on page 90.

Monitoring Wireless Networks

Sniffer Portable monitors independent basic service set (IBSS) and infrastructure wireless networks.

- **IBSS networks** are wireless networks without access to a distribution system. Traffic stays within the IBSS network. IBSS networks are also known as ad hoc or independent networks.
- **Infrastructure networks** are wireless networks with access to a distribution system. Infrastructure networks are typically one part of an integrated wired and wireless network structure.

When you select a wireless adapter in the Select Settings dialog box (accessed from **File** > **Select Settings** or automatically the first time you select an adapter to monitor), you are by default specifying that you are monitoring both IBSS and infrastructure networks.

Setting Wireless Options

Wireless analysis options are found in the **802.11** tab of the Options dialog box. Display the **802.11** tab by selecting **Options** from the **Tools** menu and clicking the **802.11** tab in the Options dialog box (Figure 9-1).

NOTE: The **802.11** tab is only available if a wireless LAN adapter is the currently selected adapter. You can change the currently selected adapter using the **Select Settings** command in the **File** menu. See *Monitoring Wireless Networks* on page 81.

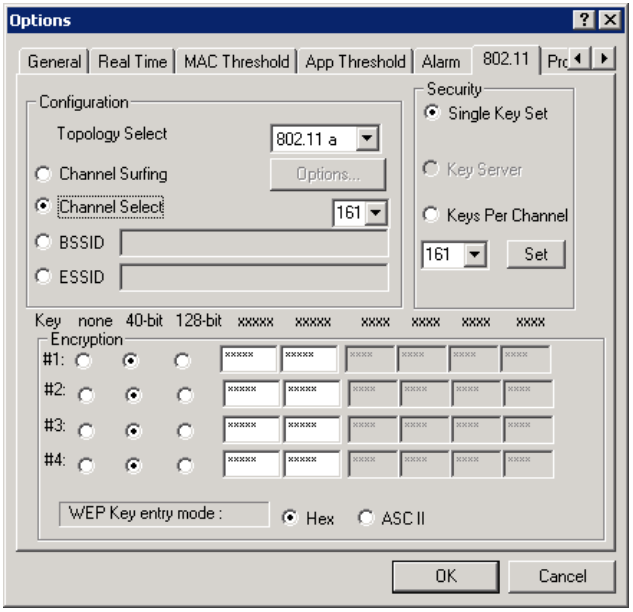


Figure 9-1. 802.11 Tab of the Options Dialog Box

The **802.11** tab lets you set the following options:

- **Configuration** options (see *Setting Configuration Options* on page 83)
- **Encryption** options (see *Setting Encryption Options* on page 85)
- **Security** options (see *Setting the Security Options* on page 89)

Setting Configuration Options

The **Configuration** options (shown in Figure 9-1) let you select the wireless LAN channel(s) you would like the Sniffer software to monitor. You can select the channel(s) to monitor in one of the following ways:

- **Topology Select.** Specify **802.11a** or **802.11b/g** for all wireless cards. After changing the wireless topology mode, the channel surfing and selection options within the 802.11 tab will change dynamically according to the different channels for each mode. When you change the topology from 802.11a to 802.11b/g or vice versa, any monitoring or capture screens are closed and then re-opened (similar to when you log off and log on).

  In an 802.11b/g combination card, 802.11b and 802.11g are monitored at the same time—not separately. Proxim and Cisco combination cards support 802.11a and 802.11b/g modes.

NOTE: After making a change to the **Topology Select** option, the Sniffer software will save and cache the last selected wireless mode. The cached wireless mode will be selected by default the next time the Sniffer software is started.

- Enable the **Channel Surfing** option to select a set of channels you would like the Sniffer software to monitor for specified amounts of time. Click the adjacent **Options** button to open the Channel Surfing Select dialog box (Figure 9-2) and specify the channels to monitor, as well as the time to monitor each channel.

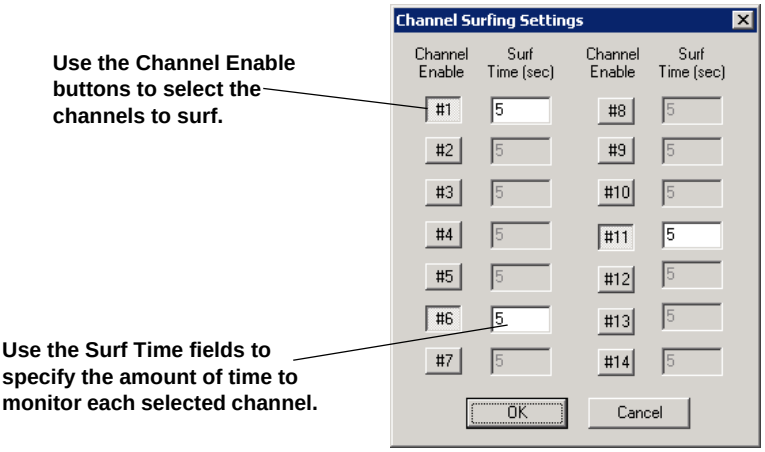


Figure 9-2. Channel Surfing Settings (802.11b/g Network)

NOTE: The Channel Surfing Settings dialog box will appear differently depending on whether the currently selected adapter is 802.11a or 802.11b/g. The dialog box for 802.11a will have more (and different) channels available for selection. They both work in the same way, however.

When **Channel Surfing** is enabled, the Sniffer software monitors the channels selected in the **Channel Surfing Settings** dialog box (Figure 9-2) in a cycle. The Sniffer software monitors each selected channel for the amount of time specified by its **Surf Time** field before moving on to the next selected channel.

NOTE: By default on an 802.11b/g network, Channels **1**, **6**, and **11** are enabled since these are the non-overlapping channels in an 802.11b wireless LAN. As such, they are the channels most often used.

- Enable the **Channel Select** option to specify a specific channel to monitor. Use the adjacent drop-down list to select the channel for monitoring.
- Enable the **BSSID** option to specify a six-byte Basic Service Set ID (BSSID) to monitor. Specify the BSSID in the adjacent field. If you select this option, the Sniffer software will monitor the first channel on which it detects the specified BSSID.
- Enable the **ESSID** option to specify an Extended Service Set ID (ESSID) to monitor. Specify the ESSID in the adjacent field. If you select this option, the Sniffer software will monitor the first BSSID on which it detects the specified ESSID.

NOTE: Some wireless networks are configured so that Access Points do not include ESSIDs in their beacon frames. In cases like this, specifying an ESSID to monitor will not work since the ESSID is never included in a beacon frame. Instead, specify a BSSID (since they are always included as one of the MAC address in beacon frames) or a Channel to monitor.

Channel Surfing Mode and Capture Triggers

If a trigger event occurs while the Sniffer software is in **Channel Surfing** mode, the Sniffer software will start capture on the wireless channel it was monitoring when the trigger event occurred — and channel surfing will stop. To return to **Channel Surfing** mode, you must re-enable the **Channel Surfing** option in the **802.11** tab of the **Options** dialog box (accessed by selecting the **Options** command from the **Tools** menu).

Setting Encryption Options

If the network to be monitored uses Wired Equivalent Policy (WEP) encryption, you can use the **Encryption** options in the **802.11** tab to specify the keys in use on the network to be monitored. If the correct keys are specified, the Sniffer software can decrypt and decode WEP-encrypted packets during capture.

An easy way to determine whether you have entered the correct WEP keys is to check for the presence of a large number of WEP-ICV errors in the Dashboard's **Detail** tab. If the counter indicates an abnormally large number of these errors, you probably have not entered the correct WEP keys for the network being monitored.

NOTE: You can also perform postcapture WEP decryption on trace files saved without the **Encryption** options specified correctly (if you know the correct WEP keys). See *Postcapture WEP Decryption* on page 134 for information on how to decrypt WEP-encrypted data in a buffer or saved trace file.

In a WEP-encrypted network, four keys are programmed identically into each station on the network. These keys can be either 40 bits or 104 bits in length. Their use is described in the following sections.

IMPORTANT: WEP key entries are *always* case-sensitive!

40-Bit Encryption

In a network using 40-bit encryption, each station on the network is programmed with the same four 40-bit shared keys. When a station has encrypted data to send, it generates a random 24-bit *Initialization Vector* (IV) and encrypts the data to be sent with the 24-bit IV and one of its four 40-bit shared keys. Therefore, the entire key length is 64 bits (40-bit shared key plus a 24-bit IV).

Stations send the 24-bit IV in the clear along with the encrypted data. A header field tells the receiving station which of the four shared keys is in use for the encrypted data. Receiving stations use the received 24-bit IV and their own stored 40-bit keys to decrypt the received data.

IMPORTANT: 40-bit encryption is often referred to as 64-bit encryption. Both terms refer to the same thing — a 40-bit stored key used in combination with a randomly generated 24-bit initialization vector to form a 64-bit key. Since

they mean the same thing, the Sniffer software supports both 40-bit and 64-bit encryption.

128-Bit Encryption

Although the usage of 128-bit encryption keys is not specified by the 802.11b standard, most vendors implement 128-bit encryption similarly to 64-bit encryption.

In a network using 128-bit encryption, each station on the network is programmed with the same four 104-bit shared keys. When a station has encrypted data to send, it generates a random 24-bit *Initialization Vector* (IV) and encrypts the data to be sent with the 24-bit IV and one of its four 104-bit shared keys. Therefore, the entire key length is 128 bits (104-bit shared key plus a 24-bit IV).

Stations send the 24-bit IV in the clear along with the encrypted data. A header field tells the receiving station which of the four shared keys is in use for the encrypted data. Receiving stations use the received 24-bit IV and their own stored 104-bit keys to decrypt the received data.

Configuring Encryption Options

You can specify the encryption keys that allow the Sniffer software to perform WEP decryption in either **Hex** or **ASCII** format, depending on how you set the **WEP Key Entry Mode** option in the **802.11** tab. Separate procedures are provided for each mode. See *Entering Encryption Keys in Hex Format* on page 86 and *Entering Encryption Keys in ASCII Format* on page 88.

Entering Encryption Keys in Hex Format

To enter WEP encryption keys in Hex format:

1. Display the **Tools > Options > 802.11** tab.
2. Select **Hex** for the **WEP Key Entry Mode** option at the bottom of the **802.11** tab.

   If you have previously entered encryption keys in **ASCII** mode, the Sniffer software automatically converts your entries to **Hex** mode. Key entries of five ASCII characters appear as 40-bit keys in **Hex** mode. Similarly, key entries of 13 ASCII characters appear as 128-bit keys in **Hex** mode.
3. You can enter up to four separate encryption keys. For each key, do the following:

a Specify the length of the key by selecting the appropriate option. Keys can be either **None**, **40-bit**, or **128-bit**. Use the **None** option if no encryption is used on the network.

Depending on the length of the key specified, some or all of the adjacent fields become active, enabling you to specify the keys in use.

b Specify the exact, case-sensitive value for each key in the adjoining spaces provided.

NOTE: The four encryption keys in use on a WEP-encrypted network are all typically the same length — either 40-bit or 128-bit.

NOTE: Key entries appear as asterisks to preserve their security.

Figure 9-3 shows the **802.11** tab with four 40-bit encryption keys specified in **Hex** mode.

4 Click **OK**.

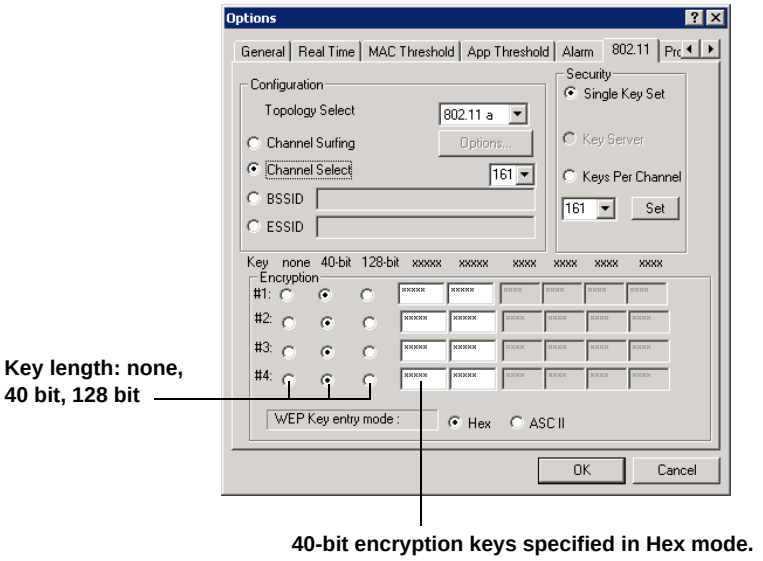


Figure 9-3. Entering Encryption Keys in Hex Mode

Entering Encryption Keys in ASCII Format

To enter WEP encryption keys in ASCII format:

1. Display the **Tools** > **Options** > **802.11** tab.
2. Select **ASCII** for the **WEP Key Entry Mode** option at the bottom of the **802.11** tab. The **802.11** tab appears as in Figure 9-4.

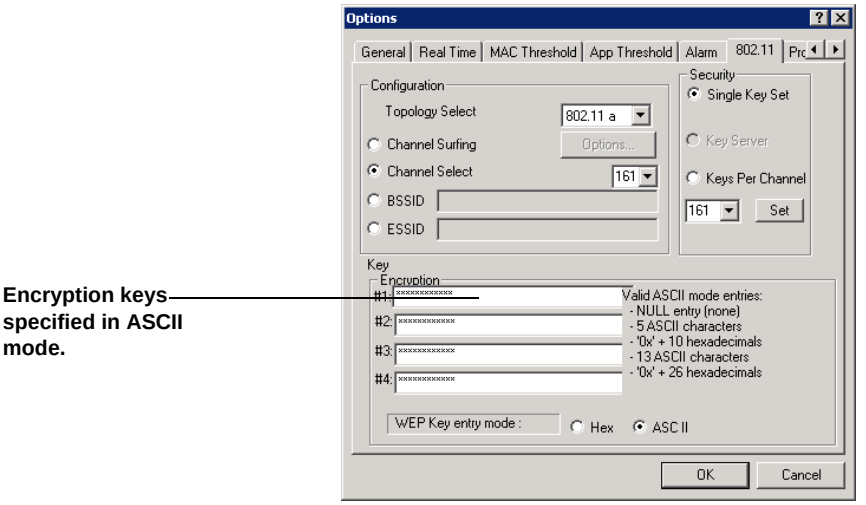


Figure 9-4. Entering Encryption Keys in ASCII Mode

If you have previously entered encryption keys in **Hex** mode, the Sniffer software automatically converts your entries to **ASCII** mode. Key entries are converted differently depending on the length specification in the **Hex** entry mode:

- If **None** was selected, the entry fields in Figure 9-4 appear empty.
- If **40-bit** was selected, the Sniffer software attempts to convert the hex key into ASCII. If conversion is possible, 5 ASCII characters appear. If conversion is not possible, 0x followed by 10 hex characters appears.
- If **128-bit** was selected, the Sniffer software attempts to convert the hex key into ASCII. If conversion is possible, 13 ASCII characters appear. If conversion is not possible, 0x followed by 26 hex characters appears.

3 You can enter up to four separate encryption keys in ASCII format. Valid ASCII entries include the letters A through Z in either upper- or lower-case, in addition to the numbers 0 through 9. Entries are case-sensitive.

Specified keys are interpreted as the following:

- An empty field is equivalent to a setting of **None** in **Hex** entry mode (that is, no encryption is used on the network).
- Five ASCII characters or 0x followed by 10 hex characters is interpreted as a 40-bit key.
- Thirteen ASCII characters or 0x followed by 26 hex characters is interpreted as a 128-bit key.

NOTE: The four encryption keys in use on a WEP-encrypted network are all typically the same length — either 40-bit or 128-bit.

NOTE: Key entries appear as asterisks to preserve their security.

4 Click **OK**.

Setting the Security Options

The Security options let you specify whether the Sniffer software should use the same WEP keys on every channel on the wireless network or different keys on different channels.

- Enable the **Single Key Set** option if you would like the Sniffer software to use the WEP keys specified in the **Encryption** portion of the **802.11** tab for every channel on the wireless network.
- Enable the **Keys Per Channel** option if you would like to specify different sets of WEP keys for different channels on the wireless network. Use the following procedure to specify different sets of WEP keys for different channels.

To specify different WEP keys for different channels using the Keys Per Channel option:

1 Display the **Tools > Options > 802.11** tab.

2 Enable the **Keys Per Channel** option.

3 Use the drop-down list under the **Keys Per Channel** option to select the channel for which you would like to specify WEP keys (Figure 9-6).

The fields in the **Encryption** section automatically populate with the current WEP key settings for the selected channel.

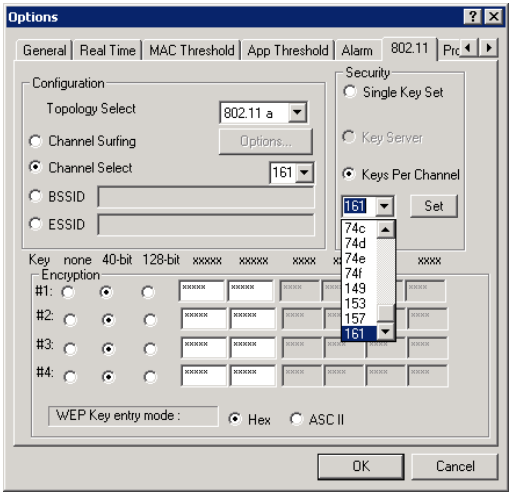


Figure 9-5. Select the Channel for Key Specification

4 Specify the WEP keys for the selected channel in the Encryption section of the **802.11** tab. See *Setting Encryption Options* on page 85 for details.

5 Click **Set** to enable the WEP keys for the selected channel.

6 Repeat Step 3 through Step 4 for each channel for which you would like to specify different WEP keys.

7 When you have finished setting keys, click **OK** on the **802.11** tab.

Setting Expert Wireless Options

Expert wireless options are found in the **802.11 Options** tab of the Sniffer software's Expert Properties dialog box. Display the **802.11 Options** tab by selecting **Expert Options** from the **Tools** menu and clicking the **802.11 Options** tab in the dialog box that appears. Figure 9-6 shows the **802.11 Options** tab of the **Expert Options** dialog box.

If this option is enabled during capture, the Expert will flag access points whose MAC addresses are not in the *Known Access Points* list as rogues.

If this option is enabled during capture, the Expert will flag mobile units whose MAC addresses are not in the *Known Mobile Units* list as rogues.

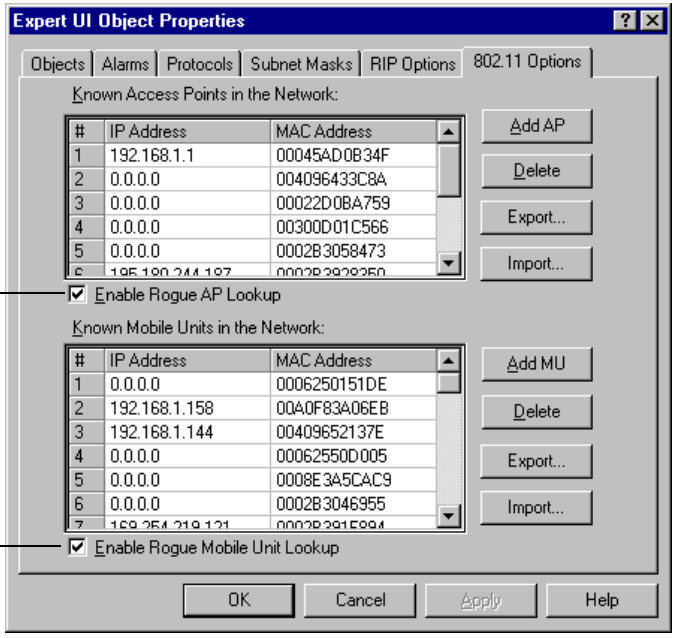


Figure 9-6. 802.11 Options Tab Settings

The **802.11 Options** tab settings let you specify how the Expert identifies rogue entities on the wireless network:

- During capture with the **Enable Rogue AP Lookup** option enabled, the Expert compares the *MAC address* (not the IP address) of each detected access point to those in the **Known Access Points in the Network** list. If the access point's MAC address is not in the list, the Expert generates the **Rogue Access Point** alarm.
- During capture with the **Enable Rogue Mobile Unit** option enabled, the Expert compares the *MAC address* (not the IP address) of each detected mobile unit to those in the **Known Mobile Units in the Network** list. If the mobile unit's MAC address is not in the list, the Expert generates the **Rogue Mobile Unit** alarm.

In addition, the Expert further identifies rogues (access points and workstations) by adding the word Rogue in parentheses following the offending stations' entries in Expert Summary and Detail displays. This provides you with a handy means of identifying units on the wireless network of which you were not aware, some of which may be unauthorized intruders.

Adding Known Addresses to the Expert's List

To use the rogue identification abilities of the Expert effectively, you must first add the MAC addresses of the known access points and mobile units on your network to the Expert's list of known wireless unit addresses. There are several ways to do this:

- Automatically from the real-time Host Table.
- Automatically from the Expert tab of the postcapture display.
- Automatically from the Address Book.
- Manually from the **802.11 Options** tab of the Expert Properties dialog box.

In addition, you can also import and export lists of known addresses (for example, if you are a Sniffer Portable user, you can import addresses from multiple Sniffer Portable installations). The following sections describe how to use each of these methods.

Adding Known Addresses from the Host Table

Use the following procedure to add the MAC addresses of known wireless units (either access points or mobile units) automatically from the Host Table during real-time monitoring.

To add known addresses automatically from the Host Table:

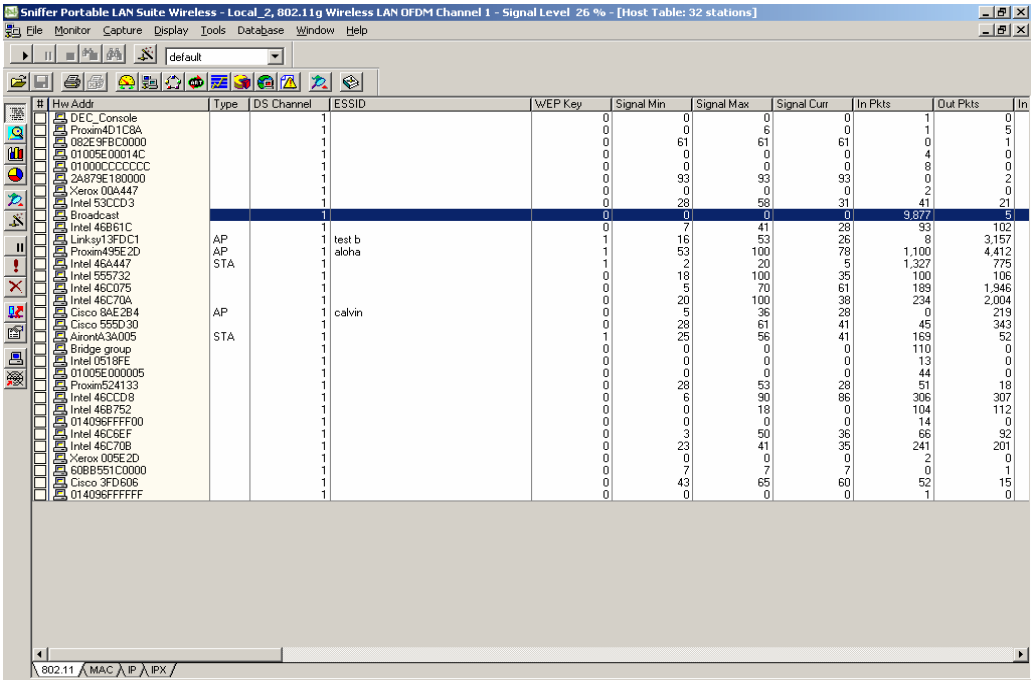
1. Open the **Monitor > Host Table** application.

   The Host Table appears. During real-time monitoring, the Host Table adds one-line entries for each detected wireless unit (access points and mobile units) on the network.

2. If the **802.11** tab is not already displayed, click its entry at the bottom of the Host Table.

3. Select which entries in the Host Table you would like to add to the Expert's list of known addresses. Select an entry by checking its corresponding box in the # column at the left of the display. You can select both access points and mobile units. The Sniffer software will add each to the appropriate list in the **Tools > Expert Options > 802.11 Options** tab.

   Figure 9-7 shows the **802.11** tab of the Host Table with sample wireless units selected in the # column.



#	Hw Addr	Type	DS Channel	ESSID	WEP Key	Signal Min	Signal Max	Signal Curr	In Pkts	Out Pkts	In
	DEC_Console		1		0	0	0	0	1	0	
	Proxim4D1C8A		1		0	0	6	0	1	5	
	082E9FBC0000		1		0	61	61	61	0	1	
	01005E00014C		1		0	0	0	0	4	0	
	010000CCCCCC		1		0	0	0	0	8	0	
	2A879E180000		1		0	93	93	93	0	2	
	Xerox 00A447		1		0	0	0	0	2	0	
	Intel 53CCD3		1		0	28	58	31	41	21	
	Broadcast		1		0	0	0	0	9,877	5	
	Intel 46B61C		1		0	7	41	28	93	102	
	Linksy13FDC1	AP	1	test b	1	16	53	26	8	3,157	
	Proxim495E2D	AP	1	aloha	1	53	100	78	1,100	4,412	
	Intel 46A447	STA	1		1	2	20	5	1,327	775	
	Intel 555732		1		0	18	100	35	100	106	
	Intel 46C075		1		0	5	70	61	189	1,946	
	Intel 46C70A		1		0	20	100	38	234	2,004	
	Cisco 8AE2B4	AP	1	calvin	0	5	36	28	0	219	
	Cisco 555D30		1		0	28	61	41	45	343	
	AirontA3A005	STA	1		1	25	56	41	169	52	
	Bridge group		1		0	0	0	0	110	0	
	Intel 0518FE		1		0	0	0	0	13	0	
	01005E000005		1		0	0	0	0	44	0	
	Proxim524133		1		0	28	53	28	51	18	
	Intel 46CCD8		1		0	6	90	86	306	307	
	Intel 46B752		1		0	0	18	0	104	112	
	014096FFFF00		1		0	0	0	0	14	0	
	Intel 46C6EF		1		0	3	50	36	66	92	
	Intel 46C708		1		0	23	41	35	241	201	
	Xerox 005E2D		1		0	0	0	0	2	0	
	60BB551C0000		1		0	7	7	7	0	1	
	Cisco 3FD606		1		0	43	65	60	52	15	
	014096FFFFFF		1		0	0	0	0	1	0	

Figure 9-7. The Host Table's 802.11 Tab

4 Right-click any entry in the Host Table and select the **Add to Known Wireless Units List** command from the context menu that appears.

The selected addresses are added to the Expert's list. You can verify that they have been added by displaying the **Tools > Expert Options > 802.11 Options** tab. The **Known...in the Network** lists will include the newly added addresses.

Adding Known Addresses from the Postcapture Display

Use the following procedure to add the MAC addresses of known wireless units (either access points or mobile units) automatically from the Expert tab of the postcapture display.

To add known addresses automatically from the postcapture display:

1 Display either a capture buffer or a saved trace file.

2 Click the **Expert** tab of the postcapture display.

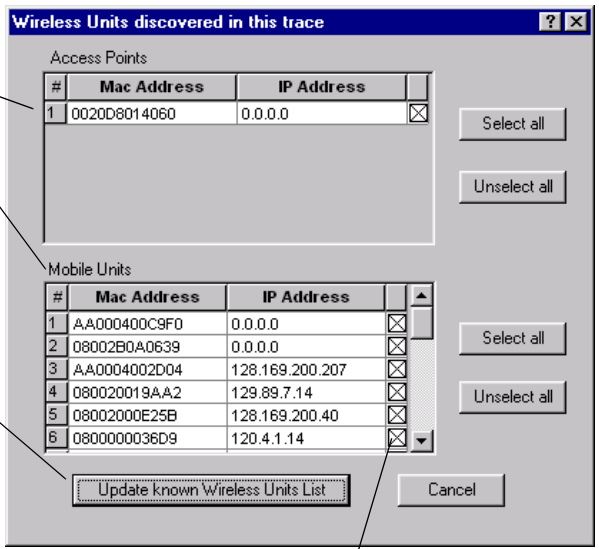
NOTE: If the Expert tab is not available, make sure the **Expert tab** option is enabled in the **Display > Display Setup > General** tab.

3 Click **Wireless Units List** at the top of the Expert pane.

The **Wireless Units Discovered in this trace** dialog box appears (Figure 9-8). This dialog box has two separate lists of wireless units discovered in the capture buffer or trace file — one for access points and one for mobile units.

NOTE: You can edit the **IP Address** field in either list. In some cases, the Expert may be unable to determine a station's IP address. In these cases, you can manually enter an IP address using this feature.

Discovered access points are listed in the upper list; discovered mobile units are listed in the lower list. IP Address fields are editable — you can enter a custom IP address.



Selected access points and mobile units will be added to the Expert list of known addresses by clicking this button.

By default, all discovered addresses are selected for addition to the Expert's list (the box at the right of each entry in the list is checked). You can select and deselect individual entries for addition or click Select All and Deselect All for faster selection.

Figure 9-8. Adding Discovered Addresses Postcapture

4 Select the access points and mobile units you would like to add to the Expert's list of known addresses by checking the checkbox at the right of each desired entry. By default, all discovered addresses are selected for addition. You can change selections in the following ways:

- By clicking **Select All** and **Unselect All**.

- By clicking in the checkbox for individual entries to toggle them between selected and unselected.

5 When you have finished selecting the addresses for addition, click **Update Known Wireless Units List** at the bottom of the dialog box.

Those selected addresses not already in the Expert's list are added. You can verify that they have been added by displaying the **Tools > Expert Options > 802.11 Options** tab. The **Known Access Points in the Network** and **Known Mobile Units in the Network** lists will include the newly added addresses.

Autodiscovering and Adding Addresses from the Address Book

The Address Book provides you with the ability to autodiscover access points and mobile units on the wireless network. Then, you can add discovered access points to the Expert's list automatically.

To autodiscover access points and add them from the Address Book:

1 Display the Address Book (**Tools > Address Book**).

2 Click **Autodiscovery**  .

3 In the Autodiscovery Options dialog box, make sure the **Discover Mobile Units** and **Discover Access Points** options are enabled.

4 Click **OK**.

Autodiscovery proceeds. Discovered addresses appear in the Address Book.

5 Click **Export AP**  in the Address Book's toolbar to add the addresses of all the access points in the Address Book to the Expert's list of known access points.

Addresses not already in the Expert's list are added. You can verify that they have been added by displaying the **Tools > Expert Options > 802.11 Options** tab. The **Known Access Points in the Network** list will include the newly added addresses.

NOTE: Clicking **Export AP** only adds those addresses in the Address Book with a **Type** value set to **Access Point**. Mobile units are not added.

Adding Known Addresses Manually in the 802.11 Options Tab

Use the following procedure to add the MAC addresses of known wireless units manually (either access points or mobile units) to the Expert's list.

To add known addresses manually in the 802.11 Options tab:

1. Display the **802.11 Options** tab of the Expert Properties dialog box by selecting the **Tools > Expert Options** command and clicking the **802.11 Options** tab in the dialog box that appears.

2. Do you want to add the address of an access point or a mobile unit?

   - To add the address of an access point, click **Add AP**.

     A new entry line becomes active in the **Known Access Points in the Network** list with the active cursor in the **MAC Address** column.

   - To add the address of a mobile unit, click **Add MU**.

     A new entry line becomes active in the **Known Mobile Units in the Network** list with the active cursor in the **MAC Address** column.

3. Enter the MAC address of the access point or mobile unit in the appropriate **MAC Address** column. You must enter the entire address in hexadecimal format. The dialog box will not let you enter an address that is not the proper length and format (twelve characters, hexadecimal only). If you do not know the full hexadecimal addresses of the access points in your network, see *Determining a Wireless Unit's Full Hexadecimal Address* on page 97.

4. Once you have entered a legal MAC address, you can also enter an IP address in the **IP Address** column. For this release, IP addresses are for your own reference only. **The Expert only compares MAC addresses when flagging wireless units as rogues**!

5. Repeat Step 2 through Step 4 for each access point or mobile unit you want to add to the Expert's list. You can enter as many addresses as you like.

6. Turn on the **Enable Rogue AP Lookup** option and/or **Enable Rogue Mobile Unit Lookup** option by checking the appropriate boxes.

7. Click **OK** in the Expert Properties dialog box.

Once you have enabled the **Rogue AP Lookup** and/or **Enable Rogue Mobile Unit Lookup** option and clicked **OK**, during subsequent captures (and openings of trace files), the Expert will compare the MAC addresses of detected access points and mobile units to those in the corresponding lists in the **802.11 Options** tab. Wireless units not found in the appropriate list will be flagged as rogues in Expert Summary and Detail displays. In addition, either the **Rogue Access Point** or **Rogue Mobile Unit** alarm will be generated for each detected rogue.

Determining a Wireless Unit's Full Hexadecimal Address

If you do not know the full hexadecimal address of a wireless unit (either an access point or a mobile unit) in your network, you should first check the unit. Often, the address is written on the equipment itself.

If this does not work, you can use the Expert's displays to discover the address. However, because most of the Expert's displays substitute textual manufacturer IDs for the first three bytes of a hexadecimal MAC address (that is, a hexadecimal address of 0020d8014060 would usually be identified in Expert displays as Netwav014060), you need to know where to look in Expert displays to find the entire address in hexadecimal.

To determine a wireless unit's full hexadecimal address:

1. Start capturing from the network containing the unit whose address you want to determine. Alternatively, you can open a trace file captured from that network.
2. In the Expert display, examine the Station Function column in the Summary pane at the Wireless layer. In this column, locate an entry for either an Access Point or a Mobile Unit. Highlight this entry.

   The Detail pane automatically updates to show statistics for the entry selected in the Summary pane.
3. In the Detail pane, scroll down to the Wireless Address field. This field shows the entire hexadecimal address of the selected unit. A textual manufacturer's ID is not substituted for the first portion of the address.
4. Repeat this procedure for each access point on the network whose full hexadecimal address you want to determine.

Importing and Exporting Known Addresses

The Sniffer software also provides export and import capabilities for the known address lists in the **Tools** > **Expert Options** > **802.11 Options** tab.

You can export the contents of either the **Known Access Points** or the **Known Mobile Units** list using the corresponding **Export** button in the **802.11 Options** tab. Exported files are saved in comma-separated values (CSV) format. The exported file consists of a heading row with the **IP Address** and **MAC Address** column headings followed by multiple data rows in the format IP Address,MAC Address. For example, a small exported CSV file might appear:

```
IP Address,MAC Address
192.168.1.40,08002000E25B
192.168.1.14,0800000036D9
192.168.1.25,080020061107
```

NOTE: MAC addresses are always presented in the CSV file in hexadecimal format.

Similarly, you can also import CSV files into the **Known Access Points** or the **Known Mobile Units** list using the corresponding **Import** button in the **802.11 Options** tab. You can import either CSV files created by exporting the lists from other Sniffer software installations, or CSV files you create yourself following the model above (that is, multiple rows in the IP Address,MAC Address format).

NOTE: You can use the **Import** and **Export** buttons together to share known address lists among multiple Sniffer software installations.

Advanced Features for Wireless Analysis 10

Overview

This chapter describes advanced features wireless analysis with the Sniffer software. Advanced features are a combination of standard Sniffer software features — network monitoring, capturing, decoding, and filtering, as well as features specifically for wireless LANs:

- The Dashboard includes counters for many different wireless LAN frame types, as well as a **Throughput** gauge measuring the bit rate of data packets. See *Dashboard Counters for Wireless Networks* on page 101.
- The Monitor's Host Table includes an **802.11** tab with entries for all detected wireless stations. Each station is listed with several wireless LAN-specific counters. See *Host Table Counters for Wireless Networks* on page 114.
- The Monitor's Global Statistics application includes a **Channel Surfing** tab with statistics for each channel in the wireless LAN. See *Global Statistics Counters for Wireless Networks* on page 118.
- The **Matrix**, **Host Table**, and **Protocol Distribution** post-analysis tabs in the Display window each include **802.11** views, allowing you to focus specifically on 802.11 statistics for wireless stations. See *Post-Analysis Views for Wireless Networks* on page 121.
- The **Statistics** post-analysis tab in the Display window includes many wireless-specific statistics. See *Post-Analysis Views for Wireless Networks* on page 121.
- The Define Filter dialog box's **Advanced** tab includes wireless LAN packet types on which you can filter (for example, **PLCP Errors**). See *Define Filter Options for Wireless Networks* on page 130.
- The Decode display can completely decode 802.11 traffic. In addition, the Sniffer software can perform WEP decryption either during capture or after capture if the correct WEP keys are specified. See *Protocol Decodes for Wireless Networks* on page 133.

- The Expert analyzer provides Expert analysis specifically for wireless stations at the **Wireless** Expert layer. In addition, the Expert can generate many wireless-specific Expert alarms. All of the usual upper layer Expert analysis is provided. See *Expert Objects and Alarms for Wireless Networks* on page 136 and *Expert Alarms for Wireless Networks* on page 146.

NOTE: During monitoring or capture, the window title bar shows the channel currently being monitored, as well as the signal strength and the type of network being monitored (802.11a or 802.11b/g). You can use this display to get a quick feel for the strength of the signal being monitored and determine whether you need to move the analyzer closer to an access point to get a stronger signal.

Differences Between Wireless Network Displays

In contrast to 802.11b networks, 802.11a and 801.11g networks support much faster data rates. Whereas 802.11b data rates range from 1 Mbps to 11 Mbps, 802.11a and 802.11g data rates range from 6 Mbps to 54 Mbps. 802.11g is backwards compatible with 802.11b because they both use the same frequency spectrum. However, 802.11a uses a different frequency spectrum than 802.11b/g. 802.11b/g works at the 2.4 to 2.4835 Ghz range and 802.11a works at the 5.15-5.835Ghz range.

The major differences between displays for 802.11 networks are related to the difference in supported rates for the 802.11a/b/g standards. For example:

- Displays containing data rate information will have more rate categories for 802.11a than they will for 802.11b/g. For example, the Host Table for 802.11b/g networks breaks out each station's traffic according to whether it was sent at 1 Mbps, 2 Mbps, 5.5 Mbps, or 11 Mbps. In contrast, the Host Table for 802.11a networks will include data rate categories for 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, 54 Mbps, 72 Mbps, and 108 Mbps (see *Notes on Proprietary Implementations of the 802.11a Standard* on page 101 for information on why there are data rate categories beyond the 54 Mbps upper limit of the 802.11a standard).
- There are more channels on an 802.11a network than there are on an 802.11b/g network. Because of this, channel-related displays (such as the **Channel Surfing** tab in the Global Statistics application) will display more channels for 802.11a than they will for 802.11b/g.

NOTE: Wireless network channels are based on geographical location and the frequency band allocated in the country.

Notes on Proprietary Implementations of the 802.11a Standard

The Proxim Harmony 802.11a adapter card used by the Sniffer software supports a proprietary extension of the 802.11a standard called **2X**. Essentially, this extension allows 802.11a networks to operate at twice the rates stated by the 802.11a specification (for example, instead of the upper limit of 54 Mbps stated for the 802.11a specification, the 2X extension theoretically allows for an upper limit of 108 Mbps).

As a consequence of this support, the Sniffer software displays for 802.11a networks will include data rate categories beyond the 54 Mbps limit claimed by the 802.11a specification. You will only see frames counted in these categories when monitoring or capturing from an 802.11a network implementing Proxim's proprietary 2X extensions.

NOTE: Turbo G or 72, 108 Mbps are currently not supported for 802.11g.

Dashboard Counters for Wireless Networks

The Dashboard for wireless networks works in the same way as the Dashboard for other networks — you display it by clicking the Dashboard icon in the Toolbar or by selecting the **Dashboard** option from the **Monitor** menu. In response, the Dashboard appears (Figure 10-1), displaying the monitored network's utilization, packet rate, error rate, and throughput (the measured data rate in bits per second) in real time.

For wireless displays, however, the Dashboard includes a number of wireless-specific counters. These counters are described in this section and are found in:

- The **Gauge** tab (see *The Dashboard's Gauge Tab* on page 104)
- The **Detail** tab (see *The Dashboard's Detail Tab* on page 104)
- The **802.11** tab (see *The Dashboard's 802.11 Tab* on page 106)
- The Dashboard Graphs (see *Dashboard Graphs for Wireless Networks* on page 111)

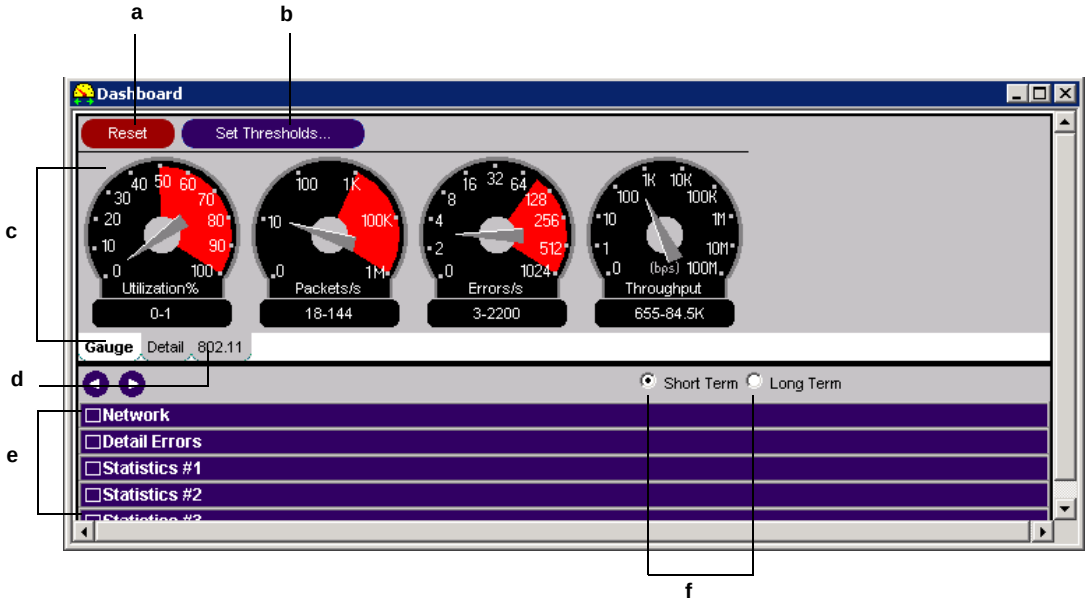


Figure 10-1. The Dashboard Gauge View

Table 10-1. Dashboard Contents

Item in Figure 10-1	Name	Description
a	Reset	Click **Reset** to reset all counters to zero.
b	Set Thresholds	Click **Set Thresholds** to set thresholds for alarms based on Dashboard statistics.
c	Gauge tab and Dashboard gauges	When the Gauge tab is selected, four 802.11- specific dashboard gauges are present: • Utilization percentage (see *How Utilization is Calculated* on page 103) • Packets per second • Errors per second • Throughput Red zones in gauges indicate the alarm threshold settings.
d	802.11 tab	Click the 802.11 tab to see wireless LAN statistics.

Table 10-1. Dashboard Contents

Item in Figure 10-1	Name	Description
e	Distribution graphs	Click (+) to expand and view configurable graphs of the corresponding statistics.
f	Short Term and Long Term options	Click these options to narrow (Short term) or widen (Long term) the scale of the Network, Detail Errors, and Size Distribution graphs.

How Utilization is Calculated

The Dashboard provides network utilization percentage measurements on both the **Gauge** and **Detail** tabs. The Sniffer software calculates network utilization by storing the airtime (in microseconds) for each observed frame in a buffer. Every second, the value in this buffer is divided by 1,000,000 microseconds (that is, a second) to obtain a percentage utilization measurement.

The airtime for each frame is calculated as follows:

1. First, the duration of the frame's PLCP header is stored. PLCP headers can be either:
   - **192 microseconds**. This is the Long header format specified in IEEE 802.11b/g for 1 and 2 Mbps wireless LANs.
   - **96 microseconds**. This is the Short header format specified in IEEE 802.11b/g for 5.5 and 11 Mbps wireless LANs.

   NOTE: The calculations for 802.11a are performed similarly except that they use the duration of the PLCP header specified for different 802.11a rates.

2. Each frame's PLCP header includes a field indicating the length of the data portion of the frame in microseconds. The Sniffer software adds this value to the duration of the PLCP header observed in the previous step and stores the sum in a buffer.
3. Each second, the value in the buffer is divided by 1,000,000 microseconds to obtain a percentage utilization measurement.

The Dashboard's Gauge Tab

The **Gauge** tab is displayed by default when you start the Dashboard. You can see the **Gauge** tab in Figure 10-1 on page 102.

When capturing from wireless networks, the Dashboard's **Gauge** tab provides a **Throughput** gauge. This gauge provides a real-time measurement of the data rate (in bits per second) observed by the Sniffer software. When calculating throughput, the Sniffer software only counts data frames. Management and control frames are not part of this calculation. However, the throughput measurement does include the header portions of data frames.

The Dashboard's Detail Tab

To view wireless Dashboard counters, click the **Detail** tab on the Dashboard. The counters shown in Figure 10-2 appear.

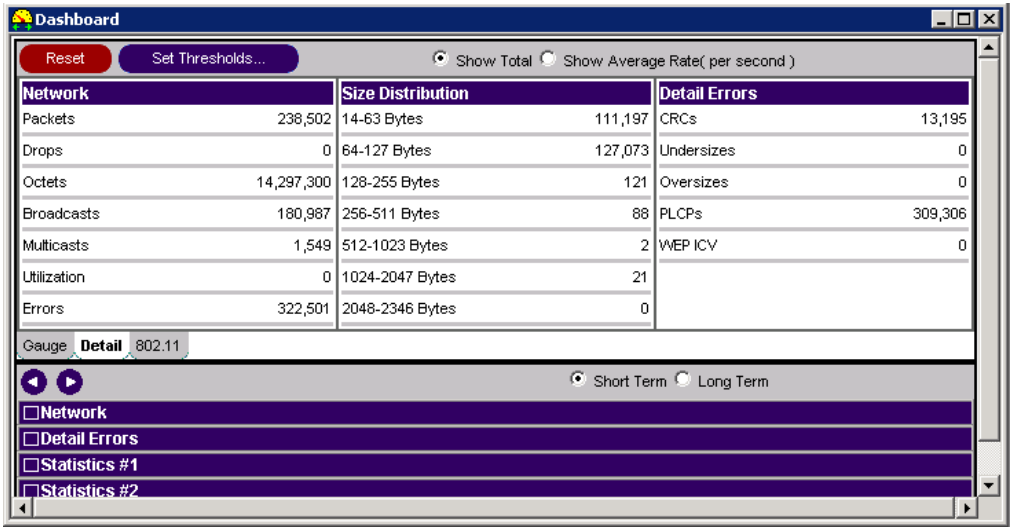


Figure 10-2. The Dashboard's Detail Tab

As you can see in Figure 10-2, in addition to the standard Dashboard **Network** and **Size Distribution** counters, the **Detail Errors** column provides counters for the wireless LAN-specific errors described in Table 10-2.

Table 10-2. Detail Error Counters in the Dashboard's Detail Tab

Counter	Description
PLCPs	The number of PLCP errors seen on the network. PLCP errors occur when a wireless station receives a Physical Layer Convergence Protocol header with an invalid checksum. Before frames are sent between wireless stations, the physical layer (PHY) sends a PLCP header to a receiving station to negotiate the size of the frames to be sent, the speed at which they should be sent, and so on. This PLCP header includes a checksum which the receiving station uses to validate that the received PLCP header is not corrupt. If this checksum is corrupt, it is considered a PLCP error.
WEP ICVs	The number of packets sent indicating an invalid WEP ICV. The Wired Equivalent Policy (WEP) is used to encrypt data sent between stations on the wireless network. When two stations exchange WEP-encrypted data, they go through an authentication sequence wherein challenge messages are encrypted and decrypted by sender and receiver. If an Integrity Check Value does not match between sender and receiver, the receiver indicates a communications failure (that is, an invalid WEP ICV).

The Dashboard's 802.11 Tab

To view wireless Dashboard statistics, click the **802.11** tab on the Dashboard. In response, the counters shown in Figure 10-3 appear.

The Dashboard's **802.11** tab includes counters for wireless LAN **Statistics**, **Management** frame types, and **Control** frame types.

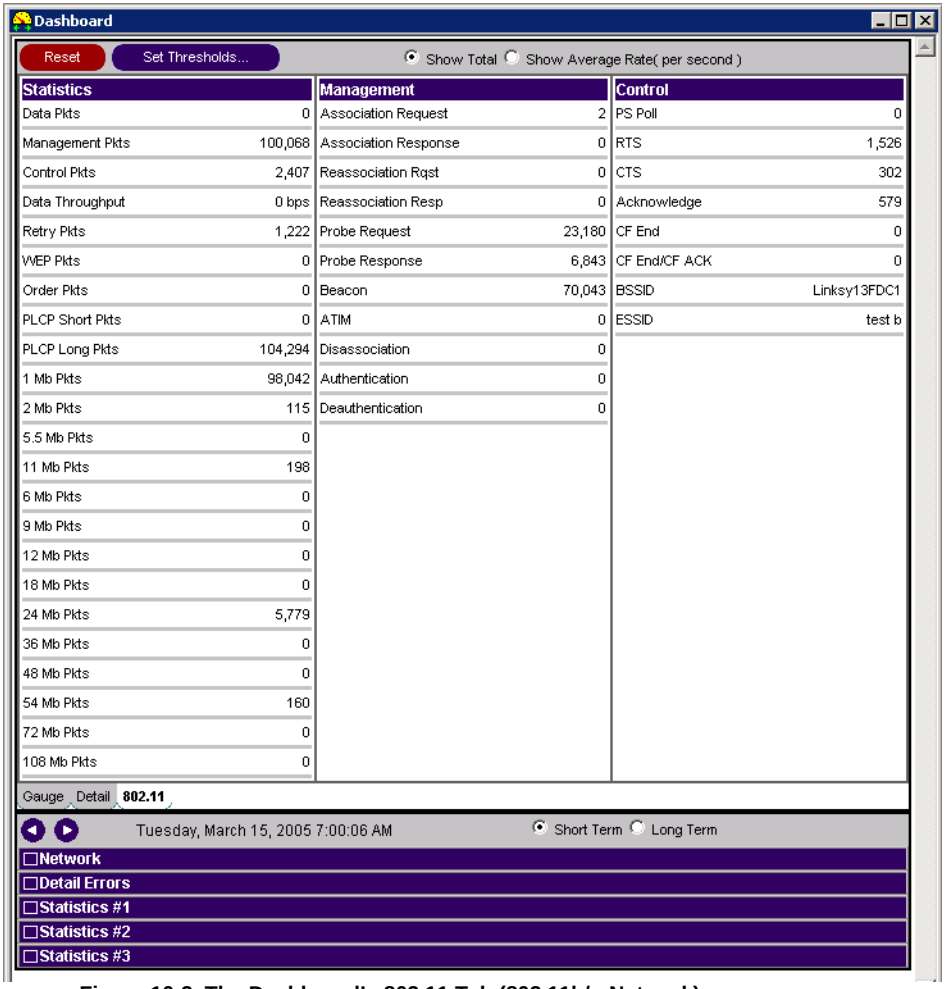


Figure 10-3. The Dashboard's 802.11 Tab (802.11b/g Network)

Statistics Counters in the 802.11 Tab

Table 10-3 lists and describes the **Statistics** counters in the Dashboard's **802.11** tab.

Table 10-3. Statistics Counters in the Dashboard's 802.11 Tab (1 of 2)

Counter	Description
Data Pkts	The number of data packets observed on the wireless LAN.
Management Pkts	The number of Management packets observed on the wireless LAN. Management packets include Association Requests, Probe Requests, and so on. They are counted individually in the **Management** column of the **802.11** tab.
Control Pkts	The number of Control packets observed on the wireless LAN. Control packets include PS Polls, CF Ends, and so on. They are counted individually in the **Control** column of the **802.11** tab.
Data Throughput	The current data rate (in bits per second) observed by the Sniffer software. When calculating throughput, the Sniffer software only counts data frames. Management and control frames are not part of this calculation. However, the throughput measurement does include the header portions of data frames.
Retry Pkts	The number of Retry packets observed on the wireless LAN. Stations send retry packets when they receive no acknowledgment to a previously sent packet.
WEP Pkts	The number of packets observed on the wireless LAN with the WEP bit in the Frame Control field set to true. This indicates that Wired Equivalent Policy encryption was used on the packet.
Order Pkts	The number of packets observed on the wireless LAN with the Order bit in the Frame Control field set to true. This indicates that packets must be processed in order.
PLCP Short Pkts	The number of Physical Layer Convergence Protocol (PLCP) protocol data units seen with the "short" preamble and header. This form of PLCP PDU is used to achieve higher throughput and can support 5.5 and 11 Mbps transmission speeds.

Table 10-3. Statistics Counters in the Dashboard's 802.11 Tab (2 of 2)

Counter	Description
PLCP Long Pkts	The number of PLCP PDUs seen with the "long" preamble and header. This form of PLCP PDU is compatible with legacy equipment from older wireless LANs and supports and operates at either 1 Mbps or 2 Mbps.
Data Rate Counters	These counters vary depending on the monitored network: • For 802.11b/g networks, there are separate counters for the number of frames sent at 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54, 72, 108 Mbps. • For 802.11a networks, there are separate counters for the number of frames sent at 6, 9, 12, 18, 24, 36, 48, 54, 72, and 108 Mbps. • For legacy 802.11b cards, the speeds remain at 1, 2, 5.5, 11 Mbps. **NOTE:** 802.11g is backward-compatible with 802.11b, therefore the speed counters seen in 802.11b are also shown in 802.11g. 802.11b and 802.11g share the same frequency band (2.4 GHz) and same number of channels (1-14). 802.11b goes from speeds 1 Mbps to 11 Mbps and 802.11g goes from speeds 1 Mbps to 54 Mbps. 802.11a and 802.11g share similar speeds (6, 9, 12, 18, 24, 36, 48, 54, 72, and 108 Mbps – 72 and 108 Mbps are proprietary implementations).

Management Frame Type Counters in the 802.11 Tab

Management frames are used to set up the initial communications between stations and access points on the wireless network. Table 10-4 lists and describes the **Management** frame counters in the Dashboard's **802.11** tab.

Table 10-4. Management Frame Counters in the Dashboard's 802.11 Tab (1 of 3)

Counter	Description
Association Requests	The number of Association Requests observed on the wireless network. Stations send Association Requests to become associated with access points.

Table 10-4. Management Frame Counters in the Dashboard's 802.11 Tab (2 of 3)

Counter	Description
Association Responses	The number of Association Responses observed on the wireless network. Access points send Association Responses in response to Association Requests from wireless stations.
Reassociation Requests	The number of Reassociation Requests observed on the wireless network. Stations send Reassociation Requests when they need to associate with a new access point (for example, because they are out of range of their old access point). This way, the new access point knows to set up forwarding of traffic from the old access point.
Reassociation Responses	The number of Reassociation Responses observed on the wireless network. Access points send Reassociation Responses in response to Reassociation Requests from wireless stations.
Probe Requests	The number of Probe Requests observed on the wireless network. Stations send Probe Requests to other stations or access points to retrieve information (for example, to determine whether a given access point is open for new associations).
Probe Responses	The number of Probe Responses observed on the wireless network. Stations and access points send Probe Responses containing requested parameters in response to Probe Requests.
Beacons	The number of Beacon packets observed on the wireless network. Access points send beacon packets at a regular interval to synchronize timing between stations on the same network.
ATIMs	The number of Announcement Traffic Indication Messages (ATIMs) observed on the wireless network. Stations send ATIMs immediately after a beacon packet transmission to inform other stations that they have data to transmit to them.
Disassociations	The number of Disassociation packets observed on the wireless network. Stations and access points send Disassociations to end associations.

Table 10-4. Management Frame Counters in the Dashboard's 802.11 Tab (3 of 3)

Counter	Description
Authentications	The number of Authentication packets observed on the wireless network. Stations and access points send Authentications to identify one another securely.
Deauthentications	The number of Deauthentication packets observed on the wireless network. Stations and access points send Deauthentications to end secure communications with one another.

Control Frame Type Counters in the 802.11 Tab

Once stations and access points on the wireless networks have established communications with one another (through the Association and Authentication packet types described in the previous section), Control frames are used in the transmission of data frames. Table 10-5 lists and describes the **Control** frame counters in the Dashboard's **802.11** tab.

Table 10-5. Control Frame Counters in the Dashboard's 802.11 Tab (1 of 2)

Counter	Description
PS Polls	The number of Power Save (PS) Poll packets observed on the wireless network. PS Poll packets are sent by stations to inform other stations of time windows during which they will not be transmitting.
RTS	The number of Request to Send (RTS) packets observed on the wireless network. RTS packets are sent by stations to negotiate how a data frame will be sent.
CTS	The number of Clear to Send (CTS) packets observed on the wireless network. Stations send CTS packets to acknowledge the receipt of an RTS packet and to indicate that they are ready to receive data.
Acknowledge	The number of Acknowledge packets observed on the wireless network. Stations send acknowledge packets to indicate that they have received an error-free packet.
CF End	The number of Contention-Free (CF) End packets observed on the wireless network. CF End packets are sent to indicate the end of a contention period.

Table 10-5. Control Frame Counters in the Dashboard's 802.11 Tab (2 of 2)

Counter	Description
CF End/CF ACK	CF End/CF ACK packets are sent to acknowledge CF End packets.
BSSID	The Basic Service Set Identification (BSSID) for the access point on the channel being monitored.
ESSID	The Extended Service Set Identification (ESSID) for the channel being monitored.

Dashboard Graphs for Wireless Networks

The Dashboard for wireless networks also provides configurable graphs for each of the following groups of statistics:

- Network statistics
- Detail Errors
- Statistics #1
- Statistics #2
- Statistics #3 is present if an 802.11 a/b/g card is used

NOTE: Each of the statistics found in these graphs can also be found in the **Detail** or **802.11** tabs at the top of the Dashboard. See the previous sections for descriptions of the various statistics.

You work with the Dashboard graphs for wireless networks in the same way you work with all Dashboard graphs — by clicking the box corresponding to the desired group of statistics at the bottom of the Dashboard (item a, Figure 10-4). A graph appears at the bottom of the Dashboard showing the selected statistics.

Figure 10-4 shows a sample of the Detail Errors graph for wireless networks.

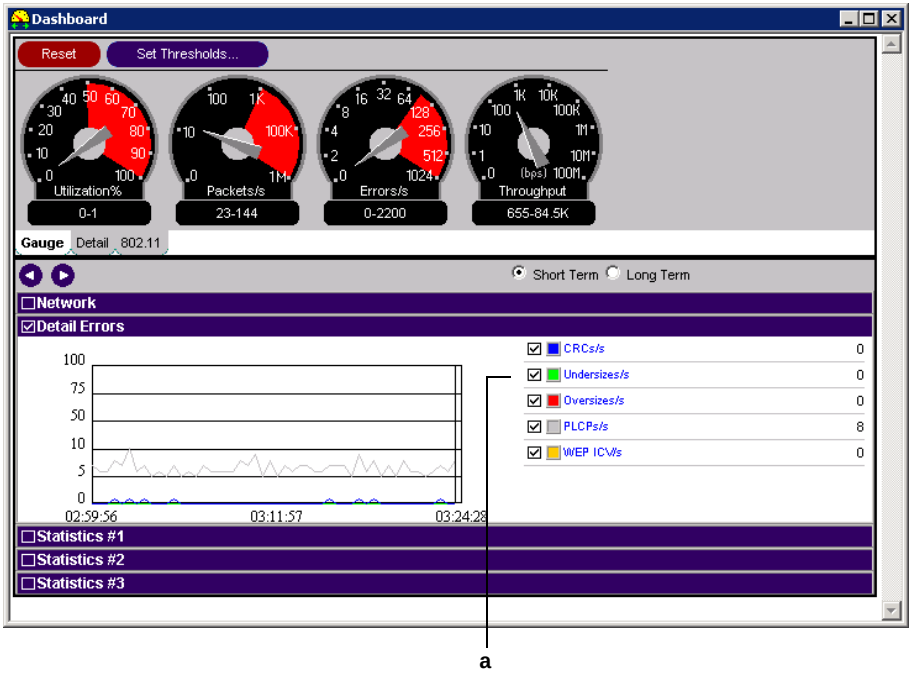


Figure 10-4. Configurable Dashboard Graph

Working with the Dashboard Graphs

You work with the configurable graphs as follows:

- Each possible statistic for the graphs is listed at the right of the graph. Check the boxes of the statistics you would like included in the graph. A line in the corresponding color will appear in the graph for the selected statistic.
- If you are having difficulty viewing the line for a particular statistic, allow your mouse to hover over the entry for the statistic at the right of the graph. The corresponding line will appear in bold in the graph while your mouse is hovering over its entry at the right.
- The graph includes a vertical “current” line. The statistics counters at the right of the graph are based on the position of the “current line.” You can move the current line in either of the following ways:
  - Clicking the arrow buttons at the top of the graph.
  - Clicking to the right or the left of the “current” line in the graph.

  The time and date entry at the top of the graph shows the current position of the “current” line.

- You can widen or narrow the time scale of the graph by clicking the **Long term** (widen) or **Short term** (narrow) buttons at the top of the graph.
- You can reset the statistics in the Dashboard (including the graphs) by clicking **Reset** at the top of the Dashboard.

Setting Thresholds for the Dashboard Statistics

You can set alarm thresholds for each of the dials on the Dashboard (as well as many other network statistics). When a threshold is exceeded, an entry is made in the Alarm log. You can monitor the Alarm log to keep watch over your network.

To set a threshold value, click the **Set Thresholds** button at the top of the Dashboard (*Figure 10-4*). Alternatively, you can select **Options** from the **Tools** menu and click the **Mac Threshold** tab.

You will see a complete list of network parameters that can trigger a threshold alarm. The exact parameters depend on the currently selected adapter. Figure 10-5 shows the network parameters for a Wireless LAN adapter.

The High Threshold value for each measure will be the average per second value measured during the monitor sampling interval

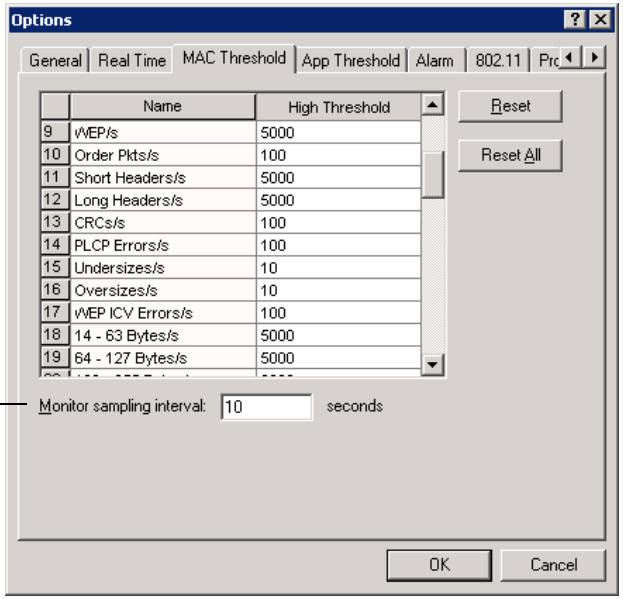


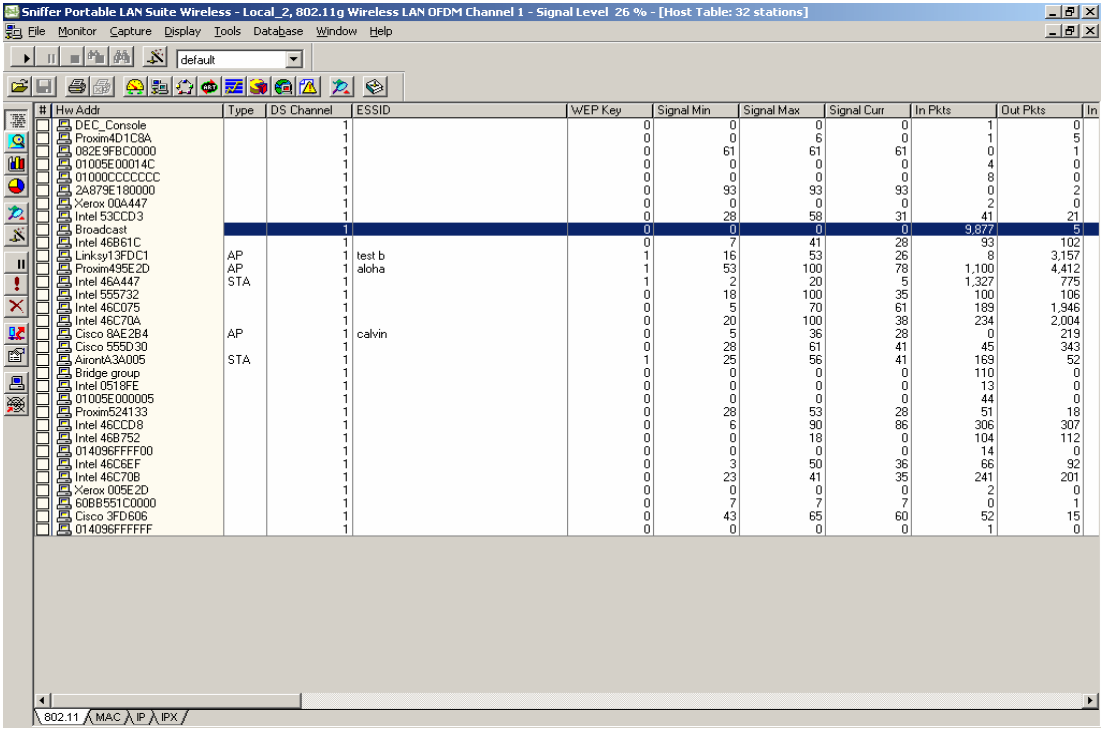
Figure 10-5. Setting Threshold Options

Host Table Counters for Wireless Networks

The Host Table for wireless networks works in the same way as the Host Table for other networks — you display it by clicking the Host Table icon in the Toolbar or by selecting the **Host Table** option from the **Monitor** menu. In response, the Host Table appears (Figure 10-6), displaying real-time network traffic statistics for each detected station.

NOTE: You can add the entries in the Host Table to the Expert's list of known access points and mobile units by clicking in the # column to select individual entries, right-clicking, and selecting the **Add to Known Wireless Units List** command from the menu that appears. The Expert uses this list to generate **Rogue Access Point** and **Rogue Mobile Unit** alarms (detected stations whose addresses are not in the list result in **Rogue** alarms). See *Setting Expert Wireless Options* on page 90 for details.

In addition to the standard Host Table features available for all networks, The Sniffer software adds a **802.11** tab with counters specifically for MAC-layer wireless stations. You can see these counters in Figure 10-6.



#	Hw Addr	Type	DS Channel	ESSID	WEP Key	Signal Min	Signal Max	Signal Curr	In Pkts	Out Pkts	In
	DEC_Console		1		0	0	0	0	1	0	
	Proxim4D1C8A		1		0	0	6	0	1	5	
	082E9FBC0000		1		0	61	61	61	0	1	
	01005E00014C		1		0	0	0	0	4	0	
	01000CCCCCCC		1		0	0	0	0	8	0	
	2A879E180000		1		0	93	93	93	0	2	
	Xerox 00A447		1		0	0	0	0	2	0	
	Intel 53CCD3		1		0	28	58	31	41	21	
	Broadcast		1		0	0	0	0	9,877	5	
	Intel 46B61C		1		0	7	41	28	93	102	
	Linksy13FDC1	AP	1	test b	1	16	53	26	8	3,157	
	Proxim495E2D	AP	1	aloha	1	53	100	78	1,100	4,412	
	Intel 46A447	STA	1		1	2	20	5	1,327	775	
	Intel 555732		1		0	18	100	35	100	106	
	Intel 46C075		1		0	5	70	61	189	1,946	
	Intel 46C70A		1		0	20	100	38	234	2,004	
	Cisco 8AE2B4	AP	1	calvin	0	5	36	28	0	219	
	Cisco 555D30		1		0	28	61	41	45	343	
	AirontA3A005	STA	1		1	25	56	41	169	52	
	Bridge group		1		0	0	0	0	110	0	
	Intel 0518FE		1		0	0	0	0	13	0	
	01005E000005		1		0	0	0	0	44	0	
	Proxim524133		1		0	28	53	28	51	18	
	Intel 46CCD8		1		0	6	90	86	306	307	
	Intel 46B752		1		0	0	18	0	104	112	
	014096FFFF00		1		0	0	0	0	14	0	
	Intel 46C6EF		1		0	3	50	36	66	92	
	Intel 46C70B		1		0	23	41	35	241	201	
	Xerox 005E2D		1		0	0	0	0	2	0	
	60BB551C0000		1		0	7	7	7	0	1	
	Cisco 3FD606		1		0	43	65	60	52	15	
	014096FFFFFF		1		0	0	0	0	1	0	

Figure 10-6. The Host Table's 802.11 Tab

You display the Host Table's **802.11** tab by clicking it at the bottom of the Host Table window. For each MAC-layer wireless station detected on the network, the **802.11** tab provides the statistics listed and described in Table 10-6.

Table 10-6. Host Table Counters in the 802.11 Tab (1 of 4)

Counter	Description
HwAddr	The hardware address for this station.
Type	The type of station. Station types include: • AP — Access Point. • STA — Wireless Station.
In Pkts	The number of packets received by this station.
Out Pkts	The number of packets transmitted by this station.
In Bytes	The number of bytes received by this station.
Out Bytes	The number of bytes transmitted by this station.
Broadcast	The number of broadcast packets transmitted by this station.
Multicast	The number of multicast packets transmitted by this station.
Retry Pkts	The number of retry packets transmitted by this station. Stations send retry packets when they receive no acknowledgment to a previously sent packet.

Table 10-6. Host Table Counters in the 802.11 Tab (2 of 4)

Counter	Description
Data Rate Counters	These counters vary depending on the monitored network: • For 802.11b/g networks, there are separate counters for the number of frames sent at 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54, 72, 108 Mbps. • For 802.11a networks, there are separate counters for the number of frames sent at 6, 9, 12, 18, 24, 36, 48, 54, 72, and 108 Mbps. • For legacy 802.11b cards, the speeds remain at 1, 2, 5.5, 11 Mbps. **NOTE:** 802.11g is backward-compatible with 802.11b, therefore the speed counters seen in 802.11b are also shown in 802.11g. 802.11b and 802.11g share the same frequency band (2.4 GHz) and same number of channels (1-14). 802.11b goes from speeds 1 Mbps to 11 Mbps and 802.11g goes from speeds 1 Mbps to 54 Mbps. 802.11a and 802.11g share similar speeds (6, 9, 12, 18, 24, 36, 48, 54, 72, and 108 Mbps – 72 and 108 Mbps are proprietary implementations).
Beacons	The number of beacon packets transmitted by this station. Access points send beacon packets at a regular interval to synchronize timing between stations on the same network.
Out Errors	The number of error packets transmitted by this station. Error packets include CRC errors, undersize errors, oversize errors, WEP ICV errors, and PLCP errors.
CRC	The number of packets with CRC errors sent by this station.
Undersize	The number of packets with undersize errors sent by this station.
Oversize	The number of packets with oversize errors sent by this station.

Table 10-6. Host Table Counters in the 802.11 Tab (3 of 4)

Counter	Description
WEP ICV	The number of packets with WEP ICV errors sent by this station. The Wired Equivalent Policy (WEP) is used to encrypt data sent between stations on the wireless network. When two stations exchange WEP-encrypted data, they go through an authentication sequence wherein challenge messages are encrypted and decrypted by sender and receiver. If an Integrity Check Value does not match between sender and receiver, the receiver indicates a communications failure (that is, a WEP ICV error).
DS Channel	The wireless network channel on which this station was last seen transmitting.
ESSID	The Extended Service Set ID to which this station was last seen belonging.
WEP Key	The last Wired Equivalent Policy key seen used by this station. Each wireless station supporting WEP encryption is programmed with four different WEP keys it can use to encrypt data. Possible values for this counter are: • **0** – This station has not sent a WEP-encrypted packet. • **1** – The last WEP-encrypted packet seen from this station was encrypted with WEP key number 1. • **2** – The last WEP-encrypted packet seen from this station was encrypted with WEP key number 2. • **3** – The last WEP-encrypted packet seen from this station was encrypted with WEP key number 3. • **4** – The last WEP-encrypted packet seen from this station was encrypted with WEP key number 4.
Signal Min	Of the measured signal strengths for this station, the lowest (expressed as a percentage).
Signal Max	Of the measured signal strengths for this station, the highest (expressed as a percentage).
Signal Curr	The average of all measured signal strengths for this station.

Table 10-6. Host Table Counters in the 802.11 Tab (4 of 4)

Counter	Description
Update Time	The last time this station was updated in the Host Table with new statistics.
Create Time	The time this station's entry was first added to the Host Table.

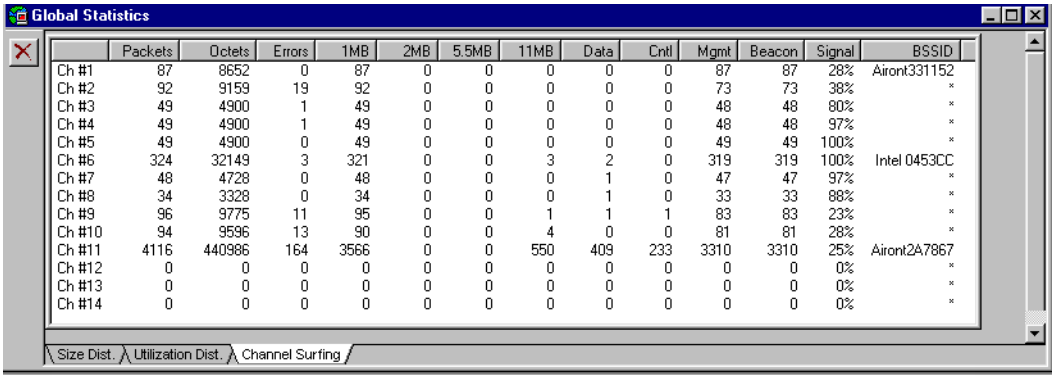
Global Statistics Counters for Wireless Networks

The Monitor's Global Statistics application for wireless networks works in the same way as Global Statistics for other networks — you display it by clicking the Global Statistics icon in the Toolbar or by selecting the **Global Statistics** option from the **Monitor** menu. In response, the Global Statistics window appears (Figure 10-7), displaying real-time network statistics to help you with traffic analysis.

In addition to the standard Global Statistics tabs available for all networks, the Sniffer software adds a **Channel Surfing** tab. The **Channel Surfing** tab provides you with a quick snapshot of network activity on all the channels in the wireless network. Each channel is listed in the display with the same sets of statistics, enabling you to see at a glance what is happening on each channel.

NOTE: The **Channel Surfing** tab will appear differently depending on whether the monitored network is 802.11a or 802.11b/g. The **Channel Surfing** tab for 802.11a networks will display more channels and data rates than the one for 802.11b/g.

IMPORTANT: When you use the **Channel Surfing** tab, be sure to enable the **Channel Surfing** option in the **Tools > Options > 802.11** tab. This option causes the Sniffer software to cycle between monitoring selected channels for specified durations. Channel surfing statistics will only be available for channels selected in the **802.11** tab in the Options dialog box. For more information on setting up Channel Surfing options, see *Setting Configuration Options* on page 83.



	Packets	Octets	Errors	1MB	2MB	5.5MB	11MB	Data	Cntl	Mgmt	Beacon	Signal	BSSID
Ch #1	87	8652	0	87	0	0	0	0	0	87	87	28%	Aironf331152
Ch #2	92	9159	19	92	0	0	0	0	0	73	73	38%	*
Ch #3	49	4900	1	49	0	0	0	0	0	48	48	80%	*
Ch #4	49	4900	1	49	0	0	0	0	0	48	48	97%	*
Ch #5	49	4900	0	49	0	0	0	0	0	49	49	100%	*
Ch #6	324	32149	3	321	0	0	3	2	0	319	319	100%	Intel 0453CC
Ch #7	48	4728	0	48	0	0	0	1	0	47	47	97%	*
Ch #8	34	3328	0	34	0	0	0	1	0	33	33	88%	*
Ch #9	96	9775	11	95	0	0	1	1	1	83	83	23%	*
Ch #10	94	9596	13	90	0	0	4	0	0	81	81	28%	*
Ch #11	4116	440986	164	3566	0	0	550	409	233	3310	3310	25%	Aironf2A7867
Ch #12	0	0	0	0	0	0	0	0	0	0	0	0%	*
Ch #13	0	0	0	0	0	0	0	0	0	0	0	0%	*
Ch #14	0	0	0	0	0	0	0	0	0	0	0	0%	*

Figure 10-7. The Global Statistics Application's Channel Surfing Tab (802.11b/g Network)

You display the Global Statistics application's **Channel Surfing** tab by clicking it at the bottom of the Global Statistics window. For each channel on the wireless network, the **Channel Surfing** tab provides the statistics listed and described in Table 10-7.

Table 10-7. Counters in the Channel Surfing Tab (1 of 2)

Counter	Description
Packets	The number of packets seen on this channel.
Octets	The number of bytes seen on this channel.
Errors	The number of error packets seen on this channel. Error packets include CRC errors, undersize errors, oversize errors, WEP ICV errors, and PLCP errors.

Table 10-7. Counters in the Channel Surfing Tab (2 of 2)

Counter	Description
Data Rate Counters	These counters vary depending on the monitored network: • For 802.11b/g networks, there are separate counters for the number of frames sent at 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54, 72, 108 Mbps. • For 802.11a networks, there are separate counters for the number of frames sent at 6, 9, 12, 18, 24, 36, 48, 54, 72, and 108 Mbps. • For legacy 802.11b cards, the speeds remain at 1, 2, 5.5, 11 Mbps. **NOTE:** 802.11g is backward-compatible with 802.11b, therefore the speed counters seen in 802.11b are also shown in 802.11g. 802.11b and 802.11g share the same frequency band (2.4 GHz) and same number of channels (1-14). 802.11b goes from speeds 1 Mbps to 11 Mbps and 802.11g goes from speeds 1 Mbps to 54 Mbps. 802.11a and 802.11g share similar speeds (6, 9, 12, 18, 24, 36, 48, 54, 72, and 108 Mbps – 72 and 108 Mbps are proprietary implementations).
Data	The number of data packets seen on this channel. Data packets are used to transmit data between stations.
Cntl	The number of Control Packets seen on this channel. Control packets are used to regulate the transmission of data packets after initial authentication has taken place.
Mgmt	The number of Management Packets seen on this channel. Management packets are used to set up the initial communications between stations and access points on the wireless network.
Beacon	The number of beacon packets seen on this channel. Access points send beacon packets at a regular interval to synchronize timing between stations on the same network.
Signal	The signal strength measured for this channel, expressed as a percentage.
BSSID	The Basic Service Set ID used for communications on this channel.

Post-Analysis Views for Wireless Networks

When you display the contents of the capture buffer or a capture file, the Sniffer software interprets and decodes the higher-level protocols within the captured packets using its *protocol interpreters*.

You can display the decoded packets in a variety of formats. Each format appears on a tab at the bottom of the Display window. In addition to the standard information provided in each of these tabs, the Sniffer software adds special 802.11 information to the following tabs, allowing you to concentrate on statistics specifically for wireless stations:

- **Matrix** tab (see *802.11 View in the Post-Analysis Matrix Tab* on page 121)
- **Host Table** tab (see *802.11 View in the Post-Analysis Host Table Tab* on page 123)
- **Protocol Distribution** tab (see *802.11 View in the Post-Analysis Protocol Distribution Tab* on page 125)
- **Statistics** Tab (see *802.11 Information in the Post-Analysis Statistics Tab* on page 127)

NOTE: The Matrix, Host Table, and Protocol Distribution tabs appear at the bottom of the Display window *only* if the **Post analysis tabs** box is checked on the **General** tab of the **Display Setup** dialog box.

NOTE: The post-analysis tabs described in this section all count various 802.11 frame types. The purposes of these frame types in an 802.11 network are all described in the *Dashboard Counters for Wireless Networks* on page 101. See that section if you have a question about a particular frame type.

802.11 View in the Post-Analysis Matrix Tab

The **Matrix** tab collects statistics for conversations between network nodes. In addition to the standard MAC, IP, and IPX views present for all networks, the Sniffer software provides an additional 802.11 view that allows you to concentrate on information specifically for wireless stations.

NOTE: In this release, the Matrix view also includes an 802.11 view during real-time monitoring.

You display the 802.11 view by clicking the **Matrix** tab at the bottom of the Display window and then selecting the 802.11 option from the drop-down list at the upper left of the window. The 802.11 view appears as shown in Figure 10-8 (in this case, with the traffic map shown).

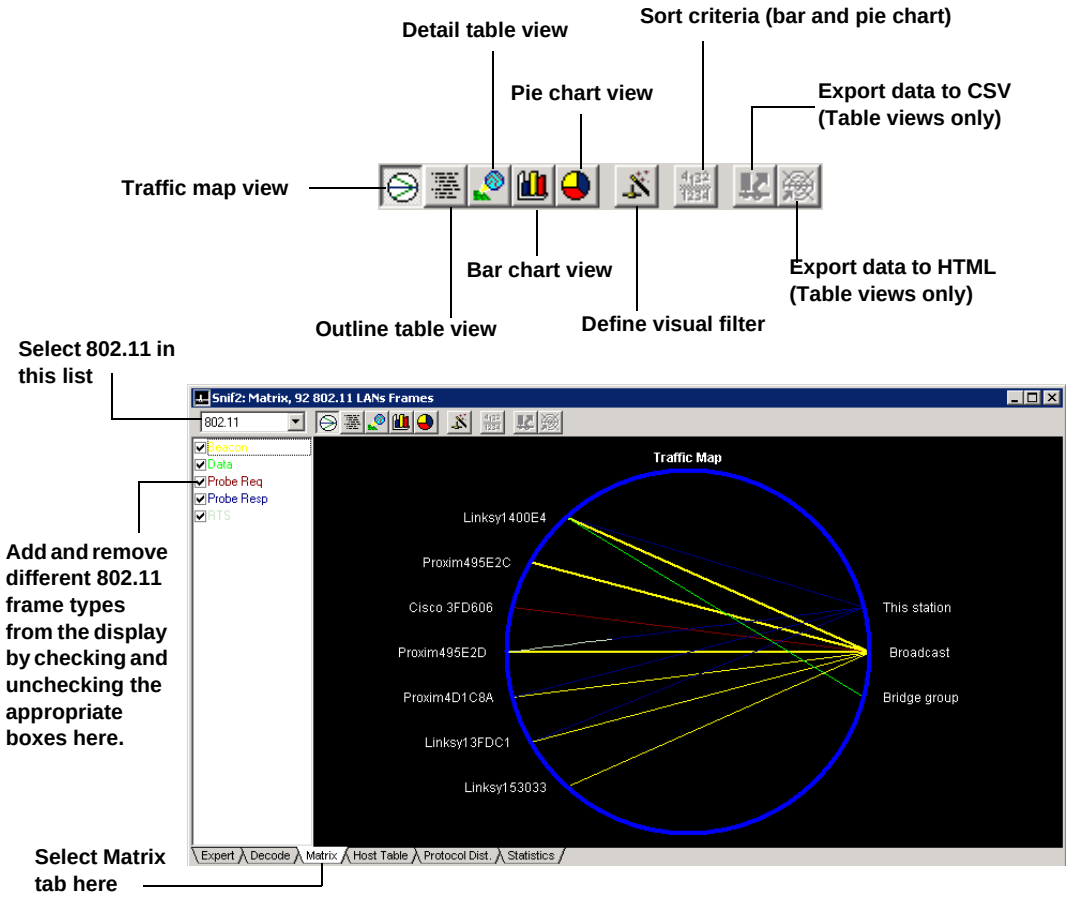


Figure 10-8. The 802.11 View in the Post-Analysis Matrix Tab

You can view accumulated 802.11 data as a traffic map, as a table, or as a bar or pie chart.

- The *traffic map* provides a birds-eye view of network traffic patterns between nodes. You can filter out unwanted traffic by unchecking certain 802.11 frame types at the left of the window.
- The *matrix tables* display traffic count statistics for node pairs:

- The *outline table* provides a quick summary of total bytes and packets transmitted between pairs of network nodes. You can also cascade each entry in the table open to see counts of various types of 802.11 frames sent by each station.
- The *detail table* provides a quick summary of the 802.11 frame types transmitted by each conversation node pair.

You can sort a matrix table by clicking a column heading (for example, to sort the statistics by packets, click the **Packets** column heading). Click a second time to sort in reverse order.

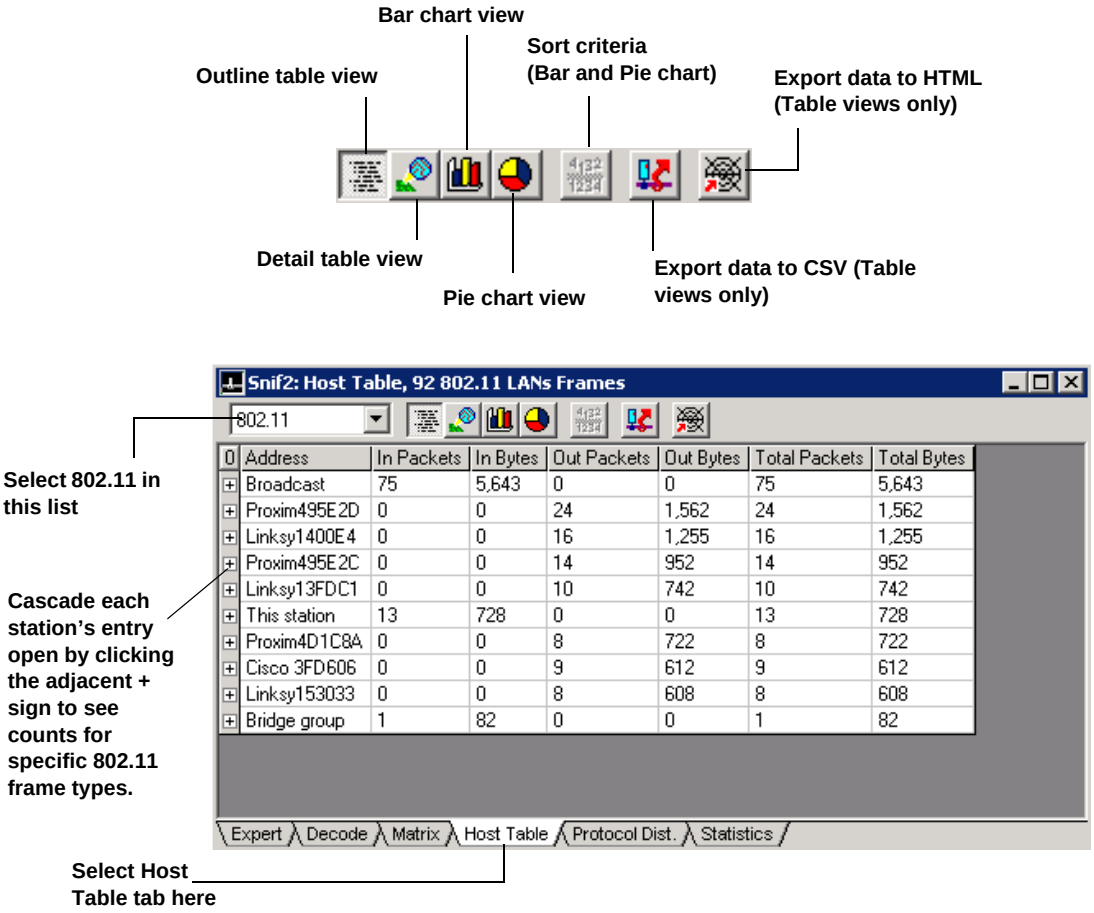
- The *bar chart* displays the busiest conversation node pairs by total bytes transmitted.
- The *pie chart* displays the busiest conversation node pairs as relative percentages of the total load of traffic (measured in bytes).

In the table views, you can export the statistics for tabulation or charting.

802.11 View in the Post-Analysis Host Table Tab

The **Host Table** tab collects each network node's traffic statistics. In addition to the standard MAC, IP, and IPX views present for all networks, the Sniffer software provides an additional 802.11 view that allows you to concentrate on traffic statistics specifically for wireless stations.

You display the 802.11 view by clicking the **Host Table** tab at the bottom of the Display window and then selecting the 802.11 option from the drop-down list at the upper left of the window. The 802.11 view appears as shown in Figure 10-9 (in this case, with the outline table shown).



0	Address	In Packets	In Bytes	Out Packets	Out Bytes	Total Packets	Total Bytes
+	Broadcast	75	5,643	0	0	75	5,643
+	Proxim495E2D	0	0	24	1,562	24	1,562
+	Linksy1400E4	0	0	16	1,255	16	1,255
+	Proxim495E2C	0	0	14	952	14	952
+	Linksy13FDC1	0	0	10	742	10	742
+	This station	13	728	0	0	13	728
+	Proxim4D1C8A	0	0	8	722	8	722
+	Cisco 3FD606	0	0	9	612	9	612
+	Linksy153033	0	0	8	608	8	608
+	Bridge group	1	82	0	0	1	82

Figure 10-9. The 802.11 View in the Post-Analysis Host Table Tab

You can view accumulated data as a table, bar chart, or pie chart.

- The *table* views display traffic count statistics for each network node.
  - The *outline table* provides a quick summary of total bytes and packets transmitted in and out of each network node. You can also cascade each entry in the table open to see counts of various types of 802.11 frames sent by each station.
  - The *detail table* provides a quick summary of the higher layer protocol type and its traffic load transmitted in and out of each network node.

You can sort a host table by clicking a column heading (for example, to sort the statistics by incoming packets, click the **In Pkts** column heading). Click a second time to sort in reverse order.

- The *bar chart* displays the busiest wireless stations by bytes transmitted.
- The *pie chart* displays the busiest wireless stations as relative percentages of the total load of traffic.

In the table views, you can export the statistics for tabulation or charting.

802.11 View in the Post-Analysis Protocol Distribution Tab

The **Protocol Distribution** tab reports network usage by protocol. In addition to the standard views for MAC, IP, and IPX protocols, the Sniffer software provides an additional 802.11 view that allows you to view network usage by 802.11 frame types (for example, Association Requests, Probe Requests, Beacons, and so on).

You display the 802.11 view by clicking the **Protocol Dist** tab at the bottom of the Display window and then selecting the 802.11 option from the drop-down list at the upper left of the window. The 802.11 view appears as shown in Figure 10-10 (in this case, with the bar chart shown).

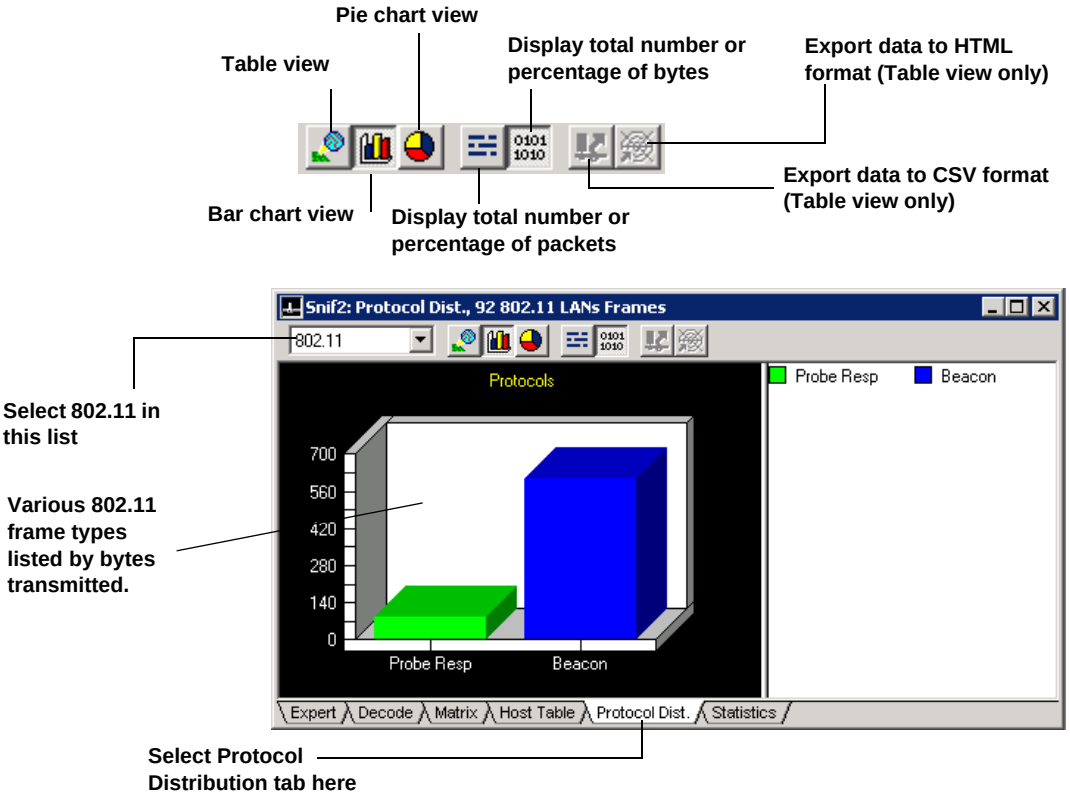


Figure 10-10. The 802.11 View in the Post-Analysis Protocol Distribution Tab

You can view accumulated data as a table, bar chart, or pie chart.

- The *table* view lists each 802.11 frame type detected along with the total number of packets and bytes of that frame type seen.

  You can sort the table by clicking a column heading (for example, to sort the statistics by number of packets, click the **Packets** column heading). Click a second time to sort in reverse order.

- The *bar chart* displays 802.11 frame types seen by bytes or packets transmitted (as selected in the toolbar; see Figure 10-10).

- The *pie chart* displays the 802.11 frame types seen as relative percentages of the total load of traffic.

In the table views, you can export the statistics for tabulation or charting.

802.11 Information in the Post-Analysis Statistics Tab

For each capture session, the Sniffer software accumulates statistical information to help you analyze the network traffic during the capture period. A summary of this information is displayed in a table on the **Statistics** tab (Figure 10-11) in the post-analysis Display window. The table displays:

- The date and time of the capture
- The amount of traffic seen during the capture period
- Utilization statistics

In addition to the standard counters on the **Statistics** tab, the Sniffer software adds a variety of wireless-specific statistics. These statistics are listed and described in Table 10-8 on page 128.

You can export the information in the **Statistics** tab to a CSV file (importable by spreadsheets and other applications) using the button, or to an HTML file using the button.

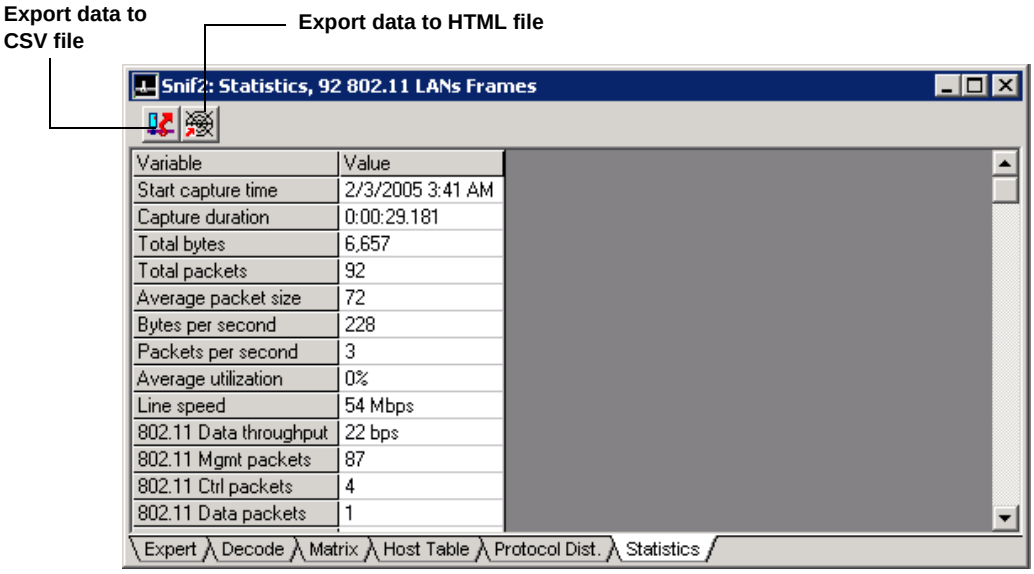


Figure 10-11. The Statistics Tab

Table 10-8. 802.11 Counters in the Statistics Tab (1 of 2)

Counter	Description
802.11 Data Throughput	The data rate (in bits per second) observed by the Sniffer software for this capture session. When calculating throughput, the Sniffer software only counts data frames. Management and control frames are not part of this calculation. However, the throughput measurement does include the header portions of data frames.
802.11 Management Pkts	The number of Management packets observed on the wireless LAN during this capture session.
802.11 Control Pkts	The number of Control packets observed on the wireless LAN during this capture session.
802.11 Data Packets	The number of data packets observed on the wireless LAN during this capture session.
802.11 Mgmt Pkt Util	Of the total number of MAC layer frames observed during this session, the percentage that were Management packets.
802.11 Ctrl Pkt Util	Of the total number of MAC layer frames observed during this session, the percentage that were Control packets.
802.11 Data Pkt Util	Of the total number of MAC layer frames observed during this session, the percentage that were Data packets.
802.11 Retry Pkts	The number of Retry packets observed on the wireless LAN during this capture session. Stations send retry packets when they receive no acknowledgment to a previously sent packet.
802.11 WEP Pkts	The number of packets observed on the wireless LAN during this capture session with the WEP bit in the Frame Control field set to true. This indicates that Wired Equivalent Policy encryption was used on the packet.
802.11 Short PLCPs	The number of Physical Layer Convergence Protocol (PLCP) protocol data units seen with the “short” preamble and header during this capture session. This form of PLCP PDU is used to achieve higher throughput and can support 5.5 and 11 Mbps transmission speeds.

Table 10-8. 802.11 Counters in the Statistics Tab (2 of 2)

Counter	Description
802.11 Long PLCPs	The number of PLCP PDUs seen with the “long” preamble and header during this capture session. This form of PLCP PDU is compatible with legacy equipment from older wireless LANs and supports and operates at either 1 Mbps or 2 Mbps.
Data Rate Counters	These counters vary depending on the monitored network: • For 802.11b/g networks, there are separate counters for the number of frames sent at 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54, 72, 108 Mbps. • For 802.11a networks, there are separate counters for the number of frames sent at 6, 9, 12, 18, 24, 36, 48, 54, 72, and 108 Mbps. • For legacy 802.11b cards, the speeds remain at 1, 2, 5.5, 11 Mbps. **NOTE:** 802.11g is backward-compatible with 802.11b, therefore the speed counters seen in 802.11b are also shown in 802.11g. 802.11b and 802.11g share the same frequency band (2.4 GHz) and same number of channels (1-14). 802.11b goes from speeds 1 Mbps to 11 Mbps and 802.11g goes from speeds 1 Mbps to 54 Mbps. 802.11a and 802.11g share similar speeds (6, 9, 12, 18, 24, 36, 48, 54, 72, and 108 Mbps – 72 and 108 Mbps are proprietary implementations).

Define Filter Options for Wireless Networks

The Sniffer software adds several wireless-specific filtering options, including:

- IEEE 802.11 Packet Type Filters
- Error Packet Filters

You set wireless-specific filters in the Define Filter dialog box's **Advanced** tab. You display this tab by selecting the **Define Filter** command from either the **Monitor**, **Capture**, or **Display** menu. Filters defined from the **Monitor** menu are monitor filters — they apply to data analyzed by the monitor. Similarly, filters defined from the **Capture** menu are capture filters — they apply to captured data. Filters defined from the **Display** menu are display filters — they temporarily remove captured data from the display so you can concentrate on the protocols in which you are most interested.

Figure 10-12 shows the **Advanced** tab of the Define Filter dialog box with the 802.11 packet types and error packet types available for filtering.

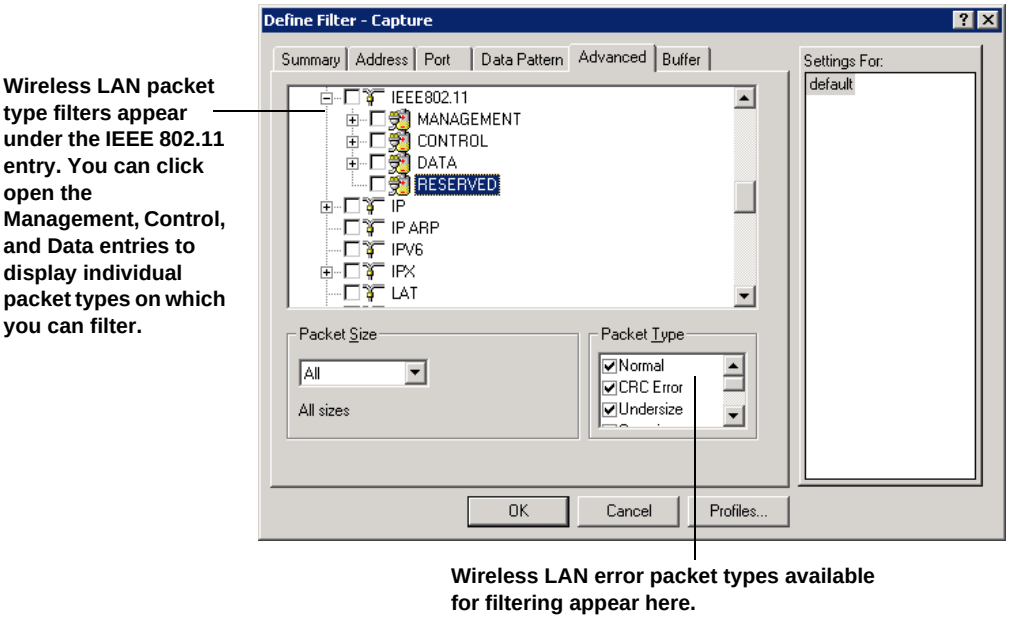


Figure 10-12. Setting Advanced Filters on WLAN Packet Types

Filters for 802.11 Packet Types

You can set filters on the wireless LAN error packet types listed and described in Table 10-9.

Table 10-9. 802.11 Packet Types Available for Filtering

Family	Packet Type	Description
Management	Association Request	Stations send Association Requests to become associated with access points.
Management	Association Response	Access points send Association Responses in response to Association Requests from wireless stations.
Management	Reassociation Request	Stations send Reassociation Requests when they need to associate with a new access point (for example, because they are out of range of their old access point). This way, the new access point knows to set up forwarding of traffic from the old access point.
Management	Reassociation Response	Access points send Reassociation Responses in response to Reassociation Requests from wireless stations.
Management	Probe Request	Stations send Probe Requests to other stations or access points to retrieve information (for example, to determine whether a given access point is open for new associations).
Management	Probe Response	Stations and access points send Probe Responses containing requested parameters in response to Probe Requests.
Management	Beacon	Access points send beacon packets at a regular interval to synchronize timing between stations on the same network.
Management	ATIM	Stations send ATIMs immediately after a beacon packet transmission to inform other stations that they have data to transmit to them.
Management	Disassociation	Stations and access points send Disassociations to end associations.
Management	Authentication	Stations and access points send Authentications to identify one another securely.
Management	Deauthentication	Stations and access points send Deauthentications to end secure communications with one another.
Management	Association Requests	Stations send Association Requests to become associated with access points.
Control	PS Poll	PS Poll packets are sent by stations to inform other stations of time windows during which they will not be transmitting.
Control	RTS	RTS packets are sent by stations to negotiate how a data frame will be sent.

Table 10-9. 802.11 Packet Types Available for Filtering

Family	Packet Type	Description
Control	CTS	Stations send CTS packets to acknowledge the receipt of an RTS packet and to indicate that they are ready to receive data.
Control	ACK	Stations send acknowledge packets to indicate that they have received an error-free packet.
Control	CF End	CF End packets are sent to indicate the end of a contention period.
Control	CF End + CF ACK	CF End/CF ACK packets are sent to acknowledge CF End packets.
Control	Control Reserved	802.11 control packets with a proprietary packet type indicated.
Data	Data Only	Data packets are sent to exchange data.
Data	Data + CF-Ack	Data packets with a CF-Ack included.
Data	Data + CF-Poll	Data packets with a CF-Poll included
Data	Data + CF-Ack + CF-Poll	Data packets with a CF-Ack/CF-Poll included.
Data	Null function (no data)	Empty data packets.
Data	CF-Ack (no data)	Empty data packets with a CF-Ack.
Data	CF-Poll (no data)	Empty data packets with a CF-Poll
Data	CF-Ack + CF-Poll (no data)	Empty data packets with a CF-Ack/CF-Poll.
Data	Data Reserved	Data packets with a proprietary extension indicated.

Filters for Wireless LAN Error Packet Types

You can set filters on the wireless LAN error packet types listed and described in Table 10-10.

Table 10-10. Wireless LAN Error Packet Types Available for Filtering

Packet Type	Description
PLCP Errors	PLCP errors occur when a wireless station receives a Physical Layer Convergence Protocol header with an invalid checksum. Before frames are sent between wireless stations, the physical layer (PHY) sends a PLCP header to a receiving station to negotiate the size of the frames to be sent, the speed at which they should be sent, and so on. This PLCP header includes a checksum which the receiving station uses to validate that the received PLCP header is not corrupt. If this checksum is corrupt, it is considered a PLCP error.
WEP ICVs	The Wired Equivalent Policy (WEP) is used to encrypt data sent between stations on the wireless network. When two stations exchange WEP-encrypted data, they go through an authentication sequence wherein challenge messages are encrypted and decrypted by sender and receiver. If an Integrity Check Value does not match between sender and receiver, the receiver sends a frame indicating a communications failure (that is, an invalid WEP ICV). This filter works on these types of packets.

Protocol Decodes for Wireless Networks

In addition to all upper layer decodes, the Sniffer software provides comprehensive decodes for 802.11 wireless LAN traffic. Since wireless LAN services take place at the physical and MAC layers, you can see the wireless-specific decodes by examining the DLC layer in the Decode display.

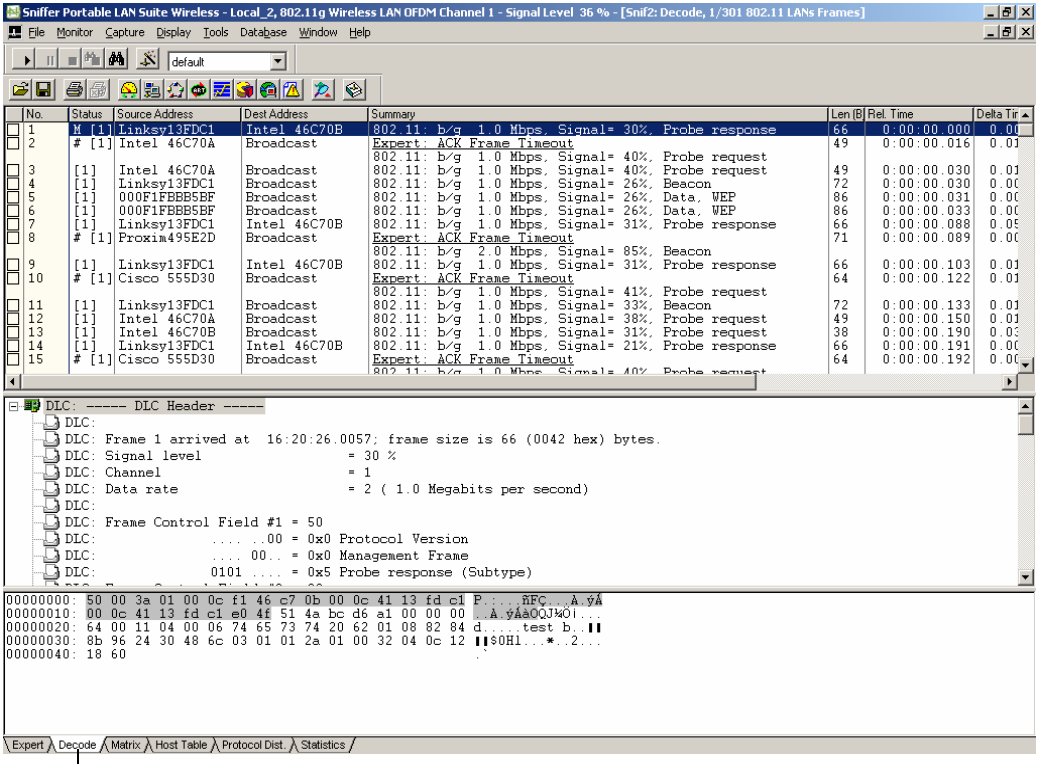
Postcapture WEP Decryption

The Sniffer software can decrypt and decode WEP-encrypted packets either during or after capture. As described in *Setting Encryption Options* on page 85, you use the **Encryption** options in the **802.11** tab of the Options dialog box to configure the automatic decryption of WEP-encrypted data during capture. However, you can also perform WEP decryption on trace files containing frames encrypted with a known WEP key set but not decrypted during capture. This section describes how.

To perform offline decryption of WEP-encrypted data:

1 Display the **Decode** tab of a trace file or capture buffer containing frames encrypted with a known WEP key set but not decrypted during capture.

Figure 10-13 shows the **Decode** tab of a saved trace file from a wireless LAN.



Decode tab selected.

Figure 10-13. Decode Tab of a Saved Trace File from a Wireless LAN

2 Right-click in the **Summary**, **Detail**, or **Hex** pane to activate the **Decode** tab's context menu.

3 Select **WEP Decrypt** to open the Select WEP Keys dialog box, as shown in Figure 10-14.

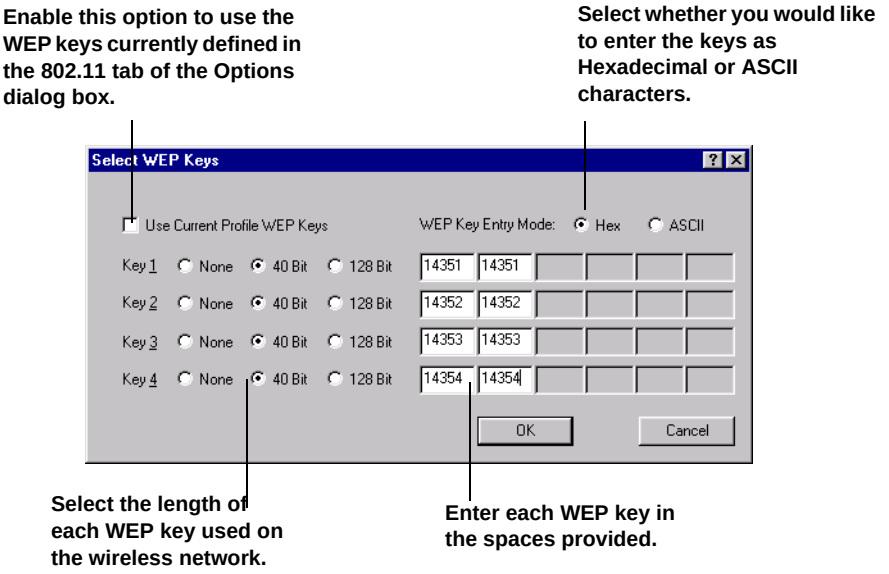


Figure 10-14. The Select WEP Keys Dialog Box

Use the Select WEP Keys dialog box to specify the WEP keys to be used for decrypting the data in the selected buffer or trace file. You can either use the WEP keys currently defined in the **802.11** tab of the Options dialog box, or you can specify new keys in the fields provided.

4 To decrypt the data in the selected buffer or trace file using the WEP keys currently defined in the **802.11** tab of the Options dialog box, enable the **Use Current Profile WEP Keys** option. Enabling this option causes the other fields in the Select WEP Keys dialog box to be grayed out, indicating that they are unavailable.

5 To specify new WEP keys for decryption, start by setting the **WEP Key Entry Mode** option to specify whether you want to enter the keys as either **Hex** or **ASCII**.

6 You can enter up to four separate encryption keys. For each key, do the following:

a Specify the length of the key by selecting the appropriate option. Keys can be either **None**, **40-bit**, or **128-bit**. Use the **None** option if no encryption is used on the network.

Depending on the length of the key specified, some or all of the adjacent fields become active, enabling you to specify the keys in use.

b Specify the exact value for each key in the adjoining spaces provided.

NOTE: The four encryption keys in use on a WEP-encrypted network are all typically the same length — either 40-bit or 128-bit.

7 Click **OK** on the Select WEP Keys dialog box.

The Sniffer software attempts to use the specified WEP keys to decrypt the data in the selected buffer or trace file and opens a new window with the results. If you specified the correct WEP keys, the new window displays the newly-decrypted data. You can save the decrypted data to a new trace file using the usual **File** > **Save** command.

NOTE: An easy way to determine whether you have entered the correct WEP keys is to check for the presence of a large number of **WEP-ICV Error** Expert alarms. If there are an abnormally large number of these alarms, you probably have not entered the correct WEP keys for the encrypted data in the selected buffer or trace file.

Expert Objects and Alarms for Wireless Networks

The Sniffer software provides several additions to the Expert analyzer for wireless networks, including:

- Information for DLC layer network objects receiving or sending information over a wireless LAN.

  During Expert analysis, the Sniffer software constructs a database of network objects from the traffic it sees. The Expert protocol interpreters learn all about the network stations, routing nodes, subnetworks, and connections related to the frames in the capture buffer. This information is presented in the Expert display.

- A dedicated Wireless Expert layer for maintaining information on wireless stations and access points. The Wireless layer is found below the DLC layer in the Expert display. The Expert creates network objects at this layer specifically for wireless stations. Unlike the objects at the DLC layer (which are concerned only with data frames), objects at the Wireless layer provide statistics for all wireless frame types (including data, control, and management frames).
- Expert symptoms and diagnoses specifically for wireless LANs.

  Using the information in its database of network objects, The Expert analyzer detects and alerts you to potential problems that may exist on the network. These problems are categorized as being either *symptoms* or *diagnoses*:

  - A *symptom* indicates that a threshold has been exceeded and may indicate a problem on your network.
  - A *diagnosis* can be several symptoms analyzed together, high rates of recurrence of specific symptoms, or single instances of particular network events that cause the Expert to conclude that the network has a real problem. A Diagnosis should be investigated immediately.

This section describes the detail displays for wireless LAN network objects, as well as the symptoms and diagnoses.

NOTE: Since it is beyond the scope of this document to describe the Expert analyzer in detail, this section assumes that you are already generally familiar with the Expert analyzer. See the product *User's Guide* and online help files for detailed information on working with Expert analyzer displays.

Expert Object Detail Displays for Wireless LANs

The Sniffer software provides Expert detail displays for wireless stations. The Expert creates network objects for wireless stations at both the Expert DLC and Wireless layers. You view Detail displays for the network objects in the same way you do for all other protocols:

1. Display either the Expert window (for analysis during capture) or the **Expert** tab in the Decode window (for post-capture analysis).
2. Select the Expert layer at which you want to view Detail displays by clicking in the **Objects** column at the desired layer in the Overview pane (see Figure 10-15). Expert Detail displays for wireless LAN network objects are found at the DLC and Wireless layers.

   The adjacent Summary pane automatically updates to show all network objects at the selected layer.

3 Highlight one of the objects in the Summary pane by clicking it. The Detail pane automatically updates to show detailed statistics for the object selected in the Summary pane.

For example, Figure 10-15 shows a network object for a wireless station selected at the Expert DLC layer. The Detail pane shows detailed statistics for the selected object.

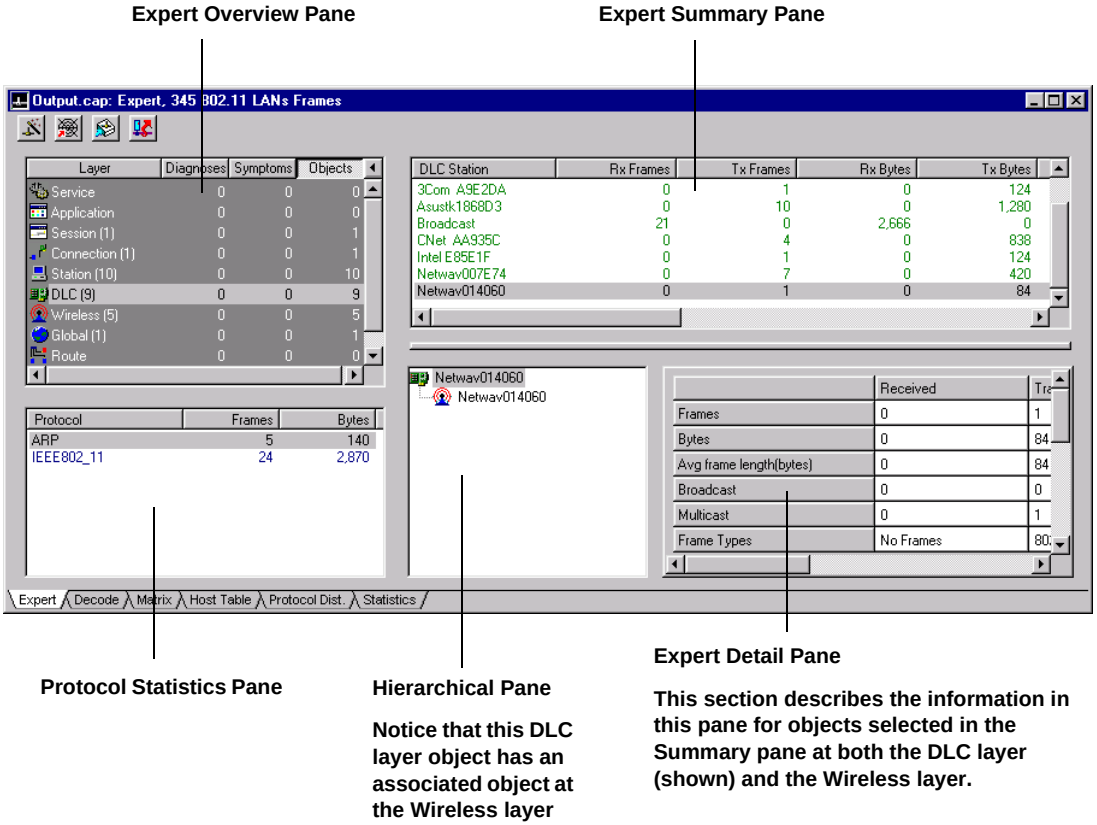


Figure 10-15. The Expert Window Panes

DLC Layer Expert Detail Display with 802.11 Information

The Expert creates objects at the DLC layer with 802.11 information based on the DLC addresses in the 802.11 traffic it observes. If the original source or final destination address in an 802.11 frame is a traditional wired station, the Expert creates a DLC layer object with 802.11 information in its Detail Display. A separate object is created for each DLC address observed (including multicast and broadcast addresses).

Objects created at the DLC layer with 802.11 information will typically have at least one associated lower layer object at the Wireless layer — for example, a multicast wireless address at the DLC layer will also have a corresponding multicast wireless address at the wireless layer. Similarly, a traditional wired DLC address sending data to a wireless station may have an associated object at the Wireless layer corresponding to the access point used to access the wireless LAN. In some cases, a single DLC layer object may have multiple associated lower layer objects at the Wireless layer — for example, an associated object for itself, as well as one for its associated access point.

You can see this relationship most easily in the Expert's hierarchical display (see Figure 10-15 on page 138 for an example of where to find the hierarchical pane). For example, the hierarchical pane shown in Figure 10-16 on page 139 shows that the DLC layer object created for the mobile unit with the DLC address Netwav007E74 has two associated wireless layer objects (indicated by the icon) — Netwav014060 (its associated access point) and Netwav007E74 (itself). Wireless layer detail displays are described in the next section.

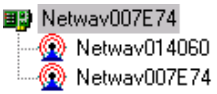


Figure 10-16. Multiple Wireless Layer Objects for Single DLC Object

Figure 10-17 shows the Expert detail display for a wireless station at the DLC layer. Following the figure, each field in the detail display is described.

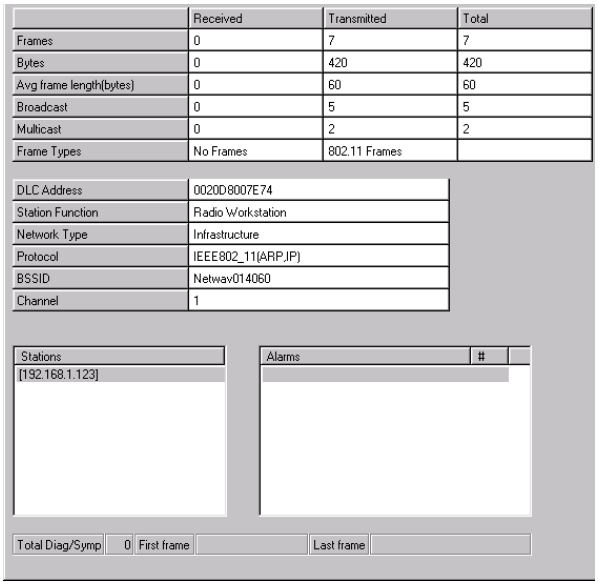


Figure 10-17. Expert Detail Pane for a Wireless LAN Station at the DLC Layer

Traffic Statistics Table

The Traffic Statistics table breaks out the frames transmitted and received by the DLC station. Each counter described in Table 10-11 is provided for frames sent from the station, frames received by the station, and total frames sent and received.

Table 10-11. Counters in the Traffic Statistics Table

Counter	Description
Frames	The number of frames sent from the station, received by the station, and the total frames sent and received by the station.
Bytes	The number of bytes sent from the station, received by the station, and the total bytes sent and received by the station.
Avg frame length (bytes)	The average length of the frames sent from the station, received by the station, and the total frames sent and received by the station.
Broadcast	The number of broadcast frames sent from the station, received by the station, and the total number of broadcast frames sent and received by the station.
Multicast	The number of multicast frames sent from the station, received by the station, and the total number of multicast frames sent and received by the station.
Frame Types	The type of frames seen transmitted and received by this station (for example, 802.11 frames).

Station Identity Table

The Station Identity table includes statistics identifying this station — its DLC address, the channel on which traffic originating from or sent to it was seen, and so on. Table 10-12 lists and describes the counters in the Station Identity table.

Table 10-12. Counters in the Station Identity Table (1 of 2)

Counter	Description
DLC Address	The DLC address for this station.

Table 10-12. Counters in the Station Identity Table (2 of 2)

Counter	Description
Station Function	The function of this station, as learned by the Expert. Possible functions include **Workstation, Mobile Unit**, **Access Point**, and so on.
Network Type	The type of network to which this station belongs. Possible types include: • **Infrastructure** - part of an extended service set network, with access to a distribution system. • **IBSS** - Independent Basic Service Set - a self-contained network with no access to a distribution system.
Protocol	The DLC layer protocol used by this station. For stations sending or receiving information over wireless networks, this will be IEEE802.11. Higher layer protocols in use may appear in parentheses following this entry, if known (for example, IP, IPX, and so on).
BSSID	The Basic Service Set ID used by this station for communications on this channel.
Channel	The channel on which this wireless station was seen.

Stations Listbox

The Stations listbox lists the objects at the next higher layer associated with this object. At the DLC layer, the next higher Expert layer is the Stations layer. For example, the Stations listbox could list IP or IPX network stations associated with this DLC layer object. You can double-click each object in the listbox to drill into the upper layers of the Expert.

Alarms Listbox

The Alarms listbox contains the alarms generated by the Expert for this object. You can double-click each listed alarm to see more detailed information about (including a link to the Expert Explain File for the alarm).

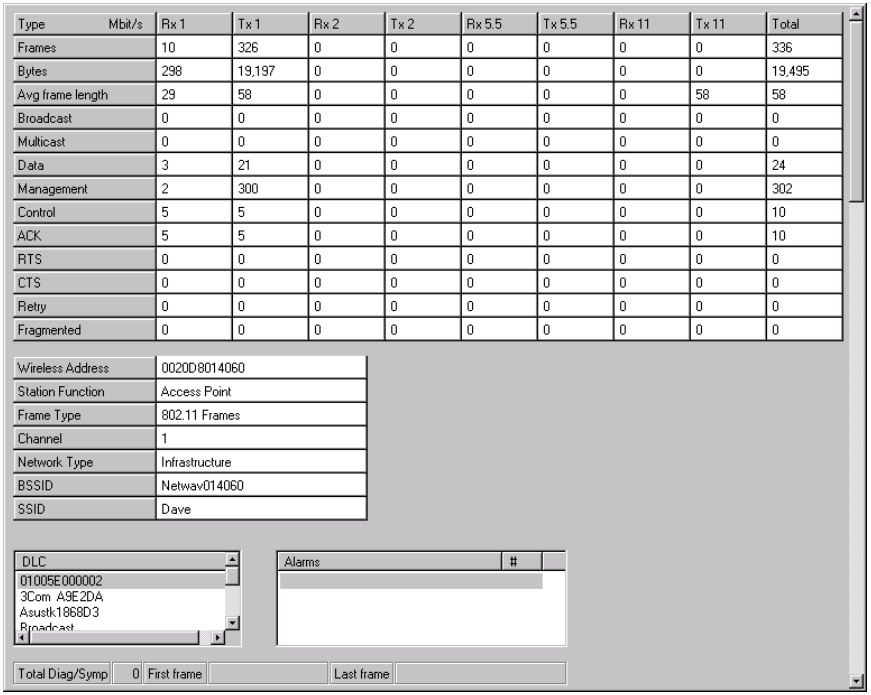
Object Information

The final grid includes the total number of diagnoses and symptoms generated for this object, the time the first frame for this object was captured, and the time the last frame for this object was captured.

Wireless Layer Expert Detail Display for a Wireless Station

The Expert creates objects at the Wireless layer for wireless stations based on the 802.11 traffic it observes. A separate object is created for each MAC layer address observed (including multicast and broadcast addresses). Unlike the DLC layer (which is concerned only with data frames for wireless stations), the Wireless layer tracks data, control, and management 802.11 frames.

Figure 10-18 shows the Expert detail display for a wireless station at the Wireless layer. Following the figure, each field in the detail display is described.



Type Mbit/s	Rx 1	Tx 1	Rx 2	Tx 2	Rx 5.5	Tx 5.5	Rx 11	Tx 11	Total
Frames	10	326	0	0	0	0	0	0	336
Bytes	298	19,197	0	0	0	0	0	0	19,495
Avg frame length	29	58	0	0	0	0	0	58	58
Broadcast	0	0	0	0	0	0	0	0	0
Multicast	0	0	0	0	0	0	0	0	0
Data	3	21	0	0	0	0	0	0	24
Management	2	300	0	0	0	0	0	0	302
Control	5	5	0	0	0	0	0	0	10
ACK	5	5	0	0	0	0	0	0	10
RTS	0	0	0	0	0	0	0	0	0
CTS	0	0	0	0	0	0	0	0	0
Retry	0	0	0	0	0	0	0	0	0
Fragmented	0	0	0	0	0	0	0	0	0

Wireless Address	0020D8014060
Station Function	Access Point
Frame Type	802.11 Frames
Channel	1
Network Type	Infrastructure
BSSID	Netwav014060
SSID	Dave

Figure 10-18. Expert Detail Pane for a WLAN Station at the Wireless Layer (802.11b/g)

Traffic Statistics Table

The Traffic Statistics table counts each of the frame types listed in Table 10-13 transmitted and received by the indicated wireless station. Each frame type is counted in a variety of different data rate categories. The available data rate categories will vary depending on whether the indicated station is an 802.11a or an 802.11b/g station.

- Frames sent and received by 802.11a stations will be broken out into data rate categories between 6 Mbps and 108 Mbps.

- Frames send and received by 802.11b/g stations will be broken out into data rate categories between 1 Mbps and 11 Mbps.

Regardless of whether the station is 802.11a or 802.11b/g, there will still be a **Total** counter indicating the total number of the indicated type of frame transmitted and received by this station in all service categories.

Table 10-13. Counters in the Traffic Statistics Table (1 of 2)

Counter	Description
Frames	The number of frames sent and received by this station, broken out by service category.
Bytes	The number of bytes sent and received by this station, broken out by service category.
Avg frame length (bytes)	The average length of the frames sent and received by this station, broken out by service category.
Broadcast	The number of broadcast frames sent and received by this station, broken out by service category.
Multicast	The number of multicast frames sent and received by this station, broken out by service category.
Data	The number of data frames sent from the station, received by the station, and the total number of data frames sent and received by the station. Data packets are used to transmit data between stations.
Management	The number of management frames sent and received by this station, broken out by service category. Management packets are used to set up the initial communications between stations and access points on the wireless network.
Control	The number of control frames sent and received by this station, broken out by service category. Control frames are used to regulate the transmission of data frames after initial authentication has taken place.

Table 10-13. Counters in the Traffic Statistics Table (2 of 2)

Counter	Description
ACK	The number of ACK frames sent and received by this station, broken out by service category. Stations send acknowledge frames to indicate that they have received an error-free frame.
RTS	The number of RTS frames sent and received by this station, broken out by service category. Stations send RTS frames to negotiate how a data frame will be sent.
CTS	The number of CTS frames sent and received by this station, broken out by service category. Stations send CTS frames to acknowledge the receipt of an RTS frame and to indicate that they are ready to receive data.
Retry	The number of Retry frames sent and received by this station, broken out by service category. Stations send retry frames when they receive no acknowledgment to a previously sent frame.
Fragmented	The number of fragmented frames sent and received by this station, broken out by service category. When possible (and if configured to do so), wireless stations break frames into smaller units (fragments) to provide a greater degree of reliability (large data units can become corrupt more easily than small ones). Receiving stations reassemble fragments into full frames (a process called defragmentation).

Station Identity Table

The Station Identity table includes statistics identifying this station — its DLC address, the channel on which it was seen, and so on. Table 10-12 lists and describes the counters in the Station Identity table.

Table 10-14. Counters in the Station Identity Table (1 of 2)

Counter	Description
Wireless Address	The MAC layer address for this wireless station.

Table 10-14. Counters in the Station Identity Table (2 of 2)

Counter	Description
Station Function	The function of this station, as learned by the Expert. Possible functions include **Mobile Unit**, **Workstation**, **Access Point**, **Broadcast**, and **Multicast**.
Frame Type	The type of frames seen transmitted by this station. For the Wireless layer, this will indicate whether the frames seen were 802.11a, 802.11b/g, and so on.
Channel	The channel on which this wireless station was seen. • For wireless stations, this will be the channel on which the Expert was capturing. • For access points, this will be the value seen for the DS Parameter Set information element inside Beacon and Probe Response frames.
Network Type	The type of network to which this station belongs. Possible types include: • **Infrastructure** - part of an extended service set network, with access to a distribution system. • **IBSS** - Independent Basic Service Set - a self-contained network with no access to a distribution system.
BSSID	The Basic Service Set ID used by this station for communications on this channel. This field will be blank for objects created for multicast/broadcast transmissions.
SSID	The Service Set Identifier used by this station, if known. This field will be blank for objects created for multicast/broadcast transmissions.

DLC Listbox

The DLC listbox lists the objects at the next higher layer associated with this object. At the Wireless layer, the next higher Expert layer is the DLC layer. For example, the DLC listbox could list multicast addresses to which this wireless station has sent frames. In the case of an access point, this listbox will typically include multiple DLC address (since many stations use an access point for ingress and egress for the wireless network). You can double-click each object in the listbox to drill into the upper layers of the Expert.

Alarms Listbox

The Alarms listbox contains the alarms generated by the Expert for this object. You can double-click each listed alarm to see more detailed information about (including a link to the Expert Explain File for the alarm).

Object Information

The final grid includes the total number of diagnoses and symptoms generated for this object, the time the first frame for this object was captured, and the time the last frame for this object was captured.

Expert Alarms for Wireless Networks

The Sniffer software includes many wireless-specific Expert alarms. As with all Expert alarms, you can set severities for each of the alarms in this section in the **Tools > Expert Options > Alarms** tab. Each alarm is described below, organized by the Expert layer at which they occur.

- *Global Layer Expert Alarms for Wireless Networks* on page 146
- *Wireless Layer Expert Alarms for Wireless Networks* on page 147

Global Layer Expert Alarms for Wireless Networks

Channel Mismatch

The Expert generates the **Channel Mismatch** alarm in the following situations:

- In an infrastructure wireless network (a wireless network with access to a distribution system), the Expert generates this alarm when it receives beacon and/or probe response frames from an access point on a channel other than the channel on which the access point is configured to operate.

- In an ad hoc wireless network (a wireless network with no access to a distribution system), the Expert generates this alarm when it receives beacon and/or probe response frames from a wireless station on a channel other than the channel on which the station is operating.

In an 802.11 infrastructure wireless network, access points send beacon frames at a regular interval. In addition, they send probe response frames in response to probe request frames sent from wireless stations wanting to join the network. In an ad hoc network, the stations themselves send beacon and probe request frames.

Among other parameters, beacon frames and probe requests specify the wireless channel on which the basic service set (BSS) is operating. The wireless stations in a single BSS can only operate on one channel at a time — the channel on which the BSS is operating. However, due to adjacent channel interference, wireless stations can occasionally receive frames from stations operating on a different channel. The Expert generates the **Channel Mismatch** alarm when this happens.

PLCP Error

The Expert generates the **PLCP Error** alarm when it receives a Physical Layer Convergence Protocol header with an invalid checksum.

Before frames are sent between wireless stations, the physical layer (PHY) sends a PLCP header to a receiving station to negotiate the size of the frames to be sent, the speed at which they should be sent, and so on. This PLCP header includes a checksum that the receiving station uses to validate that the received PLCP header is not corrupt. The Expert generates this alarm if it receives a PLCP header in which the checksum is corrupt.

Wireless Layer Expert Alarms for Wireless Networks

ACK Frame Timeout

The Expert generates the **ACK Frame Timeout** alarm when it does not see an acknowledgment to a unicast management or data frame within the time specified in the Duration field of the original management or data frame. When this happens, the sending station will resend the original frame and wait for another ACK.

Unicast management and data frames include a Duration field indicating the amount of time within which a receiving station should return an ACK frame. The value of this field is typically equal to the amount of time required to send an ACK frame plus one short interframe space (SIFS). The Duration field lets other stations on the network know that during this period, the medium is reserved for the response to the frame.

The Expert stores the value specified in the Duration field in a buffer. If it does not see the corresponding ACK to the frame (identified by matching sequence numbers) within the value specified by the Duration field, it generates this alarm.

Association Failure

The Expert generates the **Association Failure** alarm when it detects an 802.11 Association Response frame with a value other than zero in the Status Code field. A non-zero value in the Status Code field indicates that the access point sending the Association Response is denying the requested association.

To be a member of an infrastructure 802.11 wireless network, wireless stations must be associated with an access point. Wireless stations send Association Request frames to become associated with an access point. In turn, access points reply to Association Requests with Association Responses indicating the success or failure of the request. In this case, the access point denied the association request. The exact reason for the denial is found in the Status Code field of the Association Response. The Expert reports both the address of the access point denying the Association Request, as well as the reason for the denial indicated in the Status Code field.

- 1 — Unspecified failure.
- 10 — Cannot support all requested capabilities in the Capability Information field.
- 12 — Association denied due to reason outside the scope of the 802.11 standard.
- 17 — Association denied because the access point is unable to handle additional associated stations.
- 18 — Association denied due to requesting station not supporting all of the data rates in the BSSBasicRateSet parameter.

Authentication Failure

The Expert generates the **Authentication Failure** alarm when it detects an 802.11 Authentication frame with a value other than zero in the Status Code field. A non-zero value in the Status Code field indicates that the access point sending the Authentication frame is denying the requested authentication.

Wireless stations exchange Authentication frames with access points to authenticate themselves with the network, thereby providing security and privacy. The authentication sequence for 802.11 networks consists of the exchange of either two authentication frames (for open system authentication) or four authentication frames (for shared key authentication), each identified by a transaction sequence number. The extra two authentication frames for shared key authentication are for the exchange of a string of challenge text, first sent in the clear by the access point and then returned in encrypted format by the wireless station.

The Expert generates this alarm when the access point refuses to authenticate the requesting wireless station. The exact reason for the denial is found in the Status Code field of the Authentication frame. The Expert reports both the address of the access point denying the Authentication, as well as the reason for the denial indicated in the Status Code field.

- 1 — Unspecified failure.
- 13 — Responding station does not support the specified authentication algorithm.
- 14 — Received an Authentication frame with authentication transaction sequence number out of expected sequence.
- 15 — Authentication rejected because of challenge failure.
- 16 — Authentication rejected due to timeout waiting for next frame in sequence.

CTS Frame Timeout

The Expert generates the **CTS Frame Timeout** alarm when it does not see a clear to send (CTS) frame sent in response to a request to send (RTS) frame within the time specified in the Duration field of the original RTS frame.

RTS frames include a Duration field indicating the amount of time within which a receiving station should return a CTS frame. The value of this field is typically equal to the amount of time required to send the CTS frame, one ACK frame, and three short interframe spaces (SIFS). The Duration field lets other stations on the network know that during this period, the medium is reserved.

When the Expert sees an RTS frame, it stores the value specified in the Duration field in a buffer. If it does not see the corresponding CTS frame within the value specified by the Duration field, it generates this alarm.

Deauthentication

The Expert generates the **Deauthentication** alarm when it detects an 802.11 Deauthentication frame. Occasionally, wireless stations need to terminate secure communications with one another or with an access point. To do so, they send Deauthentication frames.

Deauthentication frames are a part of normal 802.11 network operations. A relatively small number of these alarms is no cause for concern. However, a large number of Deauthentication frames may indicate a potential authentication denial attack on the wireless network.

The alarm display includes the following information:

- The destination address of the Deauthentication frame (that is, the station with which the sending station want to terminate secure communications).
- The Reason Code indicating the reason the Deauthentication frame was sent. Possible values for the Reason Code field include:
  - 1 — Unspecified reason.
  - 2 — Previous authentication no longer valid.
  - 3 — Deauthenticated because sending station is leaving (or has left) the network.
  - 6 — Class 2 frame received from non-authenticated station.

Disassociation

The Expert generates the **Disassociation** alarm when it detects an 802.11 Disassociation frame. Wireless stations and access points send Disassociation frames to terminate associations with one another. For example, an access point may terminate an association with a station because it is unable to handle any more associations. Similarly, a wireless station may terminate an association if it is leaving the network.

Disassociation frames are a part of normal 802.11 network operations. A relatively small number of these alarms is no cause for concern. However, a large number of Disassociation frames may indicate a potential denial of service attack on the wireless network.

The alarm display includes the following information:

- The destination address of the Disassociation frame (that is, the station with which the sending station want to terminate its association).
- The Reason Code indicating the reason the Disassociation frame was sent. Possible values for the Reason Code field include:

- 1 — Unspecified reason.
- 4 — Disassociated due to inactivity.
- 5 — Disassociated because the access point is unable to handle all currently associated stations.
- 7 — Class 3 frame received from non-associated station.
- 8 — Disassociated because sending station is leaving (or has left) the network.
- 9 — Station requesting (re)association is not authenticated with responding station.

Mcast/Bcast Fragmentation

The Expert generates the **Mcast/Bcast Fragmentation** alarm when it detects an 802.11 frame with a multicast or broadcast destination address and fragmentation indicated in the MAC header. This is a violation of the 802.11 specification.

Wireless networks commonly implement the fragmentation and defragmentation services provided by the 802.11 MAC layer to increase transmission reliability. However, the 802.11 specification does not allow fragmentation for broadcast or multicast frames because of the overhead this would cause for the network as a whole.

Missing Fragment Number

The Expert generates the **Missing Fragment Number** alarm when it detects a jump in the fragment number of an 802.11 frame, indicating that a portion of a fragmented data unit is at least temporarily missing.

Wireless networks commonly implement the fragmentation and defragmentation services provided by the 802.11 MAC layer to increase transmission reliability. When a unicast frame's length exceeds an internal threshold in the MAC's MIB, the MAC will break up the frame into smaller constituent frames — *fragments* — with the same sequence number.

Each fragment of a larger data unit is identified with a fragment number indicating its intended ordered position within the reassembled data unit at the receiving station. The Expert observes each transmitted fragment and stores the fragment numbers. If it observes a jump in the fragment number for the transmission of fragments with the same sequence number, it generates this alarm.

Possible Cause

1 A relatively small number of these alarms is no cause for concern. 802.11 guarantees the sequential arrival of fragments at a receiving station, but occasionally fragments may be missing due to interference or other network problems. This is why the fragment number exists — so that receiving stations can reassemble data units in the intended order regardless of the sequence in which they arrive.

   Because each fragment must be positively acknowledged by the receiving station, 802.11 provides a mechanism to ensure that all fragments eventually do arrive. If a sending station does not receive the ACK for a fragment, it simply resends the fragment after an internal timer expires. If the receiving station receives multiple copies of the same fragment, it discards the excess copies of the fragment.

   With this in mind, you can see that a large number of **Missing Fragment Number** alarms may indicate significant interference on the network. You should check the Dashboard to see if there are also a large number of CRC errors on the network. If this is true, you may want to adjust the fragment size used by the MAC to use smaller fragments and see if this reduces the number of CRC errors on the network (and, correspondingly, the amount of **Missing Fragment Number** alarms generated).

Oversized WLAN Frame

The Expert generates the **Oversized WLAN Frame** alarm when it detects an 802.11 MAC frame longer than the maximum acceptable length dictated by the 802.11 specification.

The maximum acceptable length for an 802.11 MAC frame is 2346 bytes.

Reassociation Failure

The Expert generates the **Reassociation Failure** alarm when it detects an 802.11 Reassociation Response frame with a value other than zero in the Status Code field. A non-zero value in the Status Code field indicates that the access point sending the Reassociation Response is denying the requested association.

Wireless stations send Reassociation Request frames to become associated with a different access point within the same network as its current access point (for example, because the station has moved and is now out of range of its old access point and within range of another). In turn, access points reply to Reassociation Requests with Reassociation Responses indicating the

success or failure of the request. In this case, the access point denied the Reassociation Request. The exact reason for the denial is found in the Status Code field of the Reassociation Response. The Expert reports both the address of the access point denying the Reassociation Request, as well as the reason for the denial indicated in the Status Code field.

- 1 — Unspecified failure.
- 10 — Cannot support all requested capabilities in the Capability Information field.
- 11 — Reassociation denied due to inability to confirm that association exists.
- 12 — Association denied due to reason outside the scope of the 802.11 standard.
- 17 — Association denied because the access point is unable to handle additional associated stations.
- 18 — Association denied due to requesting station not supporting all of the data rates in the BSSBasicRateSet parameter.

Rogue Access Point

The Expert generates the **Rogue Access Point** alarm when it detects a wireless access point on the network whose MAC address is not found in its list of known access points. You can view the Expert's list of known access points in the **Known Access Points in the Network** listbox in the **802.11 Options** tab of the Expert Properties dialog box. You access this tab by selecting **Expert Options** from the **Tools** menu and clicking the **802.11 Options** tab in the dialog box that appears.

The **Rogue Access Point** alarm provides you with a convenient means of detecting access points on the network of which you were previously unaware. To use this alarm effectively, you must add the MAC addresses of the known access points on the network to the Expert's list. You can add access points to the Expert's list in any of the following ways:

- Automatically in the real-time Host Table by selecting entries in the table, right-clicking, and selecting the **Add to Known Mobile Unit List** command.
- Automatically in the postcapture display's Expert tab by clicking the **Wireless Unit List** button and using the options in the dialog box that appears.
- Automatically in the Address Book by clicking **Export AP**.
- Manually in the **Tools > Expert Options > 802.11 Options** tab.

In addition, you must also have enabled the **Enable Rogue AP Lookup** option on the **802.11 Options** tab. When the **Enable Rogue AP Lookup** option is enabled, each time the Expert discovers a new access point, it will compare its MAC address to those in its list of known access points. If the discovered address is not found, the Expert generates the **Rogue Access Point** alarm. In addition, the Expert displays will identify the offending access point as a rogue (the word “Rogue” will appear in parentheses following the station's entries in Expert Summary and Detail displays).

Possible Cause

In most cases, this is a relatively minor alarm, probably indicating nothing more than that you neglected to add the address of a known access point to the Expert's list. However, you may want to examine the address of the access point indicated in the alarm to make sure that it is not an intruder.

Rogue Mobile Unit

The Expert generates the **Rogue Mobile Unit** alarm when it detects a mobile unit on the wireless network whose MAC address is not found in its list of known mobile units. You can view the Expert's list of known mobile units in the **Known Mobile Units in the Network** listbox in the **802.11 Options** tab of the Expert Properties dialog box. You access this tab by selecting **Expert Options** from the **Tools** menu and clicking the **802.11 Options** tab in the dialog box that appears.

The **Rogue Mobile Unit** alarm provides you with a convenient means of detecting mobile units on the network of which you were previously unaware. To use this alarm effectively, you must add the MAC addresses of the known mobile units on the network to the Expert's list. You can add mobile units to the Expert's list in any of the following ways:

- Automatically in the real-time Host Table by selecting entries in the table, right-clicking, and selecting the **Add to Known Mobile Unit List** command.
- Automatically in the postcapture display's Expert tab by clicking the **Wireless Unit List** button and using the options in the dialog box that appears.
- Manually in the **Tools > Expert Options > 802.11 Options** tab.

In addition, you must also have enabled the E**nable Rogue Mobile Unit Lookup** option on the **802.11 Options** tab. When the **Enable Rogue Mobile Unit Lookup** option is enabled, each time the Expert discovers a new mobile unit, it will compare its MAC address to those in its list of known mobile units. If the discovered mobile unit is not found, the Expert generates the **Rogue Mobile Unit Detected** alarm. In addition, the Expert displays will identify the offending mobile unit as a rogue (the word “Rogue” will appear in parentheses following the station's entries in Expert Summary and Detail displays).

Possible Cause

In most cases, this is a relatively minor alarm, probably indicating nothing more than that you neglected to add the address of a known mobile unit to the Expert's list. However, you may want to examine the address of the mobile unit indicated in the alarm to make sure that it is not an intruder.

Runt WLAN Frame

The Expert generates the **Runt WLAN Frame** alarm when it detects an 802.11 MAC frame shorter than the minimum acceptable length dictated by the 802.11 specification.

The minimum acceptable length for an 802.11 MAC frame is 34 bytes. However, some control and management frames are inherently smaller than 34 bytes. The Expert does not generate alarms for these frames.

Same Transmitter and Receiver Address

The Expert generates the **Same Transmitter and Receiver Address** alarm when it detects an 802.11 MAC frame in which the transmitter and receiver addresses indicated in the frame are the same.

Wireless LAN frames include up to four addresses in the standard 802.11 MAC format depending on the type of frame. In addition to the Source and Destination addresses (which refer to the original source of and the final destination for the protocol data in the frame body field), 802.11 MAC frames include Transmitter and Receiver addresses. These addresses are those of the wireless stations responsible for transmitting the frame onto the wireless medium (transmitter address) and the next recipient of the frame on the wireless medium (receiver address).

The Expert generates this alarm if the transmitter and receiver addresses within the frame are the same. If, however, the source and destination addresses within the same frame are also the same, the Expert will also generate the **Same Source and Destination Address** alarm at the Expert DLC layer.

Transmitter Address Is Broadcast

The Expert generates the **Transmitter Address Is Broadcast** alarm when it detects an 802.11 MAC frame with a broadcast address (all 1s) indicated in the Transmitter Address field.

Transmitter Address Is Multicast

The Expert generates the **Transmitter Address Is Multicast** alarm when it detects an 802.11 MAC frame with a multicast address indicated in the Transmitter Address field.

WEP-ICV Error

The Expert generates the **WEP-ICV Error** alarm when it detects a WEP-encrypted packet with an Integrity Check Value (ICV) which does not match the ICV calculated by the Expert using its own WEP keys. This usually happens when the Sniffer software is configured with an incorrect set of WEP keys.

In a wireless network using shared key authentication, each station on the network is programmed with the same four WEP keys (1-4). Wireless stations send WEP-encrypted packets with header fields indicating which of the four shared WEP keys was used to encrypt the data. Receiving stations use the shared key indicated in the packet's header (1-4) for decryption and calculate an expected Integrity Check Value (like a checksum for the encrypted data) to compare against the ICV included in the received packet.

When the Sniffer software detects a WEP-encrypted packet, it attempts to decrypt the data using its own shared WEP keys specified on the **802.11** tab of the **Options** dialog box (accessed from the **Tools > Options** menu). If the ICV it calculates using its WEP keys does not match the ICV included in the packet, the Expert generates this alarm.

Possible Causes

1. The Expert is configured with WEP keys which do not match those in use on the wireless network being analyzed. Go to the **802.11** tab of the Options dialog box (accessed from the **Tools > Options** menu), and make sure that the WEP keys specified there match those in use on the network.
2. The station that sent the offending packet is configured with the wrong WEP keys for the network. Make sure its keys are programmed correctly.

Index

Numerics

128-Bit encryption, 86
40-Bit encryption, 85
802.11 tab, 81 to 82
    Encryption options, 85
    Security options, 89
    Sniffer Configuration options, 83

A

access point
    determining full hex address, 97
ACK Frame Timeout, 147
Acknowledge counter
    in Dashboard's 802.11 tab, 110
Alarm
    Monitor thresholds, 113
alarms (Expert alarms for wireless networks), 146
Association Failure, 148
Association Requests counter
    in Dashboard's 802.11 tab, 108
Association Responses counter
    in Dashboard's 802.11 tab, 109
Atheros AR5002X
    installing in Windows 2000, 9
    installing in Windows XP, 7
    using as a normal network adapter, 10
ATIMs counter
    in Dashboard's 802.11 tab, 109
Authentication Failure, 148
Authentications counter
    in Dashboard's 802.11 tab, 110
autodiscovering wireless units, 95

B

Beacons counter
    in Dashboard's 802.11 tab, 109
    in Global Statistics, 120
    in Host Table, 116
BSSID
    counter in Dashboard's 802.11 tab, 111
    counter in Global Statistics, 120
    in Options dialog box, 84

C

CF End/CF ACK counter
    in Dashboard's 802.11 tab, 111
Channel Mismatch, 146
Channel option
    in Options dialog box, 84
channel surfing
    and triggers, 84
Channel Surfing option, 83
Channel Surfing tab
    in Global Statistics, 118
Cisco Aironet
    installation notes and issues, 66
    installing in Windows 2000, 60
    installing in Windows NT, 53
    installing in Windows XP, 58
    using as a normal adapter, 64
Cntl Pkts counter
    in Global Statistics, 120
configuring
    Encryption options, 85
    Security options, 89
    Sniffer Configuration options, 83
contacting Network General, ix
CRC counter
    in Host Table, 116
creating a local agent, 79
CTS counter
    in Dashboard's 802.11 tab, 110
CTS Frame Timeout, 149

D

Data Pkts counter
- in Dashboard's 802.11 tab, 107
- in Global Statistics, 120

Data Throughput counter
- in Dashboard's 802.11 tab, 107

Deauthentication, 150

Deauthentications counter
- in Dashboard's 802.11 tab, 110

Define Filter
- wireless options, 130

Diagnosis in Expert analysis, 137

Disassociation, 150

Disassociations counter
- in Dashboard's 802.11 tab, 109

DS Channel counter
- in Host Table, 117

E

Enable Rogue AP Lookup option, 91

Enable Rogue Mobile Unit option, 91

Encryption options, 85

Enterasys RoamAbout
- installation notes and issues, 36
- installing in Windows 2000, 31
- installing in Windows NT, 25
- installing in Windows XP, 30
- using as a normal network adapter, 35

Errors counter
- in Global Statistics, 119

ESSID
- counter in Host Table, 117
- in Options dialog box, 84

Expert
- alarms for wireless networks, 146
- diagnoses, 137
- setting Wireless options, 90
- symptoms, 137
- Wireless alarms, 146
- Wireless features, 136
- Wireless object detail displays, 137

Export AP button, 95

exporting known addresses to csv file, 97

F

features (wireless), 99

G

Global Statistics, Wireless features, 118

H

Host Table
- HwAddr counter, 115
- Wireless features, 114

HwAddr counter, 115

I

IBSS networks, 81, 141, 145

importing addresses to the known address list, 97

In Bytes counter
- in Host Table, 115

In Pkts counter
- in Host Table, 115

Infrastructure networks, 81, 141, 145

installing
- Atheros AR5002X adapters, 7
- Cisco Aironet adapters, 53
- Enterasys adapters and drivers, 25
- ORiNOCO Gold adapters and drivers, 13
- Proxim adapters and drivers, 67
- Spectrum 24 adapters and drivers, 37
- Spectrum 24 Model 4121 on Windows 2000, 45

K

Keys Per Channel option, 89

known addresses
- adding from the Host Table, 92
- adding from the postcapture display, 93
- adding to the Expert's list, 92

L

local agent, creating, 79

M

Management Pkts counter
- in Dashboard's 802.11 tab, 107

Mcast/Bcast Fragmentation, 151
Mgmt Pkts counter
in Global Statistics, 120
Missing Fragment Number, 151
monitoring wireless networks, 81
Multicast counter
in Host Table, 115

O

Octets counter
in Global Statistics, 119
offline WEP decryption, 134
Order Pkts counter
in Dashboard's 802.11 tab, 107
ORiNOCO Gold
installing in Windows 2000, 19
installing in Windows NT, 13
installing in Windows XP, 17
using as a normal network adapter, 22
Out Bytes counter
in Host Table, 115
Out Errors counter
in Host Table, 116
Out Pkts counter
in Host Table, 115
Oversize counter
in Host Table, 116
Oversized WLAN Frame, 152

P

Packets counter
in Global Statistics, 119
PLCP Error, 147
PLCP Errors
as filter option, 133
PLCP Long Pkts counter
in Dashboard's 802.11 tab, 108
PLCP Short Pkts counter
in Dashboard's 802.11 tab, 107
PLCPs counter
in Dashboard's Detail tab, 105
post-analysis views for Wireless networks, 121
postcapture WEP decryption, 134
Probe Requests counter
in Dashboard's 802.11 tab, 109
Probe Responses counter
in Dashboard's 802.11 tab, 109
Proxim adapters
installing in Windows 2000, 69
installing in Windows XP, 67
monitoring 2Xurbo networks, 75
using as a normal network adapter, 72
PS Polls counter
in Dashboard's 802.11 tab, 110

R

Reassociation Failure, 152
Reassociation Requests counter
in Dashboard's 802.11 tab, 109
Reassociation Responses counter
in Dashboard's 802.11 tab, 109
Retry Pkts counter
in Dashboard's 802.11 tab, 107
in Host Table, 115
Rogue Access Point, 153
Rogue Access Point options, 90
Rogue Mobile Unit, 154
RTS counter
in Dashboard's 802.11 tab, 110
Runt WLAN Frame, 155

S

Same Transmitter and Receiver Address, 155
Security options
configuring, 89
Signal Curr counter
in Host Table, 117
Signal Level counter
in Global Statistics, 120
Signal Max counter
in Host Table, 117
Signal Min counter
in Host Table, 117
Single Key Set option, 89
Sniffer Configuration options, 83
Spectrum 24

installation notes and issues, 51
installing in Windows 2000, 45
installing in Windows NT, 37
installing in Windows XP, 43
troubleshooting installation issues, 42
using as a normal network adapter, 50
Symptom in Expert analysis, 137

T

Thresholds
Monitor, 113
Transmitter Address Is Broadcast, 155
Transmitter Address Is Multicast, 155
triggers
and channel surfing, 84
Type counter
in Host Table, 115

U

Undersize counter
in Host Table, 116
Update Time counter
in Host Table, 118
utilization calculations (wireless), 103

W

WEP decryption
postcapture, 134
WEP ICVs
as filter option, 133
counter in Dashboard's Detail tab, 105
counter in Host Table, 117
WEP Key counter
in Host Table, 117
WEP Pkts counter
in Dashboard's 802.11 tab, 107
WEP-ICV Error, 156
Windows 2000
installing the Atheros AR500ZX, 9
installing the Cisco Aironet, 60
installing the Enterasys RoamAbout, 31
installing the ORiNOCO Gold, 19
installing the Proxim adapters, 69
installing the Spectrum 24, 45
Windows NT
installing the Cisco Aironet, 53
installing the Enterasys RoamAbout, 25
installing the ORiNOCO Gold, 13
installing the Spectrum 24, 37
Windows XP
installing the Atheros AR500ZX, 7
installing the Cisco Aironet, 58
installing the Enterasys RoamAbout, 30
installing the ORiNOCO Gold, 17
installing the Proxim adapters, 67
installing the Spectrum 24, 43