WildPackets

AiroPeek™
AiroPeek NX™

User Manual

AiroPeek for Windows, version 2.0

AiroPeek NX for Windows, version 2.0

WildPackets, Inc.
1340 Treat Blvd., Suite 500
Walnut Creek, CA 94597
USA

(925) 937-3200

www.wildpackets.com

AiroPeek Contents

Introduction

In this Chapter:

Welcome to AiroPeek, the award-winning wireless network traffic and protocol analyzer from WildPackets. AiroPeek helps network administrators meet the most demanding 802.11(a, b, g) wireless LAN (WLAN) network troubleshooting and monitoring challenges.

Designed for IT professionals at all levels of experience, AiroPeek's easy-to-use interface lets even novice users get up to speed quickly and efficiently. From troubleshooting a local network to maintaining distributed networks in the enterprise environment, AiroPeek is an indispensable tool.

AiroPeek is a feature-rich wireless analyzer that incorporates many advanced capabilities for monitoring and troubleshooting wireless LANs, including:

- Full decodes for 802.11a, 802.11b, and 802.11g WLAN standards
- Security Audit template with pre-defined filters
- Scan/surf by channel(s), ESSID or BSSID
- Display of data rate, channel, and signal strength for each packet
- WEP (Wired Equivalent Privacy) decryption, on-the-fly or offline

AiroPeek, standard and NX

This manual serves for two WildPackets products, AiroPeek standard and AiroPeek NX. The two share many features. When the text refers to “AiroPeek” without further qualification, it applies equally to either product. The sections below describe the primary differences between the two products.

AiroPeek standard

AiroPeek standard offers all the features of a great wireless network analysis tool at an affordable price. In addition, the ***Conversations*** view in Capture windows and Packet File windows is unique to AiroPeek standard. For more about the ***Conversations*** view, please see “Conversations” on page 183.

AiroPeek standard does not offer the Expert analysis functions, and does not show the ***Expert*** or ***Peer Map*** views found in AiroPeek NX.

AiroPeek NX

AiroPeek NX brings the power of Expert Analysis to AiroPeek. This real-time expert analysis tool has all the features of AiroPeek standard plus an advanced set of expert troubleshooting and diagnostic capabilities, expert problem detection heuristics, and a graphical view of pair-wise communications. The following features are unique to AiroPeek NX:

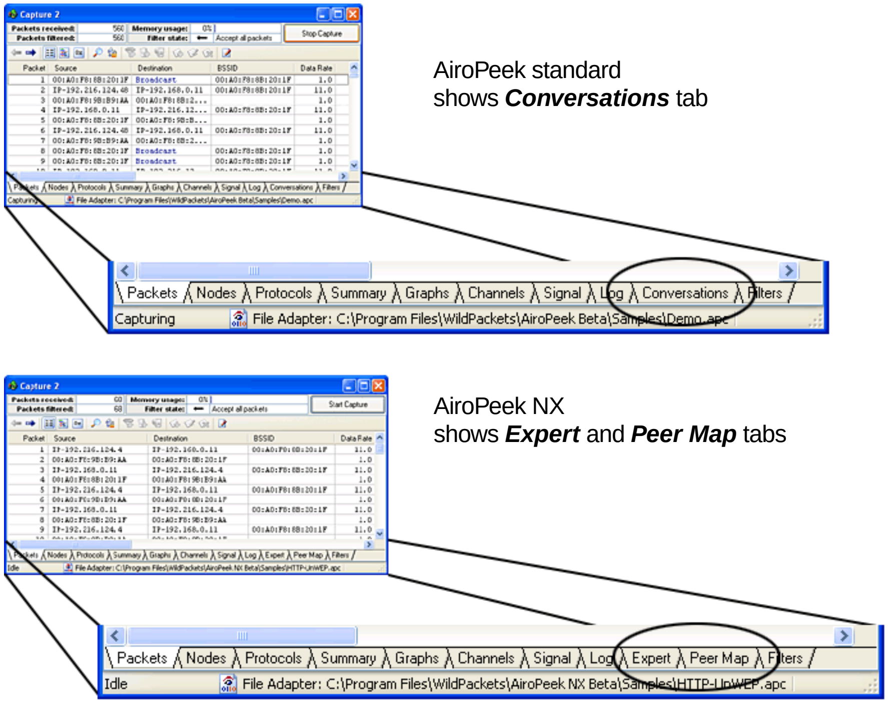
- The ***Expert*** view in Capture windows and Packet File windows provides Expert Analysis of 113 aspects of network performance in real time.
- You can fine tune the parameters for any Expert diagnostic item and get instant help with problem *Description*, *Possible Causes*, and *Possible Remedies* in the **Expert ProblemFinder Settings** window.
- You can save and reload customized Expert diagnostic settings from the **Expert ProblemFinder Settings** window.
- The ***Peer Map*** view of Capture windows and Packet File windows creates a continuously updated graphical view of traffic between pairs of network nodes, showing volume, protocol, node address, node type and more. Full customization lets you identify problems and anomalies quickly and intuitively.

For more about the Expert analysis functions, see Chapter 5, “Expert View and Expert ProblemFinder” on page 103. For more about the Peer Map, see Chapter 6, “Peer Map” on page 121.

The ***Conversations*** view, found in AiroPeek standard, is not present in AiroPeek NX. The ***Expert*** view provides all of the same functionality plus the expert features described above.

Differences in user interface

Where their features are different, AiroPeek standard and AiroPeek NX will show different items in their user interface. In particular, Capture windows (Figure 1.1) and Packet File windows will show different views and view tabs depending on the version of the program.



Packets received: 560 | Memory usage: 0%
Packets filtered: 560 | Filter state: ⟵ Accept all packets

Packet	Source	Destination	BSSID	Data Rate
1	00:A0:F8:8B:20:1F	Broadcast	00:A0:F8:8B:20:1F	1.0
2	IP-192.216.124.48	IP-192.168.0.11	00:A0:F8:8B:20:1F	11.0
3	00:A0:F8:9B:B9:AA	00:A0:F8:8B:2...		1.0
4	IP-192.168.0.11	IP-192.216.12...	00:A0:F8:8B:20:1F	11.0
5	00:A0:F8:8B:20:1F	00:A0:F8:9B:B...		1.0
6	IP-192.216.124.48	IP-192.168.0.11	00:A0:F8:8B:20:1F	11.0
7	00:A0:F8:9B:B9:AA	00:A0:F8:8B:2...		1.0
8	00:A0:F8:8B:20:1F	Broadcast	00:A0:F8:8B:20:1F	1.0
9	00:A0:F8:8B:20:1F	Broadcast	00:A0:F8:8B:20:1F	1.0

Capturing | File Adapter: C:\Program Files\WildPackets\AiroPeek Beta\Samples\Demo.apc

AiroPeek standard
shows ***Conversations*** tab

Packets received: 60 | Memory usage: 0%
Packets filtered: 68 | Filter state: ⟵ Accept all packets

Packet	Source	Destination	BSSID	Data Rate
1	IP-192.216.124.4	IP-192.168.0.11	00:A0:F8:8B:20:1F	11.0
2	00:A0:F8:9B:B9:AA	00:A0:F8:8B:20:1F		1.0
3	IP-192.168.0.11	IP-192.216.124.4	00:A0:F8:8B:20:1F	11.0
4	00:A0:F8:8B:20:1F	00:A0:F8:9B:B9:AA		1.0
5	IP-192.216.124.4	IP-192.168.0.11	00:A0:F8:8B:20:1F	11.0
6	00:A0:F8:9B:B9:AA	00:A0:F8:8B:20:1F		1.0
7	IP-192.168.0.11	IP-192.216.124.4	00:A0:F8:8B:20:1F	11.0
8	00:A0:F8:8B:20:1F	00:A0:F8:9B:B9:AA		1.0
9	IP-192.216.124.4	IP-192.168.0.11	00:A0:F8:8B:20:1F	11.0

Idle | File Adapter: C:\Program Files\WildPackets\AiroPeek NX Beta\Samples\HTTP-UnWEP.apc

AiroPeek NX
shows ***Expert*** and ***Peer Map*** tabs

Figure 1.1 Detail of Capture window view tabs in AiroPeek standard and AiroPeek NX

AiroPeek standard includes the ***Conversations*** view and all its associated features, but does not include the ***Expert*** or the ***Peer Map*** views, nor any of the features associated with them. AiroPeek NX does not have a ***Conversations*** view, but has the expert analysis features associated with the ***Expert*** and ***Peer Map*** views.

Except when describing the ***Conversations*** view, the screenshots in this manual are taken from the AiroPeek NX version of the program. Most screenshots would appear identical whether taken from one version or the other. With the exception of the differences in view tabs (described above), where a screenshot is particular to one program version, the figure title shows this as “AiroPeek standard” or “AiroPeek NX.”

New features

A complete list of new features is available in the Readme file. The following section highlights some of the most important new features. Except as noted below, these features are new to both AiroPeek standard and AiroPeek NX.

Use multiple adapters simultaneously

AiroPeek is the first wireless analyzer to allow multiple simultaneous capture sessions, each using a different adapter. This ability is limited only by the number of adapters available and the processing power of the local host. Multiple Capture windows can still capture from the same adapter, when, for example, you want to separate different types of traffic on one segment. Now multiple adapters can be used just as easily to analyze traffic on completely different network segments or RF bands at the same time. For details, please see “Capture options: adapter” on page 62.

Nested view of 802.11 nodes

The ***802.11*** view of **Node Statistics** (and the ***802.11*** view of the ***Nodes*** view of Capture windows and Packet File windows) now shows nodes nested in a hierarchy under their ESSID and BSSID. The nested view allows you to see at a glance which stations are associated with which access points, and to track not only the nodes on your network but the relationship between them. In AiroPeek NX only, you can also show the Trust setting for all nodes and change the setting for any node directly from within the ***802.11*** view. For details, please see “802.11 view of node statistics” on page 155.

Trusted, known, and unknown nodes

In AiroPeek NX only, you can use the Name Table to set a new attribute called Trust for any physical address in the Name Table. You can assign a value of Trusted, Known, or Unknown to any node. The default value, assigned to any node that is automatically added to the Name Table, and assumed for any node not listed there, is Unknown. You can assign a value of Trusted to the devices that belong to your own network. The intermediate value of Known lets you identify familiar sources that are beyond your own control, such as an access point in a neighboring office. You can set these values in the same way as any other Name Table attributes, or you can edit the Trust value for any node by selecting from the context menu of the ***802.11*** view of either the **Node Statistics** window or the ***Nodes*** view.

Trust values are very quick to set up, and because they are part of the Name Table, you can easily edit, save, and import this information. You can save separate versions of the Name Table for different locations, segments, or networks.

AiroPeek NX uses the Trust information in the ***802.11*** view of **Node Statistics**, and in **Summary Statistics**. You can set alarms and send notifications based on Trust. The ***Expert*** can also use Trust information. Setting the Trust attributes for your network makes intrusion detection fast, accurate, and easy. For details, please see “Trusted, known, and unknown nodes” on page 135.

New graphs view

The new ***Graphs*** view of Capture windows and Packet File windows allows great flexibility in the display of statistics. You can add to, delete, rearrange, create, edit, export, and import graphs of a wide range of formats, each based on single or multiple statistics from the current Capture window. You decide which statistics belong in the same graph, how they should be portrayed, and which graphs belong in the ***Graphs*** view. You can create complex or simple suites of graphs optimized for troubleshooting particular classes of problems, save these collections as named *.gph files, and reload them in a matter of a few clicks. You can save statistics from these graphs as one-off reports or save them periodically in any one of several formats. For a complete view of all the custom graphing tools available in AiroPeek, including the new ***Graphs*** view, please see Chapter 10, “Graphs of Monitor and Capture Statistics” on page 193.

RFGrabber Probe

The RFGrabber Probe™ is a separately purchased hardware device that acts like a "listen-only" access point, allowing you to capture and monitor WLAN traffic in a remote location and stream the results to AiroPeek via TCP/IP over your wired network. You can connect to any network accessible RFGrabber Probe just as you would to any other network adapter: by selecting it in the ***Adapter*** view of either the **Monitor Options** or the **Capture Options** dialog. For a detailed look at RFGrabber, please see Chapter 14, "RFGrabber Probe" on page 283.

VoIP analysis tools

The new VoIP Analysis Module, along with new and improved decoders and (in AiroPeek NX only) new and improved Expert diagnostics, combine to make AiroPeek an even more powerful tool for troubleshooting VoIP problems. AiroPeek decodes the standard VoIP protocols and performs extensive analysis of RTP, the core VoIP protocol. AiroPeek NX analyzes conversations for excessive packet loss, excessive jitter, out of sequence packets, late packet arrival, and more.

Monitor statistics and trending

Users familiar with earlier versions of AiroPeek should note that "global statistics" are now called "Monitor statistics." The new ability to use multiple adapters makes this much more than a name change. Now you can focus the streamlined statistics collection of Monitor statistics—and the related alarm functions—on any adapter, and switch from one to another with ease. The collection of Monitor statistics is entirely independent from packet capture. For details, please see "Selecting an adapter for monitor statistics" on page 18.

Improved Statistics Output options offer multiple new ways to create periodic snapshots of network conditions. You can output statistics in a variety of formats that make it easy to support trending and historical analysis. For a complete discussion of output from Monitor statistics, please see "Statistics output views" on page 188.

Make notes in packet files

The new Note tools let you add text notes to any packet(s) in the Packet List of Capture windows or Packet File windows. You can create, edit, format, or delete notes. Assign the same note to multiple packets in a single operation, or create a default note and add it to any packet(s) in two clicks. You can step through the notes, forward or backward, in packet list order. When you save packets in AiroPeek packet file format, the notes are saved alongside them. These notes are quicker to make and easier to use than notes on paper. For details, see “Making notes on packets and packet files” on page 75.

Support for Oracle, Sybase, and SQL Server

The new SQL Analysis Module helps you track Structured Query Language (SQL) traffic on your network, by providing both detail and summary decodes for some of the important TNS (Oracle) and TDS (Sybase and Microsoft SQL Server) control packets. For details, see “SQL analysis module” on page 280.

New expert diagnoses

AiroPeek NX has added more than two dozen new Expert diagnoses, including: broadcast storm, Kerberos ticket denied, LDAP slow response time, Oracle logon denied, Oracle slow response time, SQL Server fatal error, VoIP H.225 RAS reject, and many more. In addition, the ***Expert*** view now diagnoses a number of security issues ranging from breaches of security policy to denial of service (DOS) and man in the middle (MIM) attacks. For details, see Chapter 5, “Expert View and Expert ProblemFinder” on page 103.

New and improved packet decoders

AiroPeek now provides new and improved packet decoders, including: Cisco Skinny, TDS, TNS, RAS, VoIP (SIP, SDP, SAP, SCCP, more H.245), more Kerberos, ZeroConf, and DNS.

In addition, AiroPeek can identify the next generation 802.11 WLAN encryption and authentication methods, including encryption using enhanced keying methods such as TKIP (WPA) and CKIP, and improved authentication methods such as LEAP, LEAP/TLS, and PEAP. For details about tracking the use of these methods, please see “802.11 view of node statistics” on page 155.

These and all the features of AiroPeek standard and AiroPeek NX are covered in this manual. For a brief overview of some key program functions, please see the Quick Tour, available from the **Start Page**, or by choosing **Quick Tour** from the **Help** menu in the program main window.

Before beginning to use the software, please see Chapter 2, “Installing and Configuring” on page 11, to insure the program is installed in the proper system environment for maximum operability. Please refer to the Readme.htm file for other important information about program installation and use. Please visit the support pages on our website at http://www.wildpackets.com/support for the most current list of supported 802.11 WLAN adapters.

WildPackets Academy

WildPackets Academy offers comprehensive network analysis training centered on practical applications of protocol analysis techniques using EtherPeek and AiroPeek. Courses include the following topics:

- Foundations of Network Protocol Analysis
- Network Troubleshooting Methods
- TCP/IP Protocol Analysis Methods
- Wireless LAN Administration

Please see Appendix E, “Resources” on page A-47 for details on WildPackets Academy’s educational resources and a list of network analysis courses. For a complete course catalog, and information about web-delivered training and class schedules, please see the WildPackets Academy web site at: http://www.wildpackets.com/services.

Conventions used in this manual

This section describes the naming conventions used in this manual for WildPackets products and for IEEE wireless standards. It also describes how typefaces are used in this manual to distinguish elements of the user interface from ordinary text.

Names of products and wireless standards

As noted above, this manual covers two WildPackets products: AiroPeek standard and AiroPeek NX. Many features are common to both programs. Where this manual refers to “AiroPeek” without further qualification, the text applies equally to both versions. Where a feature is unique to one version, the version is referred to specifically as “AiroPeek standard” or “AiroPeek NX.”

AiroPeek analyzes traffic on networks conforming to either of the two most recent revisions of the IEEE 802.11 WLAN standard: 802.11a and 802.11b. In addition, the current version of AiroPeek adds support for, and includes drivers for pre-standards implementations of, the IEEE 802.11g WLAN standard. The IEEE 802.11a standard defines the use of Orthogonal Frequency Division Multiplexing (OFDM) in the 5 GHz band to achieve data rates up to 54 Mbps.   The IEEE 802.11b standard defines the use of Direct Sequence Spread Spectrum (DSSS) in the 2.4 GHz band to achieve data rates up to 11 Mbps. The new 802.11g standard uses the same OFDM method and achieves the same high data rates as the 802.11a standard, but operates in the same spectrum as the 802.11b standard.

Although quite distinct at the physical layer, at all higher layers these standards are virtually identical. The term “802.11 WLAN” is used throughout the text to refer to all three standards equally. Where certain features are unique to one type of network (channel numbers, for example), the text refers to them specifically as an “802.11a WLAN” or an “802.11g WLAN.” For a more complete discussion of wireless network standards, please see Appendix A, “Packets and Protocols” on page A-3.

Typographical conventions

This manual uses different typefaces to highlight elements that appear in the program user interface, and to distinguish these words and phrases from the rest of the text. In addition, keyboard shortcuts and function keys used to access program functions are set apart using different typefaces.

Table 1.1 **Typographical conventions**

Example	Uses
Edit Name dialog	The titles of dialogs and windows are shown in bold Helvetica.
File menu	Menu items are shown in bold Helvetica.
View > **Color** > **Destination**	A sequence of menu choices is sometimes shown using right angle brackets or “greater than” signs. The example at left means “From the **View** menu, choose **Color**, and within that, choose **Destination**.”

Table 1.1 **Typographical conventions (continued)**

Example	Uses
Type **Ctrl + M**, or click **F4**	Keyboard shortcuts and function keys are shown in bold Helvetica. The plus sign in keyboard shortcuts means you must hold down the Control Key (**Ctrl**) while typing the letter indicated. Keyboard shortcuts are not case sensitive. Those few keyboard shortcuts which require the **Shift** key show that fact explicitly in the notation.
Start button	Labels on buttons are shown in bold Helvetica.
Packets view	The names of individual views of windows or dialogs are shown in bold oblique Helvetica. Views provide different sets of information within a single window or dialog. They are usually accessed by clicking on a tab labeled with the name of the view.
Absolute Time column	Column headings are shown in bold oblique Helvetica.
Link speed	All other text appearing in windows and dialogs, including any text to be entered by the user, is shown in oblique Helvetica.

Installing and Configuring

AiroPeek is easy to install and configure for a variety of operating environments. If you have AiroPeek installed on a laptop, you can easily and quickly reconfigure the program to match new conditions as you move from one network segment to another.

This chapter describes the system requirements for AiroPeek, explains how to install the program, and lists the components AiroPeek installs on your computer. It explains how to set up and run the program for the first time, and how to use system memory and application configuration files to keep AiroPeek operating smoothly in all supported environments.

Note: This manual does not describe how to install 802.11 WLAN network hardware and systems to create an 802.11 WLAN network. If you do not already have a functional 802.11 WLAN network, please see the documentation that accompanies your 802.11 WLAN hardware and computer.

Important! Under certain network or program configurations, AiroPeek can enable the user to monitor information that might be considered confidential. For example, some passwords may be viewable from AiroPeek if WEP is not implemented on your network, or if you configure AiroPeek to monitor the network as a peer WEP host. Because of this, you may want to prevent unauthorized access to the program. Consider limiting access to AiroPeek by not installing it on public machines and servers.

In this Chapter:

System requirements

This section describes the recommended system requirements for running AiroPeek. Please read this section before you launch the software.

The recommended system configuration for AiroPeek is:

- 600 MHz processor or better
- 256 MB RAM or better
- Windows 2000 (SP 3 or later) or Windows XP (SP 1 or later)
- Network capture requires a supported 802.11 WLAN interface (see below)

Note: Supported operating systems require users to have “Administrator” level privileges in order to load and unload device drivers, or to select a network adapter for the program’s use in capturing packets.

- Internet Explorer 5.5 or higher is required

Supported adapters and interface requirements

AiroPeek works with a variety of adapters for 802.11a, b, and g WLANs. Please check the Readme file and the WildPackets website at http://www.wildpackets.com/support for the most recent information about supported adapters.

Special drivers

AiroPeek requires the installation of a special NDIS driver for packet capture and to control a supported network adapter. Look in the Drivers folder for the driver for your card and operating system, and its installation instructions. Hyperlinks to the driver installation instructions are also provided from the Readme file, which appears on the completion of Installation, and from the **Start Page**.

Important! You must install the new NDIS driver, even if you have previously installed an earlier set with a previous version of AiroPeek standard or AiroPeek NX. Due to possible incompatibilities among device drivers, it is recommended that you uninstall earlier versions of the program before installing the latest version of AiroPeek.

Memory

You should install AiroPeek on a workstation or laptop with 256 MB of RAM or more for best performance. The number of packets that can be kept in the capture buffer is limited by the amount of available RAM, so the more memory available to the program, the larger the number of packets that can be analyzed simultaneously in real time, or the larger the packet trace that can be loaded into the program's memory for post-capture analysis. You control the size and use of the capture buffer in the ***General*** view of the **Capture Options** dialog, accessible through the **Capture** menu.

AiroPeek is monitor only

When AiroPeek is using an 802.11 WLAN network interface card (NIC) for Monitor statistics or packet capture, it puts the NIC into a “listen only” mode. Simultaneous network services on that interface are not supported. You may receive “Network cable unplugged” or similar messages. This is normal. After quitting the program, network services should be restored.

In order to use network services while AiroPeek is running, you must have access to the network through a second adapter. Alternatively, selecting either *None* or *File* as the adapter can free the NIC for network services, if the card supports this functionality. Please see our website at http://www.wildpackets.com/support for details about specific cards.

Installing AiroPeek

To avoid possible incompatibilities, it is recommended that you uninstall any earlier versions of AiroPeek before installing the latest version on your system. If AiroPeek detects an earlier version, the installer will offer you the option to uninstall it before installing the newer version. AiroPeek features a simplified setup procedure that automatically installs all of the program's components in their designated locations.

When you launch the Installer, the first window you will see is the Welcome screen, which tells you that AiroPeek is about to be installed on your machine.

The next screen contains the WildPackets Software License Agreement. Please read it carefully so that you understand our terms and conditions concerning possession and use of AiroPeek. You must accept the terms of the license agreement to continue the installation.

The next screen presents the Installation Notes from the Readme file.

The next screen in the setup program is the **User Information** dialog that requires you to enter a name, company name, and your serial number before the program can be installed and launched.

Next, the **Choose Destination Location** dialog suggests the default location in which to install AiroPeek. Use the **Browse** button to display the **Choose Folder** dialog, in which you can navigate to an alternate installation location.

If you have iNetTools installed, the **iNetTools Integration** dialog allows you to automatically set up AiroPeek's **Tools** menu to incorporate this IP test utility suite. For more on iNetTools, see "iNetTools" on page 46. Similarly, you will be offered the option to integrate other WildPackets tools, such as NetSense or ProConvert, if these products are already installed on your system. You can also add these and other software tools to the **Tools** menu after installation. Please see "Customizing the tools menu" on page 45 for details.

When the Installer has finished installing the program files, the final **Setup Complete** screen is displayed. From this dialog, you may choose to launch the program when installation is complete. The Readme file is displayed automatically.

AiroPeek components

The sections under the following headings describe each of the installed components. The location of these files and directories is described relative to the location in which you installed AiroPeek. The most typical location under Windows 2000 or XP would be C:\Program Files\WildPackets\AiroPeek, for AiroPeek standard, or C:\Program Files\WildPackets\AiroPeek NX for AiroPeek NX.

Alarms

The 1033\Alarms directory contains two sets of predefined alarms which you can load into the **Alarms** window using the **Import** button. You can also modify any of the alarms in either of these files. The two files are called Default Alarms.alm and Additional Alarms.alm. For more information about creating, editing, and using Alarms, please see "Alarms" on page 242.

Utilities

Two command line utilities are included with AiroPeek and installed in the Bin directory where AiroPeek is installed. PeekCat concatenates packet files. UnWepPeek uses a valid user supplied key set to decrypt WEP encrypted network data in AiroPeek (*.apc) packet files as a command line utility. See the respective Readme files in the Bin directory for details and usage.

Packet decoders

The modules that decode packets are installed in the Decodes directory in the same location as AiroPeek. These modules provide AiroPeek with the instructions it needs to display packet contents, based on the types of protocols used.

AiroPeek currently provides decoders for over 1,000 protocols and sub-protocols, including IP, IPv6, AppleTalk, DECnet, Netware IPX/SPX, SNA, NetBEUI, and more. For a complete list of protocols decoded, please check the support pages at: http://www.wildpackets.com/support.

In addition to the protocol decoders provided as standard issue with AiroPeek, a decoder SDK (Software Development Kit) is available for customizing or adding to AiroPeek's decoding capabilities. If you are interested in writing your own Packet Decoders, a document and source samples are provided in the Documents directory.

Note: Some programming knowledge is required to create packet decoders using the SDK.

Documents

AiroPeek ships with a number of developer tools which are installed in the 1033\Documents directory. Software developers can use these tools to extend or customize ProtoSpecs, Decoders, and Analysis Modules for unique environments. For example, you can customize AiroPeek to recognize a proprietary protocol while it is still in development. Please see the Readme file in the Documents directory for details. The Documents directory also contains PDF versions of the AiroPeek manual and Quick Tour.

Drivers

The Driver directory contains the AiroPeek drivers for supported adapters and operating systems, along with their installation instructions.

Filters

The 1033\Filters directory contains a file called Default.flt which is the default selection of filters for use with the program. You can create, modify or delete individual filters, and save and reload various assortments of filters in named *.flt files for use in different packet capture scenarios. The Filters directory also contains additional sets of filters which you may find useful.

Graphs

The 1033\Graphs directory contains the default set of graphs for the ***Graphs*** view of Capture windows and Packet File windows in a file called Default Graph.gph.

HTML

The 1033\HTML directory contains the Start Page and, in the Quick Tour subdirectory, the Quick Tour.

Names

The 1033\Names directory contains configuration files for Name Table entries you might want to install. The Default.nam file provides a starting configuration for the Name Table.

The Name Table lets you substitute symbolic names (words) for physical and logical network addresses (numbers) to make network activity shown in packet traces and statistics displays easier to grasp at a glance. The Name Table also holds user-specified information about ports or sockets and protocols. The Names directory contains a current IEEE list of vendor IDs, already formatted for import into the Name Table. The file is VendorID.nam. The list of vendor IDs allows you to substitute the name of the manufacturer for the first three bytes of the physical, or MAC (Media Access Control), addresses on your network. You can add to or modify the names as needed.

Analysis modules

The Plugins directory contains files of Analysis Modules that enhance the program’s analyzing capabilities. For a complete description of the Analysis Modules currently available with the program and their use, please see “Analysis modules shipped with AiroPeek” on page 262.

The 1033\PluginRes directory contains resource files for use by the Analysis Modules, including an XML file of SSIDs commonly assigned as factory defaults in new access points. Please check our support pages at http://www.wildpackets.com/support for the most recent list of default SSIDs.

Reports

The 1033\Reports directory contains XML, XSL and HTML templates along with related support files for use with the **Save Report** functions and with options available in the ***Statistics Output*** views of the **Capture Options** and **Monitor Options** dialogs. A Readme file in this directory contains detailed instructions for using and customizing output from statistics functions. Please see “Output from statistics” on page 187 for more details.

Samples

The Samples directory contains a variety of sample packet files in AiroPeek format and an associated name table file. You can use these files for testing, training, and to familiarize yourself with program function. Please see the Readme file in that directory for more details.

Security audit template

The 1033\Security Audit Template directory contains the capture template (Security Audit Template.ctf), the filters file (Security Audit Template.flt), and the Security Audit Readme which explains their use in detail. The Security Audit Template creates a Capture window which uses the special filters to scan for network anomalies.

Application data

Application data (such as your current names, filters, log files, and more) is cached in the Application Data folder. The default location of the Application Data folder is different for different operating systems. Under Windows 2000 or Windows XP, the default location is in a directory in the root drive where the operating system is installed (typically C:\) with the path name: Documents and Settings\(user name)\Application Data.

AiroPeek creates a subdirectory structure within these locations to cache application data. That subdirectory structure is: WildPackets\AiroPeek (for AiroPeek standard) or WildPackets\AiroPeek NX (for AiroPeek NX). For example, the AiroPeek NX application data for the Administrator of a Windows XP system would be cached in: C:\Documents and Settings\Administrator\Application Data\WildPackets\AiroPeek NX.

Setup and configuration

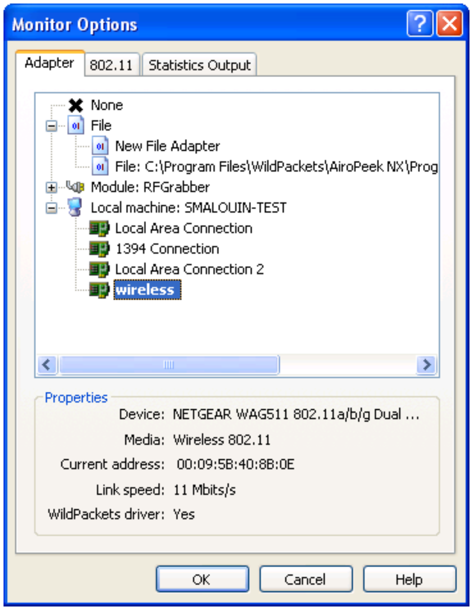
This section explains how to set up AiroPeek for the first time, how to set options for the workspace, list views, and fonts, how to optimize performance in heavy traffic environments, and how to alter the application's use of memory.

Selecting an adapter for monitor statistics

When you launch the program, you will be asked to select an adapter to use in collecting Monitor statistics. By default, the program presents the ***Adapter*** view of the **Monitor Options** dialog (Figure 2.1) on program start up.

Tip You can customize this program start up behavior in the ***Workspace*** view of the **Options** dialog, available by choosing **Options…** from the **Tools** menu. Please see "Workspace view" on page 27 for details.

The ***Adapter*** view of the **Monitor Options** dialog displays the names of all detected network interface cards (NICs) installed in your machine and a list of alternative adapter choices, arranged hierarchically by type. You can, for example, start AiroPeek without binding it to any adapter by choosing *None* in the ***Adapter*** view. You can choose to simulate network traffic by choosing a *File* as the adapter. If one or more separately purchased RFGrabber Probes are network accessible, you can choose one of them as the monitor adapter by selecting it under *Module: RFGrabber*. (For more about RFGrabber, please see Chapter 14, "RFGrabber Probe" on page 283.)



None
File
New File Adapter
File: C:\Program Files\WildPackets\AiroPeek NX\Prog
Module: RFGrabber
Local machine: SMALOUIN-TEST
Local Area Connection
1394 Connection
Local Area Connection 2
wireless

Properties

Device: NETGEAR WAG511 802.11a/b/g Dual ...
Media: Wireless 802.11
Current address: 00:09:5B:40:8B:0E
Link speed: 11 Mbits/s
WildPackets driver: Yes

Figure 2.1 Adapter view of the Monitor Options dialog

To choose an adapter for Monitor statistics, select a listed adapter or one of the alternate choices, then click **OK**.

To choose a file, expand the *File* item and select a previously used file or choose *New File Adapter*. Double-click on the item, or highlight it and click the **OK** button to make your choice. If you select *New File Adapter*, you will be asked to specify the file, using a standard file **Open** dialog. When you choose an AiroPeek packet file (one of those in the Samples directory, for example), the program cycles through the packets in that file, treating it as live traffic for purposes of calculating statistics. By choosing a file as the adapter, you can simulate network conditions for training or open other packet traces without being connected to an 802.11 WLAN network, or indeed without even having a supported NIC installed on your computer.

Tip AiroPeek remembers recently selected File adapters. To remove an adapter from the list, select the adapter, right click, and choose **Delete** from the context menu.

Selecting either *None* or *File* as the adapter can free the NIC for use in two-way network communications or for use as the Send Adapter, if the card supports this functionality.

Please see our website at http://www.wildpackets.com/support for details about specific cards.

Note: The physical layers of the various types of 802.11 WLAN (a, b, g) are quite distinct. When you select an adapter, AiroPeek displays only the channels and data rates appropriate to the protocol of the selected NIC or file.

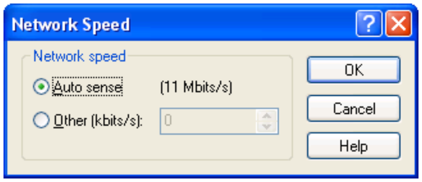
In addition to showing the currently selected adapter and its *Media* type, the ***Adapter*** view of the **Monitor Options** dialog shows the *Current address*, *Link speed*, and whether or not the *WildPackets driver* is installed for this adapter.

Important! Active name resolution and notifications using the email action require an active network connection. Because AiroPeek puts any NIC selected for Monitor or Capture functions into a “listen only” mode, network access while AiroPeek is running requires that a different network adapter must be installed for use by network services. Alternatively, selecting either *None* or *File* as the adapter can free a previously selected NIC for network services, if the card supports this functionality. Please see our website at http://www.wildpackets.com/support for details about specific cards.

Tip You can return to the ***Adapter*** view of the **Monitor Options** dialog by choosing **Select Monitor Adapter...** from the **Monitor** menu, or by double-clicking on the current Monitor statistics adapter, shown in the status bar at the bottom right of the main program window.

Network speed options

By default, AiroPeek auto-senses the network speed of the network adapter you select for its use. You may want to override this automatic behavior and set the network speed by hand in certain cases. The 802.11 WLAN protocol permits dynamic adjustment of transmission speeds to match changing conditions. Some statistics are derived from calculations based in part on the network speed. You may wish to set a nominal network speed for a particular adapter within AiroPeek to insure consistent statistics reporting.



Network Speed

Network speed

● Auto sense (11 Mbits/s)

○ Other (kbits/s): 0

Figure 2.2 Network Speed dialog

To override the automatic behavior and manually set the network speed AiroPeek should use in performing calculations based on a particular adapter, open the ***Adapter*** view in either the **Monitor Options** or the **Capture Options** dialog. Right click on the adapter whose speed you wish to set, and choose **Network Speed…** from the context menu to open the **Network Speed** dialog (Figure 2.2) for that adapter. Click the radio button beside *Other (kbits/s)* and enter the speed in kilobits per second. Click **OK** to close the **Network Speed** dialog, and click **OK** again to close the parent dialog, accepting your changes. The same network speed is assigned for all uses of a particular adapter, whether it is selected for use by Monitor statistics, Capture window(s), or both.

802.11 view

In the ***802.11*** view of the **Monitor Options** dialog or the **Capture Options** dialog, you can set the parameters the current adapter will use for channel selection or scanning, and for decryption of WEP (Wired Equivalent Privacy) encrypted packets. For channels, see “Scanning and choosing channels and access points” on page 21. For WEP, see “WEP encryption and AiroPeek” on page 24.

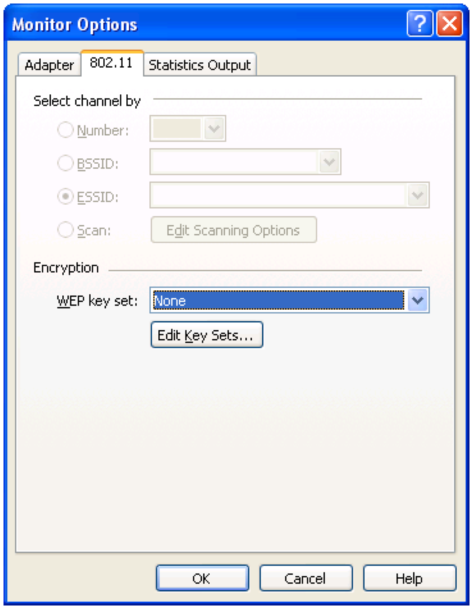
Important! The ***802.11*** view is identical in either the **Monitor Options** or the **Capture Options** dialog. Changes made in the ***802.11*** view of either dialog take effect immediately for all uses of a particular adapter, whether it is selected for use by Monitor statistics, Capture window(s), or both.

Tip You can access the features of the ***802.11*** view of the **Monitor Options** dialog directly from the main program status bar. Double-click in the current channel pane at the right of the status bar to open this view. Alternatively, you can right click in the current channel pane to access the main features of this view as a context menu. The equivalent functionality for any Capture window (giving access to the ***802.11*** view of the appropriate **Capture Options** dialog) is provided by the current adapter and current channel panes in the status bar of individual Capture windows.

Scanning and choosing channels and access points

You can specify the parameters AiroPeek will use with the current adapter to search for traffic on your 802.11 WLAN. In the ***802.11*** view of the **Monitor Options** dialog or the **Capture Options** dialog, you can tell AiroPeek to *Select channel by* the specified channel *Number*, or for traffic associated with the specified *BSSID* or *ESSID*. Alternatively, you can tell the program to *Scan* a range of channels according to the parameters set in the **Channel Scanning Options** dialog, which is opened by clicking the **Edit Scanning Options** button. Use the radio button to choose one of these options.

Use the drop-down list to choose a channel by its *Number*, or use the text entry field to specify the 6-byte hexadecimal identifier of the *BSSID* or enter the *ESSID*. You can also choose recently used values for either of these from the drop-down lists. The BSSID is, essentially, the MAC address of the base station or access point and is unique for each device. The ESSID is the ASCII name of the Extended Service Set, an infrastructure type network including at least two access points or base stations. To identify multiple base stations or access points as being part of the same ESS, a short string such as "engineering" is often used as the ESSID for all access points on the network. OEM configuration utilities often call the ESSID the "Network Name." When you choose *ESSID*, the NIC will search for the best signal among access points having the specified string as their ESSID.



Select channel by

○ Number:

○ BSSID:

● ESSID:

○ Scan: Edit Scanning Options

Encryption

WEP key set: None

Figure 2.3 802.11 view of the Monitor Options dialog

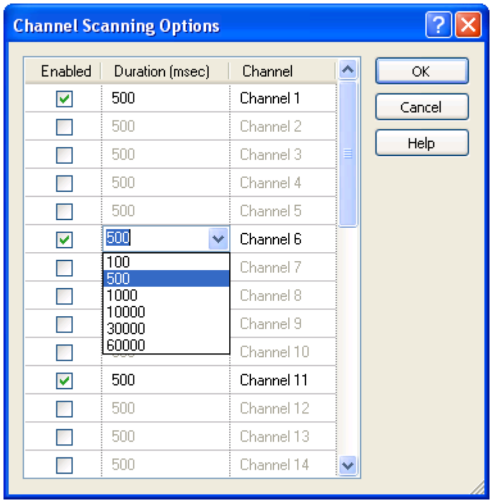
To scan for traffic on multiple channels, click the *Scan* radio button and click the **Edit Scanning Options** button to open the **Channel Scanning Options** dialog (Figure 2.4). The dialog presents a table with three columns: ***Enabled***, ***Duration (sec)***, and ***Channel***, listing the channels appropriate to the 802.11 WLAN protocol of the current adapter in ascending numerical order.

Note: The physical layers of the various types of 802.11 WLAN (a, b, g) are quite distinct. When you select an adapter, AiroPeek displays only the channels and data rates appropriate to the protocol of the selected NIC or file.

Check the checkbox in the ***Enabled*** column for a particular channel to include it in the scan. Alternatively, you can use the context menu (right click) in this column to **Enable All** or **Disable All** channels. Use the drop-down list in the ***Duration (msec)*** column to set the amount of time you want the program to spend listening on that channel. Click the **OK** button when you have set the scanning pattern to return to the ***802.11*** view. When you click **Apply** or **OK**, the program will begin scanning the channels you specified, in order, spending the amount of time you specified listening for traffic on each one. To stop the scanning process, open the ***802.11*** view and choose a different option.

Whether troubleshooting interference or optimizing the location and channel choice for new access points, the ability to scan multiple channels quickly can be invaluable. Channel scanning is often used in conjunction with the ***802.11*** view of **Node Statistics**, and with the ***Channels*** and ***Signals*** views of **Channel Statistics**. These views are available in Monitor Statistics or in Capture windows.

Note: If you have selected a multi-band adapter (supporting 802.11a and b, for example), you can scan any of the channels supported by that adapter. When setting the scan duration, however, you should allow time for the adapter to switch from one band to the other.



Enabled	Duration (msec)	Channel
☑	500	Channel 1
□	500	Channel 2
□	500	Channel 3
□	500	Channel 4
□	500	Channel 5
☑	500	Channel 6
□		Channel 7
□		Channel 8
□		Channel 9
□		Channel 10
☑	500	Channel 11
□	500	Channel 12
□	500	Channel 13
□	500	Channel 14

Figure 2.4 Channel Scanning Options view of the Options dialog

Note: 802.11a WLAN cards based on the Atheros chip set may support a proprietary mode called Turbo Mode (specific card vendors may use other names). Turbo Mode doubles the standard data rates and uses twice the RF spectrum specified for a normal channel in the 802.11a WLAN standard. For more information, please visit the support pages of our website, at: http://www.wildpackets.com/support.

When you have set the parameters in the ***802.11*** view, click **OK** to make your changes and close the **Monitor Options** dialog or the **Capture Options** dialog. To close the dialog without making any changes, click **Cancel**.

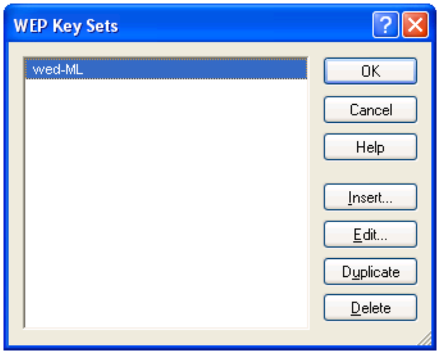
WEP encryption and AiroPeek

WEP (Wired Equivalent Privacy) is a data encryption technique supported as an option in the 802.11 WLAN protocol. The technique uses shared keys and a pseudo random number (PRN) as an initial vector (IV) to encrypt the data portion of network packets. The 802.11 WLAN network headers themselves are not encrypted.

Because WEP encrypts all the data above the 802.11 WLAN layers, it can prevent AiroPeek from decoding other network protocols and so prevent accurate troubleshooting of problems with TCP/IP, IPX, NetBEUI and so forth. To overcome this limitation, AiroPeek allows users to specify the WEP shared key set for their network. Using the shared key set, AiroPeek can decode the network data contained in 802.11 WLAN packets in the same way that every other station on the user’s network does. Because network administrators often have more than one network segment to take care of, AiroPeek can store multiple sets of shared keys, each with its own short name. This helps prevent errors in re-entering long key strings when switching from one set to another.

Important! WEP settings in AiroPeek are bound to a particular NIC or network adapter. Like other settings in the ***802.11*** view, they take effect immediately for all uses of a particular adapter, whether it is selected for use by Monitor statistics, Capture window(s), or both.

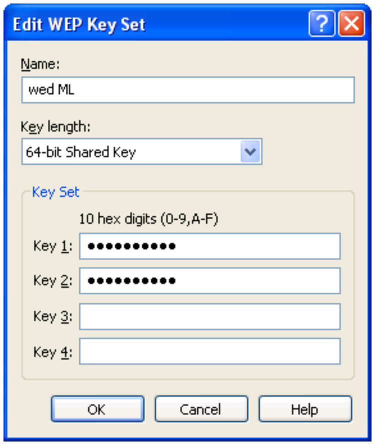
To enable AiroPeek to decrypt WEP-encrypted packets seen on a particular adapter, you must first select that adapter in either the **Monitor Options** or the **Capture Options** dialog. Choose the *802.11* tab to bring up the ***802.11*** view. In the *Encryption* section of the ***802.11*** view, use the drop-down list labeled *WEP key set* to choose a previously used key set for use in this session of AiroPeek. To use a key set, highlight its name in this list and click the **Apply** button to apply the new key set without closing the ***802.11*** view, or click **OK** to enable the new key set and close the parent dialog (either the **Monitor Options** or the **Capture Options** dialog).



wed-ML

Figure 2.5 WEP Key Sets window

Alternatively, you can click the **Edit Key Sets…** button to open the **WEP Key Sets** window. From this window you can create a new shared key set by clicking the **Insert…** button, or you can highlight an existing key set from the list and **Edit…**, **Duplicate** or **Delete** it by using the named buttons. Click **OK** to accept your changes and return to the ***802.11*** view of the **Options** dialog, or click **Cancel** to return to the ***802.11*** view of the **Monitor Options** or the **Capture Options** dialog without making any changes.



Name: wed ML

Key length: 64-bit Shared Key

Key Set

10 hex digits (0-9,A-F)

Key 1: ●●●●●●●●●●

Key 2: ●●●●●●●●●●

Key 3:

Key 4:

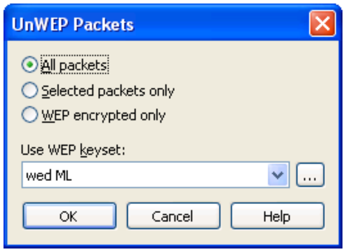
Figure 2.6 Edit WEP Key Set window

To create a new WEP key set, click the **Insert…** button in the **WEP Key Sets** window to open the **Edit WEP Key Set** dialog. Enter the *Name* for this key set. This name will appear in the **WEP Key Sets** window and in the drop-down list in the *Encryption* section of the ***802.11*** view of the **Monitor Options** or the **Capture Options** dialog, where you can enable each key set by name. Choose a *Key Length* from the drop-down list. You can choose *64-bit Shared Key*, *128-bit Shared Key*, *152-bit Shared Key*, or *User defined length Shared Key*. Enter the keys in hexadecimal notation in the text entry boxes labeled *Key 1* through *Key 4* in the section labeled *Key Set*.

Note: Hexadecimal numbers represent the values from zero through fifteen with a single digit each. They use the common Arabic numerals for values from 0 through 9, and use the first six letters of the Roman alphabet (in order) to act as digits representing the values from ten (A) through fifteen (F).

If you chose 64-bit shared key encryption, you will need to enter 10 hexadecimal digits (five bytes) to define each key. If you chose 128-bit, you must enter 26 hexadecimal digits (13 bytes). For the 152-bit keys, you must enter 32 hexadecimal digits (16 bytes). The *User defined length Shared Key* option provides for keys of arbitrary length (up to 506 hex characters, or 253 bytes). In all of these cases, the encryption algorithm adds an additional three bytes to the keys. When you have entered all the keys, click **OK** to create the new key set or click **Cancel** to close the **Edit WEP Key Set** window and return to the **WEP Key Sets** window without making any changes.

You can apply a particular WEP key set to all or some of the packets in a Packet File window or Capture window (when capture is stopped) by making it the frontmost or active window and choosing **UnWEP Packets…** from the **Tools** menu or from the (right click) context menu. This opens the **UnWEP Packets** dialog (Figure 2.7).



UnWEP Packets

● All packets
○ Selected packets only
○ WEP encrypted only

Use WEP keyset: wed ML

Figure 2.7 UnWEP Packets dialog

In the *Packet Options* section, use the radio buttons to choose whether to apply your WEP key set to *All packets*, *Selected packets only*, or to those packets in the current window which are *WEP encrypted only*. Below this section, beside the label *Use WEP key set*, use the drop-down list to choose an existing key set or click the button to the right marked with an ellipsis (**…**) to open the **WEP Key Sets** window and choose or create a key set from there. When you have made your selections, click **OK** to apply the chosen WEP key set to the chosen packets. A new Packet File window opens containing the results of the decryption. This new window has the name of the original target window, with the string "- *UnWEP*" appended to it.

If errors are encountered in performing the WEP decryption, a message dialog appears showing the error counts. Click **OK** to clear the message dialog. Errors can occur when WEP keys are applied to ill-formed target packets, such as those with CRC errors. If you see a large number of ICV errors, however, you have probably used the wrong key set. If you use the wrong key set, the decryption will still take place and AiroPeek will attempt to interpret the results, but the output will be unrelated to the original packet contents.

Note: In addition to the primary WEP capabilities described here, AiroPeek also comes with a convenient command line utility called UnWepPeek. When supplied with the correct key set, this utility can decrypt WEP-encrypted packets in files saved in the AiroPeek (*.apc) format, saving them to an output packet file as decrypted packets. The program (UnWepPeek.exe) is located in the \Bin directory where you installed AiroPeek. Please see the UnWepPeek.txt file in that same directory for instructions.

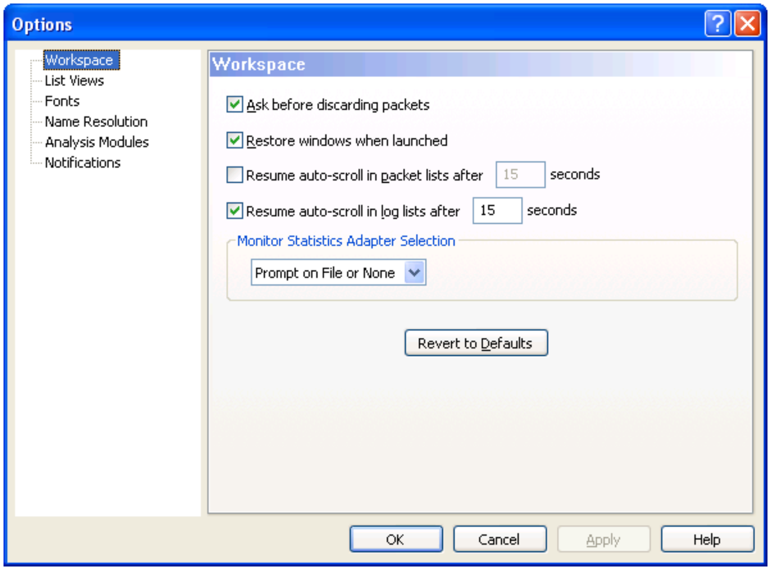
Options dialog

A number of options that apply to AiroPeek as a whole are set in the **Options** dialog. Choose **Options...** under the **Tools** menu to open the **Options** dialog. Click on the view names in the navigation pane to switch between views.

The **Options** dialog has six views, only the first three of which (***Workspace***, ***List Views***, and ***Fonts***) are described in detail in this section. Other views are described in detail in their respective sections of this manual. For the ***Name Resolution*** view, see "Name resolution view of the options dialog" on page 137. For the ***Analysis Modules*** view, see "Enabling and configuring analysis modules" on page 258. For the ***Notifications*** view, see "Notifications" on page 248.

Workspace view

Choose **Options...** under the **Tools** menu and click the *Workspace* item in the navigation pane to open the ***Workspace*** view of the **Options** dialog (Figure 2.8).



☑ Ask before discarding packets

☑ Restore windows when launched

☐ Resume auto-scroll in packet lists after 15 seconds

☑ Resume auto-scroll in log lists after 15 seconds

Monitor Statistics Adapter Selection: Prompt on File or None

Figure 2.8 Workspace view of the Options dialog

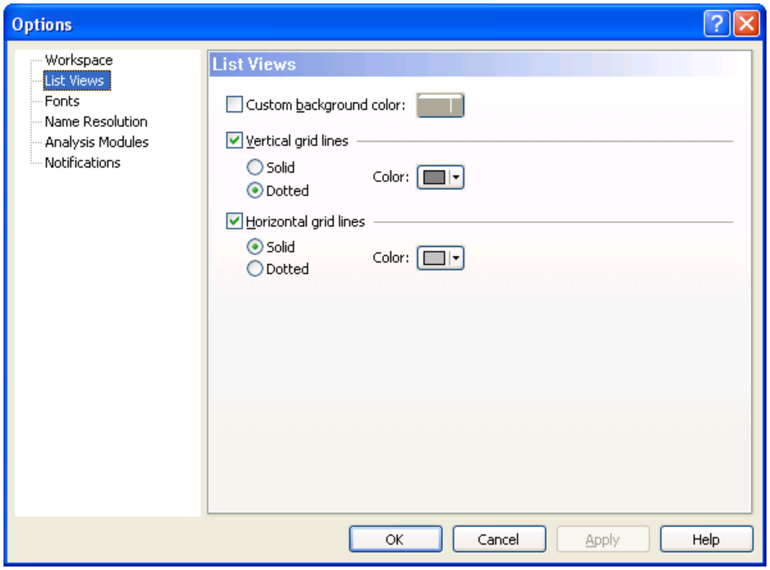
In the ***Workspace*** view, you can set default program behavior for scrolling, saving, and restoring open windows on program launch. The *Monitor Statistics Adapter Selection* drop-down list lets you control when (and whether) the program will present the ***Adapter*** view of the **Monitor Options** dialog on program launch. You can also restore AiroPeek to its initial default configuration by clicking the **Revert to Defaults** button in the ***Workspace*** view of the **Options** dialog.

CAUTION! When you **Revert to Defaults**, WEP key sets and other user-entered data will be lost.

Use the *Monitor Statistics Adapter Selection* drop-down list to tell AiroPeek whether it should *Always prompt* for a Monitor statistics adapter on program start up, *Prompt on File or None* (that is, only if the previous adapter selection was *File* or *None*), or *Never prompt* for selection of a Monitor statistics adapter. If you choose *Never prompt*, AiroPeek will attempt to use the previously selected adapter as the Monitor statistics adapter for new sessions of AiroPeek, but will never prompt for adapter selection. If the previously selected adapter is not found, AiroPeek starts silently with *None* as the adapter type.

List views view

Choose **Options...** under the **Tools** menu and click the *List Views* item in the navigation pane to open the ***List Views*** view of the **Options** dialog (Figure 2.9).



☐ Custom background color:

☑ Vertical grid lines

○ Solid
● Dotted
Color:

☑ Horizontal grid lines

● Solid
○ Dotted
Color:

Figure 2.9 List Views view of the Options dialog

In the ***List Views*** view you can set the background color of list displays and the style and color of vertical and horizontal grid lines. When you have made your choices, click **Apply** to see them applied to the display. Click **OK** to accept your changes or click **Cancel** to close the dialog without making any changes.

Fonts view

Choose **Options...** under the **Tools** menu and click the *Fonts* item in the navigation pane to open the ***Fonts*** view of the **Options** dialog.

The ***Fonts*** view allows you to set the font, style, and size of the text used throughout the program to display information discovered by AiroPeek. Examples include the Packet List pane of the ***Packets*** view and all statistics views of Capture windows and Packet File windows, as well as data presented in Monitor statistics windows.

In the ***Fonts*** view, click the **Choose Font…** button to open the **Font** dialog, displaying the fonts installed on the local system. From this dialog you can choose any locally installed font, set the style (bold, italic, and so forth) and size, and choose the *Script* type (for example, *Western* for western languages such as English, German, and so forth). The **Font** dialog shows a sample of the new font. Click **OK** in the **Font** dialog to accept your changes or click **Cancel** to close without changing the font.

The ***Fonts*** view also shows a sample of the font currently in use. To restore the font selection to the program's initial default, click the **Default** button.

When you have made your choices, click **Apply** to see them applied to the display. Click **OK** to accept your changes or click **Cancel** to close the dialog without making any changes.

Optimizing performance

The performance of AiroPeek depends on several factors, some of which the user can control more easily than others. Understanding how AiroPeek works is important to getting the most out of the application, particularly in demanding environments.

Processor speed

Faster processors, those running at higher clock rates, help AiroPeek performance in two major ways: they process packets more quickly and they pass packets among drivers, applications and buffers more quickly. Both help prevent AiroPeek from dropping packets.

Capture buffer and memory use

Packet capture in AiroPeek is handled by dedicated Capture windows, each with its own capture buffer of a user-defined size. In addition to setting the size of the capture buffer, the user also specifies how the Capture window will use that buffer. In the simplest arrangement, you can fill the buffer once and stop capture. Alternatively, you can use one of two methods to perform continuous capture. You can either discard all packets as the buffer becomes full, or you can use a ring buffer which continuously overwrites the same buffer, overwriting the oldest packets first. You can also save all packets captured with either of these continuous capture methods, periodically saving packets to disk before the buffer contents are discarded or overwritten. Each of these options, along with the size and number of capture buffers currently in use, has an effect on performance. Wrapping the buffer (emptying it in preparation for re-filling) can contribute to dropped packets, particularly when traffic volumes are high. Writing the contents of the capture buffer to disk before emptying can also allow some packets to be dropped in high traffic environments.

For a complete discussion of packet capture, including the **Capture Options** dialog, see Chapter 4, “Packet Capture” on page 49.

Starting AiroPeek from the command line

You can invoke AiroPeek from the command line using the following syntax:

```
Peek.exe [/autoload |/autostart ] [template1] [templateN]
```

The `/autoload` switch loads the specified Capture Template (*.ctf) file(s). The `/autostart` switch loads the specified template(s) and begins capture. Multiple templates may be listed, separated by a space. You can use the `*` (asterisk) character or the ? (question mark) character as wildcards in specifying template names, following standard Windows wildcard usage.

On a default install of AiroPeek NX, the command line would be started from:

```
C:\Program Files\WildPackets\AiroPeek NX
```

To automatically load template file capture1.ctf, for example, the command would be:

```
peek /autoload [template file location]\capture1.ctf
```

You can also invoke AiroPeek from the command line specifying an AutoCapture (*.wac) file as its object. For more about AutoCapture files, please see “AutoCapture” on page 91.

AiroPeek Menus and Toolbar

This chapter provides a complete list of AiroPeek menu commands, as well as an introduction to context menus and the AiroPeek toolbar. It also describes how to customize the **Tools** menu so you can launch such utilities as iNetTools directly from within AiroPeek.

In this Chapter:

AiroPeek menus

This is a listing of AiroPeek menus, with a brief description of each item’s function. It is intended as a quick reference only, as several important caveats and other significant details are left out of the descriptions. Menu items followed by ellipses (for example, **New…**) open a dialog or window. Most sub-headings are either toggle choices (on or off, with a ✔ checkmark indicating the entry is on); or groups of alternative choices, only one of which may be active at a given time. The active choice is indicated by a checkmark.

You can make menu choices either by navigating the menus or by using the **Ctrl** key combinations shown beside certain items in the menus and in the list below.

File menu

New…	**Ctrl + N**	Creates a new Capture window.
New From Template ➤		Creates a new Capture window whose layout matches the template selected by one of the two methods below.
Choose…		Opens a file **Open** dialog wherein you can navigate to the Capture window template of your choice.
(recent templates)		A list of the most recently used Capture window templates. Choose one to create a new Capture window using this template.
Open…	**Ctrl + O**	Opens an AiroPeek packet file or other supported file type in a new Packet File window.
AutoCapture ➤		
Create New…		Opens an empty **AutoCapture File** window in which you can define the parameters for a new AutoCapture file.
Edit Existing…		Opens a file **Open** dialog in which you can navigate to the AutoCapture (*.wac) file of your choice.
Close		Closes the active window or file.

Save All Packets…	**Ctrl + S**	Opens the **Save** dialog to save all packets in the active window.
Save Selected Packets…		Opens the **Save** dialog to save selected packets in the active window. This item is displayed as **Save Filters…** when the **Filters** window is active, as **Save Graph…** when a **Graph** window or the ***Graphs*** view of a Capture window or Packet File window is active, as **Save Names…** when the **Name Table** window is active, or as **Save Log…** when the **Log** window is active. When a statistics window is active, it changes to allow you to save the active statistics window or view, and will appear as, for example: **Save Node Statistics…** or **Save Size Statistics…**, and so forth.
Save Report…		Opens the **Save Report** dialog to choose the file format and location in which to save a report on any of several collections of statistics for the current Capture window or Packet File window. Formats include text (*.txt, *.csv), HTML, or XML.
Save Capture Template…		Opens the **Save** dialog to save the Capture Options of the current Capture window as a capture template (*.ctf), so it can be used to format subsequent new Capture windows.
Print Setup…		Opens the **Print Setup…** dialog for configuring printer functions.
Print…	**Ctrl + P**	Prints the active window in a format appropriate to its type.
Print Selected Packets…		Opens the **Print** dialog to allow you to print the ***Decode*** view of the selected packets as a single document. That is, without page breaks between packets.
Recent File		Following the **Print Selected Packets…** command is a numbered list of recently opened packet files, with the most recently opened listed first. You can select a file from this list to open it.
Exit	**Alt + F4**	Quits AiroPeek.

Edit menu

Undo	**Ctrl + Z**	Undoes the last edit.
Cut	**Ctrl + X**	Cuts the highlighted item(s) and copies to the clipboard.
Copy	**Ctrl + C**	Copies highlighted item(s) to the clipboard.
Paste	**Ctrl + V**	Pastes the current contents of the clipboard.
Insert	**Ins**	When the **Filters** window is active, opens the **Edit Filter** dialog; when the **Name Table** window is active, opens the **Edit Name** dialog.
Delete	**Del**	Deletes the highlighted item(s).
Clear All Packets	**Ctrl + B**	Deletes all packets from the active Capture window.
Hide Selected Packets	**Ctrl + H**	Removes selected packets from the display without deleting them. Hidden packets are not processed further.
Hide Unselected Packets	**Ctrl + Shift + H**	Removes unselected packets from the display without deleting them. Hidden packets are not processed further.
Unhide All Packets	**Ctrl + U**	Restores all previously hidden packets to normal status.
Select…	**Ctrl + E**	Opens the **Select** dialog, where you can use filters, ASCII or hex strings, packet length, and Analysis Modules to select captured packets.
Select Related Packets ➤		Searches for and selects packets that provide best matches to the highlighted item(s), based on the set of characteristics chosen from the list below.
By Source		Chooses packets with matching source address.
By Destination		Chooses packets with matching destination address.

By Source and Destination		Chooses packets with matching source and destination addresses.
By Protocol		Chooses packets with matching protocol.
By Port		Chooses packets with matching port.
By Conversation		Chooses packets sent between two nodes, using the matching protocol.
Select All	**Ctrl + A**	Selects all packets, text, or items in a window.
Select None	**Ctrl + D**	Removes all highlighting and selection.
Invert Selection		Unselects items that were selected and selects items that were unselected.
Find Pattern	**Ctrl + F**	Opens the **Find Pattern** dialog to search for a user-defined string in specified parts of packets.
Find Next	**F3**	Finds the next match in sequence to the previous **Find Pattern** search.
Go To…	**Ctrl + G**	Opens the **Go To** dialog where you can choose a packet number to jump to. If packets are selected, the number of the first selected packet is shown.
Go To Next Selected	**Ctrl + J**	Jumps to the next selected packet.

View menu

Filters	**Ctrl + M**	Opens the **Filters** window.
Name Table		Opens the **Name Table** window.
Log Window	**Ctrl + L**	Opens the **Log** window.
Alarms		Opens the **Alarms** window.
Display Format ➤		The following options control display format for nodes:

Name Table Entry Display using the names found in the Name Table when available (on by default).

Logical Address Display using the logical address of the node where available (on by default).

Physical Address Display using the hardware (MAC) address only.

Color ➤ The following options control the use of color in ***Packets*** views and other displays:

Source Use the color assigned to the source node.

Destination Use the color assigned to the destination node.

Protocol Use the color assigned to the protocol.

Filter Use the color assigned to the filter that allowed the packet to be captured.

Flag Use the color assigned to flagged packets.

Independent Each item uses its own color.

No Color Use no color coding in ***Packets*** view and other displays.

Toolbar Operates as a toggle setting. When enabled (the default), displays toolbar of convenient button versions of many of these menu commands.

Status Bar Operates as a toggle setting. When enabled (the default), displays status alerts, the current adapter and the current channel, BSSID, or ESSID in a bar at the bottom of the main program window.

Capture menu

Start Capture	**Ctrl + Y**	Toggles the packet capture function. When capture is active, the item is displayed as **Stop Capture**. When the active window has a Start Trigger, this item can display as **Start Trigger** to start the trigger or **Abort Trigger** to abort the trigger process.
Capture Options…		Opens the **Capture Options** dialog, where you can use the various views to set ***General*** properties such as the capture buffer options, and specify the ***Adapter***, ***Triggers***, ***Filters***, and ***Statistics Output*** options for the active Capture window.

Send menu

Initiate Send	**Ctrl + I**	Starts sending packets using the parameters you set in the **Send Window**.
Transmit One	**Ctrl + T**	Sends one copy of the designated Send Packet.
Send Selected Packets		Sends selected packets onto the network.
Set Send Packet		Designates a Send Packet.
Edit Send Packet...		Opens the designated Send Packet in a Decode window with edit capabilities.
Send Window		Opens the **Send Window**, where you can control transmissions from AiroPeek.
Select Send Adapter…		Opens the **Select Send Adapter** dialog in which you can choose an adapter to use in performing Send functions.

Monitor menu

Nodes	**Ctrl + 1**	Opens the monitor **Node Statistics** window.

Protocols	**Ctrl + 2**	Opens the monitor **Protocol Statistics** window.
Network	**Ctrl + 3**	Opens the monitor **Network Statistics** window.
Size	**Ctrl + 4**	Opens the monitor packet **Size Statistics** window.
Summary	**Ctrl + 5**	Opens the monitor **Summary Statistics** window.
History	**Ctrl + 6**	Opens the monitor **History Statistics** window.
Channel	**Ctrl + 7**	Opens the monitor **Channel Statistics** window.
Statistics Output…		Opens the ***Statistics Output*** view of the **Monitor Options** dialog, where you can specify that the program should periodically write Monitor statistics to text, XML, or HTML files in a user-specified directory.
Monitor Statistics		Operates as a toggle setting. When enabled (the default), collects all network statistics, independent of any Capture window.
Reset Statistics		This action clears all accumulated Monitor statistics information and resets all values to zero.
Select Monitor Adapter…		Opens the ***Adapter*** view of the **Monitor Options** dialog, where you can select an adapter for use in collecting Monitor statistics.

Tools menu

UnWEP Packets…	Opens the **UnWEP Packets** dialog, where you can choose a WEP key set and apply it to all, selected, or only WEP encrypted packets in the current Capture window or Packet File window.
Options…	Opens the **Options** dialog where you can specify default program behavior in the areas corresponding to each of this dialog's views: ***Workspace***, ***List Views***, ***Name Resolution***, ***Analysis Modules***, and ***Notifications***. From the ***Workspace*** view of this dialog you can also globally restore program defaults.

Customize…		Opens the **Customize Tools Menu** dialog from which you can add items to the **Tools** menu, allowing you to launch other programs from within AiroPeek. Use this dialog to add utilities from iNetTools, for example, to the AiroPeek menu.

Window menu

Cascade		Arranges all open windows one behind the other, with only the tops of those behind showing above the others.
Tile Vertically		Fills the screen with open windows, arranged side-by-side.
Tile Horizontally		Fills the screen with open windows, arranged one above the other.
Arrange Icons		Lines up the icons of minimized open files.
Next	**Ctrl + Tab**	Makes the next window in sequence the active window.
Previous	**Ctrl + Shift + Tab**	Makes the previous window in sequence the active window.
Close All		Closes all open windows.

At the bottom of the **Window** menu is a numbered list of open windows, with a checkmark beside the name of the active or front-most window. Selecting a window from this list makes it the active window and brings it to the front of the display.

Help menu

Help Topics	**F1**	Launches the Windows Help function for AiroPeek.
Show Start Page		Opens the **Start Page**.

Readme

Opens the Readme file, containing information about the program which may have appeared since the publication of the current manual.

Quick Tour

Opens the AiroPeek Quick Tour, introducing some of the key program features.

WildPackets on the Web ➤

The following indented items will launch the default Internet browser and load the appropriate page from the WildPackets website.

Product News

Loads the latest product news about AiroPeek and related WildPackets products.

Technical Support

Loads the technical support pages.

Training

Loads pages describing WildPackets' extensive courses in AiroPeek and related network troubleshooting tools and techniques.

WildPackets Home Page

Loads the WildPackets home page.

About AiroPeek

Appears as **About AiroPeek NX** in AiroPeek NX, and as **About AiroPeek** in AiroPeek standard. Displays the AiroPeek about box, including the last 10 characters of the serial number of your copy, and the support function, described below.

Support…

Click the **Support…** button in the **About AiroPeek** dialog to display key system and program information useful in troubleshooting and technical support. You can also save this information to a text file from this dialog.

Context menus

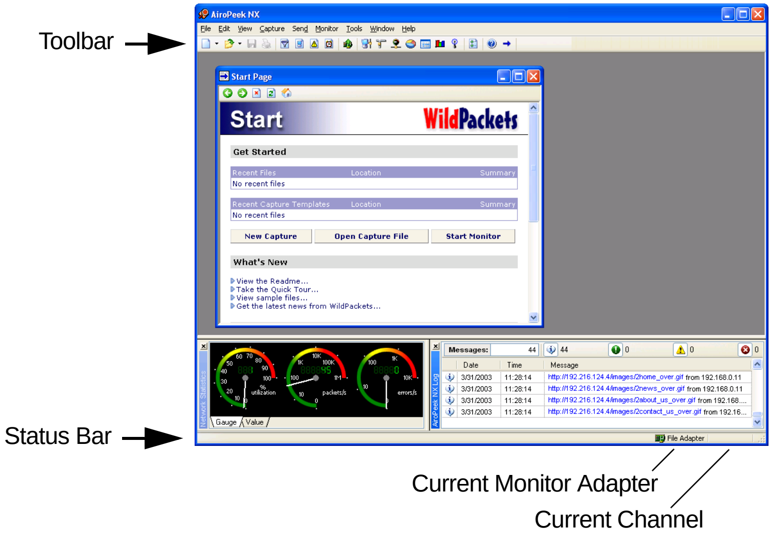
Context-specific menus are available in most windows of AiroPeek by right-clicking inside the window. The content of these menus changes with the active window and depends in some cases on whether or not items are selected.

Main program window start page and tools menu

This section describes two useful features of the AiroPeek main program window, the toolbar and status bar, and describes the **Start Page** which appears on program start-up under the default settings. It also shows how to customize the **Tools** menu by adding other programs, and describes one of those programs in detail: WildPackets' IP test suite, iNetTools.

AiroPeek toolbar

You can show or hide the toolbar for AiroPeek by selecting or deselecting the **Toolbar** item in the **View** menu. The toolbar provides button navigation for frequently-used tasks in AiroPeek. The name of each button's function appears when the cursor is moved over the button.



Recent Files	Location	Summary
No recent files		

Recent Capture Templates	Location	Summary
No recent files		

Messages: 44 | 44 | 0 | 0 | 0

Date	Time	Message
3/31/2003	11:28:14	http://192.216.124.4/images/2home_over.gif from 192.168.0.11
3/31/2003	11:28:14	http://192.216.124.4/images/2news_over.gif from 192.168.0.11
3/31/2003	11:28:14	http://192.216.124.4/images/2about_us_over.gif from 192.168....
3/31/2003	11:28:14	http://192.216.124.4/images/2contact_us_over.gif from 192.16...

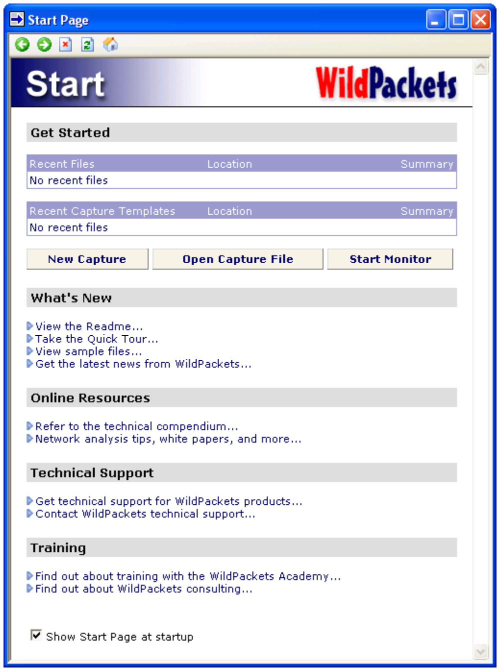
Figure 3.1 Main program window, showing location of Toolbar and Status Bar

AiroPeek program window status bar

Located at the bottom of the main program window, the main program status bar shows brief context-sensitive messages on the left and the current Monitor statistics adapter and channel on the right. You can click on the current adapter item to open the ***Adapter*** view of the **Monitor Options** dialog. Use this view to select an adapter for use in collecting Monitor statistics. When an adapter other than *File* or *None* is selected, the current channel item to the right shows the channel, BSSID or ESSID being scanned. Double-click in the current channel item to open the ***802.11*** view of the **Monitor Options** dialog, or right click to open a context menu with a summary of those same choices displayed. Choose **Status Bar** under the **View** menu to toggle the display of this main program status bar. A checkmark appears beside this item when it is enabled, as it is by default.

Start Page

The first time you open AiroPeek, the **Start Page** appears. This is an HTML page with links to useful resources, both local and online. From the **Start Page**, you can open recently used Packet files, start a new Capture window, browse sample Packet files or other Packet files, view the Readme file or manual, take the Quick Tour, and more.



Get Started

Recent Files	Location	Summary
No recent files		

Recent Capture Templates	Location	Summary
No recent files		

What's New

- View the Readme...
- Take the Quick Tour...
- View sample files...
- Get the latest news from WildPackets...

Online Resources

- Refer to the technical compendium...
- Network analysis tips, white papers, and more...

Technical Support

- Get technical support for WildPackets products...
- Contact WildPackets technical support...

Training

- Find out about training with the WildPackets Academy...
- Find out about WildPackets consulting...

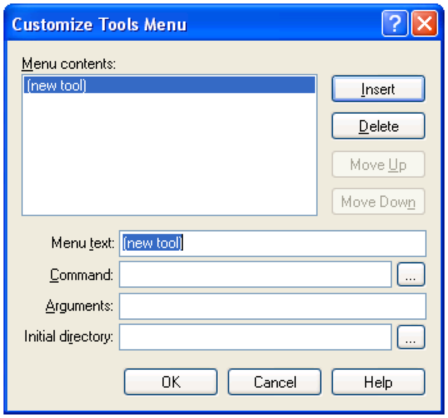
☑ Show Start Page at startup

Figure 3.2 Start page

Check the checkbox at the bottom of the **Start Page** to *Show Start Page at start-up*. Alternatively, you can always view the **Start Page** by choosing **Show Start Page** from the **Help** menu.

Customizing the tools menu

You can add programs to the **Tools** menu, allowing you to launch them from within AiroPeek. Choose **Customize…** from the **Tools** menu to open the **Customize Tools Menu** dialog. This dialog lets you manage add-in items that appear in the **Tools** menu.



Menu contents: [new tool]

Menu text: [new tool]

Command:

Arguments:

Initial directory:

Figure 3.3 Customize Tools Menu dialog

To add a program to the **Tools** menu, click the **Insert** button. This creates a blank item called *[new tool]*, highlighted in the *Menu contents* list. Use the text entry boxes to set the parameters for this new item. The *Menu text* field sets the name of the tool as it will appear in the **Tools** menu. In the *Command* field, type the path to the program, or use the **…** (ellipsis) button to navigate to its location. Optionally, you can enter any *Arguments* for the program, and set its initial directory by typing the path or using the **…** (ellipsis) button to navigate to its location.

To remove an item, highlight its name in the *Menu contents* list and click the **Delete** button. Items appear at the end of the **Tools** menu in the same order in which they appear in the *Menu contents* list. To change the order, highlight an item and use the **Move Up** and **Move Down** buttons. When you have made your changes, click **OK** to accept your changes and close the dialog, or click **Cancel** to close the dialog and discard your changes.

An example of tools that can be added to the menu is the iNetTools suite of applications. Each individual part of the iNetTools suite can be added to the **Tools** menu as a separate menu choice. If you accept the option to add iNetTools to the **Tools** menu during installation, for example, all the parts of the suite will be added.

iNetTools

WildPackets' iNetTools is a collection of easy-to-use GUI-based tools for testing Internet and IP-based networks. The iNetTools suite is included on the AiroPeek distribution CD, and is also available from the WildPackets website at http://www.wildpackets.com. The current tools are shown in Table 3.1 below.

Table 3.1 iNetTools components

iNetTool	Description
Ping	uses the ICMP protocol to send echo request packets to a device and times the responses.
Ping Scan	pings a range of IP addresses to find out which addresses are currently in use.
Trace Route	traces the route packets take from your computer to any device with an IP address.
Name Lookup	resolves names to IP addresses and IP addresses to names.
Name Scan	performs a Name Lookup for a range of IP addresses.
DNS Lookup	provides detailed information on Internet hosts by querying Domain Name Servers.
Port Scan	scans ports on a machine to find supported services, such as HTTP, telnet, and FTP.
Service Scan	scans a range of IP addresses for services, such as FTP, HTTP, and telnet.
Finger	uses the finger protocol to get information about a user on a given server.

Table 3.1 iNetTools components (continued)

iNetTool	Description
Whois	uses the WHOIS protocol to query database servers such as whois.internic.net for Internet directory information.
Throughput	connects to an FTP or an HTTP (Web) server to test download speed of FTP or Web files.

In addition to the above tools, iNetTools features the following reports and references:

Network/IP Configuration Information… uses ‘IPCONFIG’ under Windows 2000 or Windows XP.

Network Statistics… uses the NETSTAT command to display routing information and other network traffic details.

ARP Cache Content… uses the ARP command to list a system-cached record of associations between IP addresses and physical addresses.

Internet Port Description… lists Internet port numbers and descriptions, downloaded from the IANA (Internet Assigned Numbers Authority) site.

Important! Active name resolution and notifications using the email action require an active network connection. Because AiroPeek puts the NIC into a “listen only” mode when the network adapter is selected, network access while AiroPeek is running requires that a second network adapter must be installed for use by network services. Alternatively, selecting either *None* or *File* as the adapter can free the NIC for network services, if the card supports this functionality. Please see our website at http://www.wildpackets.com/support for details about specific cards.

Packet Capture

AiroPeek can capture packets in multiple configurable Capture windows, each with its own selected adapter, its own dedicated capture buffer and its own settings for filters, triggers, and statistics output. Capture windows let you monitor, collect statistics, and capture from multiple adapters simultaneously. You can establish and view multiple Capture windows up to the limits of available memory and screen space.

Capture windows allow you to:

- view and monitor network traffic in real time
- use a different adapter for each Capture window
- use expert analysis to monitor and troubleshoot
- apply filters, both before and after capture
- start and/or stop capture based on network events
- separate potential problems from severe ones
- view statistics based on selected network traffic
- view packet contents, raw and/or decoded
- save packets for post-capture analysis in Packet File windows
- create snapshots of particular network conditions for future comparison

The default setting for a new Capture window is to capture all packets. Once you are more familiar with AiroPeek, you can restrict packet capture using filters (see Chapter 11, “Filters” on page 207), and triggers (see Chapter 12, “Triggers, Alarms and Notifications” on page 235).

This chapter explains how to set up a Capture window and configure its use of adapters and memory, how to customize its appearance, how to save packets and reload them in a Packet File window, and how to print out captured packets.

In this Chapter:

Capture window basics

This section presents the basic form and function of the Capture window. To capture packets in AiroPeek, you create a Capture window, set or accept its parameters, and click the **Start Capture** button. It's as simple as that. Because Capture windows can be configured to meet a variety of user needs, there are multiple ways to perform each of these functions. These are covered in detail in the sections below. The Capture window basics section ends with an overview of Capture window layout and structure.

Creating a new capture window

You can create a new Capture window in any of several ways. You can click the **New Capture** button on the **Start Page**. You can select **New…** from the **File** menu or type **Ctrl + N**. Alternatively, if you have created one or more capture templates, you can choose **New From Template** from the **File** menu to select a recently used capture template from the submenu list, or use the **Choose…** submenu item to navigate to a capture template (*.ctf) and open it as a new Capture window using a standard file **Open** dialog. Finally, if no Capture window is open, selecting **Start Capture** from the **Capture** menu or typing **Ctrl + Y** will also open a new Capture window.

The first time you open a Capture window, you will see the **Capture Options** dialog. The **Capture Options** dialog defines all the parameters for a Capture window. At a minimum, the definition of a Capture window requires a selected adapter, a memory allocation called a capture buffer, and a set of parameters defining how to use the buffer. All of these parameters must be set for each Capture window when it is created. You can set them by hand, accept the defaults, or use the settings stored in a capture template. Please see "Capture options: general" on page 56, for details about the **Capture Options** dialog and how to use it. Choose new values for the parameters or accept the defaults and click **OK** to create a new Capture window.

Using default settings and capture templates

If you do not want to be presented with the **Capture Options** dialog each time you open a new Capture window, you have two choices.

The first method is to set the parameters in the **Capture Options** dialog to the values you wish to use for all subsequent Capture windows and uncheck the checkbox beside *Show this dialog when creating a new capture window.* Each time you create a new Capture window, it will open immediately using these parameters. New windows will be named *Capture 1*, *Capture 2*, and so forth in sequence as each new window is created during a session of AiroPeek. To return to having the **Capture Options** dialog presented each time you open a new Capture window, make a Capture window the active (frontmost) window, choose **Capture Options…** from the **Capture** menu to open the **Capture Options** dialog, and re-enable that option by checking the checkbox.

The second method is to create one or more capture templates and use them to create new Capture windows. Templates supply the **Capture Options** dialog settings for windows created from them. You can save any Capture window as a named capture template by making that Capture window the active window and choosing **Save Capture Template…** from the **File** menu. This opens a **Save As** dialog where you can choose the location in which to save the template and give the template a name. Save the template as a *Capture Template* format (*.ctf) file. A capture template contains all of the settings in the **Capture Options** dialog, and applies these to any Capture window created using the **New From Template…** command under the **File** menu. When you create a new Capture window from a template, the new window uses the Capture window title specified in the template, adding the numbers *1*, *2*, *3*… only when necessary to distinguish between multiple instances open at the same time. Capture windows created from templates are created without opening the **Capture Options** dialog, regardless of whether the checkbox labeled *Show this dialog when creating a new capture window* is checked or unchecked.

Capture templates are also used when invoking AiroPeek from the command line. Please see “Starting AiroPeek from the command line” on page 31. The AutoCapture feature also allows you to create, import, and export settings from capture templates, and use them to programmatically invoke capture by AiroPeek, EtherPeek, TokenPeek, or Packet Grabber. Please see “AutoCapture” on page 91.

Important! The definition of a Capture window must include the selection of a valid adapter. If the adapter named in your default settings or capture template is not found, AiroPeek will present an error message. Click **OK** to clear this error message and bring up the ***Adapter*** view of the **Capture Options** dialog, from which you can select a valid adapter for the new Capture window.

Starting and stopping capture in a capture window

To start capturing packets, click the **Start Capture** button in the upper right of the Capture window (see Figure 4.1). The label on the button will change to **Stop Capture** when capture is under way. Alternatively you can use the **Start Capture** command from the **Capture** menu or press **Ctrl + Y** to start capture in whichever Capture window is the active (frontmost) window at the time. Both the **Ctrl + Y** sequence and the choices under the **Capture** menu act as toggles, starting or stopping capture depending on the state of the active Capture window.

Tip You can also start and/or stop capture based on a time event or a filter match, by setting a trigger for the new Capture window. For more on triggers, please see "Triggers" on page 236.

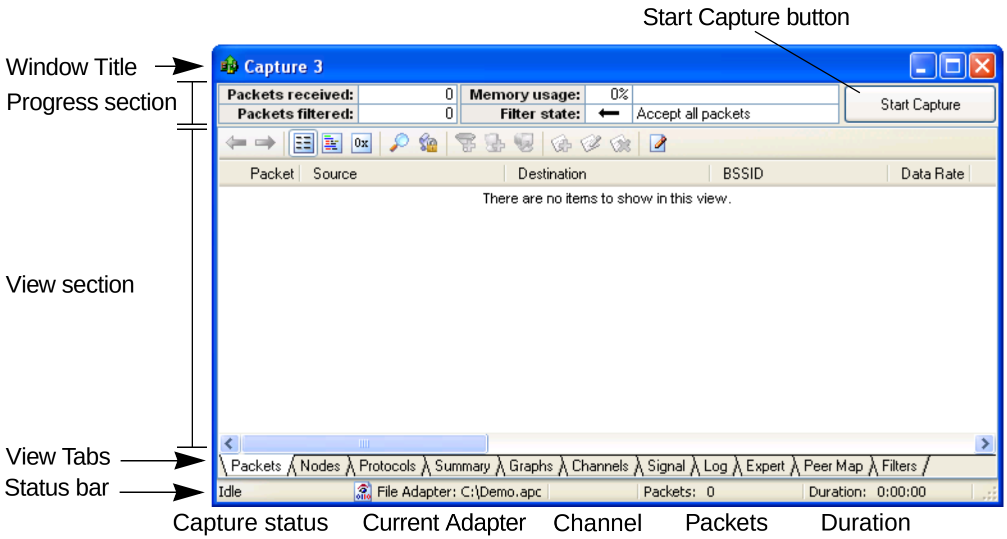
A progress bar labeled *Memory usage* tracks the percentage of that particular Capture window's capture buffer that has been filled. You will notice that the *Memory usage* bar resets to zero when the buffer becomes full and is dumped to begin refilling. This can happen when the buffer wraps automatically under continuous capture, or when you clear the buffer manually, either by using the **Clear All Packets** command from the **Edit** menu, typing **Ctrl + B**, or by restarting capture in that window without saving already captured packets. The other indicators in the progress section (*Packets received* and *Packets filtered*) will continue to increment without interruption, even when the buffer wraps.

When you stop capture, all of the packets currently in the buffer for that Capture window are retained, and any statistics shown in any of the other views will be based on all the packets seen since capture was initiated for that Capture window. If you then restart capture for that Capture window, AiroPeek will clear the window's buffer *and its statistics* and begin again from zero. The only way to restart capture in a Capture window without clearing the buffer (thus retaining any packets and any statistics collected so far) is to use **Shift + Click**. Hold down the **Shift** key while you click the **Start Capture** button to restart capture without clearing the existing contents of the buffer.

Because all packets and statistics will be lost when you close a Capture window without saving, AiroPeek warns you each time you close a Capture window. To change this and other default display behaviors, use the **Options** dialog, available by choosing **Options…** under the **Tools** menu.

Capture window structure

Each Capture window has a progress section at the top showing basic statistics for the window as a whole, and a lower section showing one of several different views selected by clicking the appropriate view tab.



Packets received: 0
Packets filtered: 0
Memory usage: 0%
Filter state: Accept all packets

There are no items to show in this view.

Idle | File Adapter: C:\Demo.apc | Packets: 0 | Duration: 0:00:00

Figure 4.1 Parts of a Capture window

The parts of the Capture window common to every view are labeled in Figure 4.1 and described in Table 4.1. For a description of the individual views available in a Capture window please see “Capture window views” on page 66.

Table 4.1 **Parts of a Capture window (see Figure 4.1)**

Window part	Description
Capture window title	The user-defined (or default) title of the Capture window.
Start Capture	Click the **Start Capture** button to begin capturing packets. When capture is under way, the label on the button changes to **Stop Capture**. When a trigger is set for the Capture window, this button can be labeled in different ways. Please see “Triggers” on page 236 for details.
Progress section	The progress section shows the following four parameters of capture activity:

Table 4.1 **Parts of a Capture window (see Figure 4.1) (continued)**

Window part	Description
Packets received	Shows total packets presented to the filters since capture was initiated for this window—essentially, the total number of packets on the network since capture was initiated for this Capture window.
Packets filtered	Shows, of those received, the total number of packets matching the filter or filters set for this window. If there are no filters, then *Packets Received* and *Packets Filtered* will be equal. One exception might be any packets dropped when the buffer is wrapping.
Memory usage	Shows the percentage of configured capture buffer memory used so far in packet capture for the current Capture window. This percentage is displayed as a number and graphically by a progress bar which fills more of the width of the display as memory is used. Also, as memory use approaches 100%, the color of the bar changes from blue to warmer colors, eventually showing red when 100% of the capture buffer is used.
Filter state	Summarizes any enabled filter conditions. For example, *Accept only packets matching any of two filters*. An icon indicates whether filters are set to accept or reject matching packets. Double-click in this area to open the ***Filters*** view of the **Capture Options** dialog.
View section	Shows the current view of the Capture window, which can be selected by using the view tabs located just below the view section near the bottom of the window.
View Tabs	Shows the current and the available views. The tab for the current view is shown in white. The others are shown in gray. Click on a tab to see a particular view of the Capture window displayed in the view section.
Status bar	At the bottom of the window, these four items show the status of capture activity.
Capture status	Shows the current state of the capture process for the Capture window. For example, *Idle* or *Capturing*.

Table 4.1 **Parts of a Capture window (see Figure 4.1) (continued)**

Window part	Description
Current Adapter	Shows the currently selected adapter. Double-click on this item to open the ***Adapter*** view of the **Capture Options** dialog, where you can select another adapter, set the network speed, and so forth.
Channel	Shows the current channel, BSSID, or ESSID being scanned by the adapter. Double-click to open the ***802.11*** view of the **Capture Options** dialog for this window, where you can set channel scanning parameters for the current adapter globally.
Packets	Shows the number of packets in the buffer. When some packets have been hidden, shows, for example, *2 (of 48)*.
Duration	Shows the difference between the earliest and the most recent packet in the current window.

Capture options dialog

The **Capture Options** dialog defines all the parameters for a Capture window. The parameters are displayed in six views, accessible by clicking their named tabs: ***General***, ***Adapter***, ***802.11***, ***Triggers***, ***Filters***, and ***Statistics Output***. Each of these views and all their parameters are described below.

Note: At a minimum, you must set the capture buffer options (in the ***General*** view) and select a valid adapter (in the ***Adapter*** view) to define a Capture window. The other capabilities are optional.

Very briefly the functions of the views of the **Capture Options** dialog are as follows:

General Set the size and method of use of the capture buffer for this Capture window. Also controls packet slicing (saving only the first *n* bytes of each packet). (Please see “Capture options: general” on page 56.)

Adapter Choose the adapter from which this particular Capture window will capture packets. Choose any supported adapter: file or local 802.11 WLAN card. (Please see “Capture options: adapter” on page 62.)

802.11 Control channel selection and scanning for this adapter and define WEP decryption for packets captured on it. (Please see “802.11 view” on page 21.)

Triggers Define time, network, or capture events to trigger the start and/or stop of capture in this Capture window. (Please see “Triggers” on page 236.)

Filters Select filters and define how they will be used to limit the packets captured into this Capture window. (Please see “Capture options: filters” on page 65.)

Statistics Output Choose from a variety of formats and statistics for periodic output from this Capture window, at a frequency you set. (Please see “Statistics output views” on page 188.)

Each Capture window is defined by its own **Capture Options** settings. You can have multiple Capture windows open simultaneously, capturing and displaying in real time. You can quickly create a new Capture window using either your own or the factory default settings. You can also save **Capture Options** settings as a capture template and use these templates to create a fully configured Capture window—complete with triggers, filters, and statistics output options—in a matter of a few clicks or keystrokes. You can import settings from these templates into an AutoCapture file and invoke capture in remote instances of AiroPeek and have the resulting packet files emailed or FTP’ed to you as soon as capture is complete.

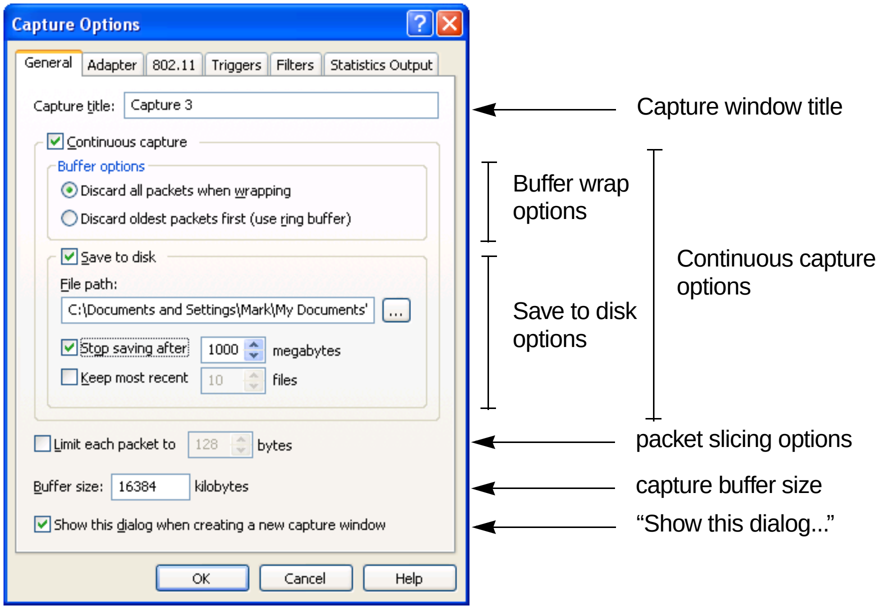
Capture options: general

This section describes how to use the ***General*** view of the **Capture Options** dialog to set the capture buffer size and other important packet capture parameters for Capture windows.

Each Capture window has its own assigned memory allocation called a capture buffer, and a set of parameters telling the Capture window how to use that memory. In addition, a Capture window can be set to use a space-saving technique called packet slicing, in which it captures only a specified number of bytes from the beginning of each packet and ignores the rest. These parameters must be set for each Capture window when it is created, either directly by the user in the **Capture Options** dialog, or by configuring AiroPeek to always use default Capture Options settings, or by using the Capture Options settings contained in a capture template. In addition, you can change the Capture Options settings for any Capture window by making it the active window and choosing **Capture Options…** from the **Capture** menu to bring up the **Capture Options** dialog and editing the values displayed there.

If the checkbox beside the *Show this dialog when creating a new capture window* item in the ***General*** view of the **Capture Options** dialog is checked, as it is by default, the **Capture Options** dialog will display each time you create a new Capture window using the **New…** command under the **File** menu or typing **Ctrl + N**. If no Capture windows are open, selecting **Start Capture** from the **Capture** menu or typing **Ctrl + Y** will do the same thing. This brings up the **Capture Options** dialog, shown in Figure 4.2.

In the ***General*** view of the **Capture Options** dialog, you can choose whether the Capture window will continuously capture packets (either discarding or saving previously captured packets each time the buffer becomes full), or simply stop capturing packets when all of its buffer memory has been used. The default setting is to stop capture when the buffer is full.



Capture title: Capture 3

☑ Continuous capture

Buffer options

● Discard all packets when wrapping

○ Discard oldest packets first (use ring buffer)

☑ Save to disk

File path: C:\Documents and Settings\Mark\My Documents'

☑ Stop saving after 1000 megabytes

□ Keep most recent 10 files

□ Limit each packet to 128 bytes

Buffer size: 16384 kilobytes

☑ Show this dialog when creating a new capture window

Figure 4.2 General view of the Capture Options dialog

Your options are:

- **Capture until buffer is full:** This is the initial default setting. When the buffer is full, capture stops. When the *Continuous capture* check box is unchecked, capture will stop when the buffer becomes full.
- **Continuous Capture**: Periodically discards packets from the buffer to make room for new capture. When you check *Continuous capture*, capture does not stop until it is stopped manually by the user or by a stop trigger.
- **Continuous Capture, Save to Disk**: Periodically saves captured packets before emptying the buffer. You can limit the total disk space allocated for the saved files. When you check *Continuous capture*, and *Save to disk*, capture does not stop until it is stopped manually by the user or by a stop trigger.

Each of these options is explained in detail below.

You can change the settings in the **Capture Options** dialog for an existing Capture window by choosing the **Capture Options…** item under the **Capture** menu.

Capture until the buffer is full

If you accept all the program’s initial default settings, the new Capture window will stop capture when its buffer is full.

To create a new Capture window that will stop capture when its buffer becomes full:

1. Accept the default name for the new Capture window, or enter a new name in *Capture title*.
2. Make sure *Continuous capture* is disabled (unchecked), as it is by default.
3. Optionally, you can limit the amount of each captured packet to be saved. Please see “Using packet slicing” on page 61 for more details about this space-saving technique.
4. Accept the default *Buffer size: 16384 kilobytes*, or enter a new value for the buffer size.
5. When you have set all of the parameters, click **OK** to create the new Capture window.

Note: To avoid arbitrarily slicing the last packet captured, when you specify a buffer size in bytes, AiroPeek captures the whole packet that caused the specified *Buffer size* to be reached.

Continuous capture

When you check the checkbox beside *Continuous capture*, AiroPeek captures packets until capture is stopped manually by the user, or by a stop trigger. When the window’s capture buffer is full, AiroPeek discards packets to make room for new ones. Continuous capture is useful when, for example, you are waiting for a stop trigger event or notification.

Important! Continuous capture, with or without the save options, means that the Capture window continues to capture until it is stopped manually by the user or until a user-defined stop trigger is tripped.

To create a new Capture window that will continuously capture, re-using the buffer space:

1. Accept the default name for the new Capture window, or enter a new name in *Capture title*.
2. Enable *Continuous capture* by checking that checkbox.
3. Use the radio buttons in the *Buffer options* section to *Discard all packets when wrapping*, or *Discard oldest packets first (use ring buffer)*. The first option fills the buffer completely, then dumps the whole contents. The second option, in effect, writes over the older entries with newer ones.

Note: When you select the ring buffer option, once the *Memory usage* item in the Capture window header section reaches *100%*, it will stay there. In the ring buffer, new packets are continuously replacing ones captured earlier. The ring buffer, once full, remains full throughout the capture process.

4. Optionally, you can limit the amount of each captured packet to be saved. Please see “Using packet slicing” on page 61 for more details about this space-saving technique.
5. Accept the default *Buffer size: 16384 kilobytes*, or enter a new value for the buffer size.
6. When you have set all of the parameters, click **OK** to create the new Capture window.

Tip The processing time needed for continuous capture may cause AiroPeek to miss or drop some packets when its memory becomes full. This loss can be minimized by not scrolling during capture, by closing any non-essential windows, and by exiting any other programs that may be running in the background, even if they are idle.

Important! When you choose *Continuous Capture*, statistics for the Capture window will reflect all of the packets seen since it last began capturing. If you did not also choose *Save to disk*, the packets themselves may no longer be available after the buffer has wrapped (that is, dumped its packets and begun to refill).

Continuous capture saving to disk

When you choose *Continuous capture*, *Save to disk*, capture continues until it is stopped manually or by a stop trigger. Saving can continue until either a set amount of space is filled or until all available disk space at the save location is used up, or it can continue endlessly, overwriting older files with newer ones.

While saving continues, the program saves to a new file each time the buffer wraps. Each file uses the *File name* you specify, with the string “-hh.mm.ss” appended, where “hh” is the hour, “mm” the minute and “ss” the second at which the file was saved. If saving is still under way, any packets not yet saved will be saved when you stop capture.

To create a new Capture window that will continuously capture, saving all packets to disk:

1. Accept the default name for the new Capture window, or enter a new name in *Capture title*.
2. Enable *Continuous capture* by checking that checkbox.
3. Use the radio buttons in the *Buffer options* section to *Discard all packets when wrapping*, or *Discard oldest packets first (use ring buffer)*. The first option fills the buffer completely, then dumps the whole contents. The second, in effect, writes over the older entries with newer ones.
4. Check the checkbox beside *Save to disk*.
5. Use the *File path* text entry box to specify the base file name, the directory in which to store the file(s), and the file format to use in saving the buffer’s contents. You can enter the text directly, determining the file format by entering the correct file extension, or you can click the **...** (ellipsis) button to open a **Save As** dialog in which you can specify all these parameters. Your save file format choices are: *AiroPeek Packet File (*.apc*), *AiroPeek Packet File (compressed) (*.wpz)*, *Text (Tab delimited) (*.txt)*, or *CSV (Comma delimited) (*.csv)*.

Important! If you do not use one of the following options to limit the space allocated to saved files, captured traffic can continue to be saved until all available disk space at the specified *File path* is used up.

6. To limit the amount of space which can be taken up by the captured files, you have two choices: set the total disk space, or set the number of files. When you limit the total disk space, capture will continue, but no further files will be saved after this space is filled. When you limit the number of files, capture will continue, and older saved files from this Capture window will be overwritten with newer ones.

7. To set the total disk space to be occupied by the captured files, check the checkbox beside *Stop saving after... megabytes* and use the data entry box to specify the maximum amount of disk space you wish to use for the saved files.

8. Alternatively, you can limit the disk space used for captured files by setting an upper limit on the number of files to be kept. Check the checkbox beside *Keep most recent … files* and use the data entry box to specify the number of files. The Capture window writes a new file each time the buffer become full. Each file will be roughly the size you specify in *Buffer size*, below. When you limit the number of files, the oldest file is replaced by the newest. The total space taken up by saved files will be approximately equal to the buffer size times the number of files to keep.

9. Optionally, you can limit the amount of each captured packet to be saved. Please see “Using packet slicing” on page 61 for more details about this space-saving technique.

10. Accept the default *Buffer size: 16384 kilobytes*, or enter a new value for the buffer size.

11. When you have set all of the parameters, click **OK** to create the new Capture window.

Using packet slicing

Use packet slicing to capture only a portion of each packet instead of the whole packet. This saves space in the capture buffer. The packet slicing option is found in the ***General*** view of the **Capture Options** dialog. If you have not changed the default program settings, the **Capture Options** dialog is opened each time you create a new Capture window. To enable packet slicing for an existing Capture window, make it the active window and choose **Capture Options…** under the **Capture** menu to open the **Capture Options** dialog, and click the *General* tab to open the ***General*** view (shown in Figure 4.2).

To enable packet slicing, click the checkbox labeled *Limit Each Packet to…. Bytes* and enter a number of bytes in the edit field. For example, if you enter “*132*,” AiroPeek saves only the first 132 bytes of each packet it captures.

Note: You cannot enter a slice value of less than 14 bytes. In choosing a slice value, you should consider any filters and Name Table entries that you want to apply to your captured packets. Logical addresses and protocol fields both occur after the first 14 bytes. We recommend keeping the slice value at 128 bytes or greater. This typically will include all of the packet headers but little or no packet data.

Because 802.11 WLAN packets have a variable header length, a given slice value will not always capture identical information from every packet. Table 4.2 shows the slice value to use to insure that you capture the specified packet component, regardless of the 802.11 WLAN header length. For more on the structure of 802.11 WLAN packets, please see Appendix A, “Packets and Protocols” on page A-3.

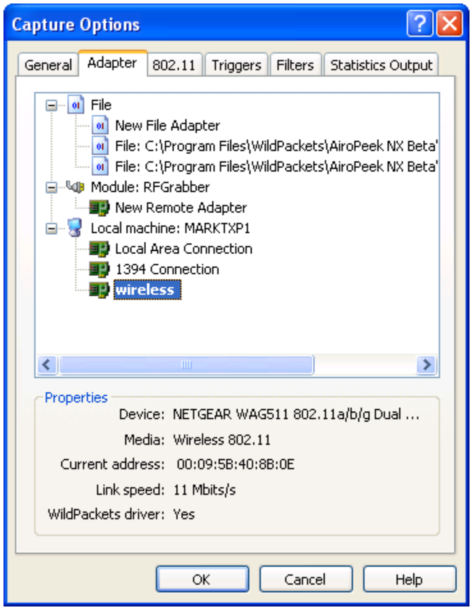
Table 4.2 **Recommended slice values for 802.11 WLAN packets**

Packet component	Must occur within
Full 802.11 MAC header	first 30 bytes
802.11 MAC header and protocol (in 802.2 header)	first 38 bytes
802.11 MAC header, 802.2 header and IP header	first 58 bytes

Capture filters are applied to packets before slicing occurs, so the slice value does not affect trigger events or filters enabled for a Capture window. However, any functions dependent on reading data from packets *after* they have been placed in the buffer *will* be affected. When used in the **Select** dialog, for example, Analysis Modules, filters, and other advanced functions read packets from the buffer, rather than directly from the network.

Capture options: adapter

Each Capture window must be assigned an adapter from which to capture network traffic. Multiple Capture windows can be assigned the same adapter, or each a different adapter, or any combination of shared or unique, so long as each Capture window has one valid adapter selected. You select an adapter in the ***Adapter*** view of the **Capture Options** dialog. The ***Adapter*** view of the **Capture Options** dialog (Figure 4.3) displays the names of all detected network interface cards (NICs) installed in your machine. In addition, the ***Adapter*** view of the **Capture Options** dialog permits you to choose a *File* as the adapter. Select a listed adapter or one of the alternate choices, then click **OK**.



```
⊟ File
    New File Adapter
    File: C:\Program Files\WildPackets\AiroPeek NX Beta'
    File: C:\Program Files\WildPackets\AiroPeek NX Beta'
⊟ Module: RFGrabber
    New Remote Adapter
⊟ Local machine: MARKTXP1
    Local Area Connection
    1394 Connection
    wireless
```

Properties

Device:	NETGEAR WAG511 802.11a/b/g Dual ...
Media:	Wireless 802.11
Current address:	00:09:5B:40:8B:0E
Link speed:	11 Mbits/s
WildPackets driver:	Yes

Figure 4.3 Adapter view of the Capture Options dialog

To choose a file as the adapter, expand the *File* item and select a previously used file or choose *New File Adapter*. Double-click on the item, or highlight it and click the **OK** button to make your choice. If you select *New File Adapter*, you will be asked to specify the file, using a standard file **Open** dialog. When you choose an AiroPeek packet file (one of those in the Samples directory, for example), the program cycles through the traffic captured in that file, treating it as live traffic for purposes of this particular Capture window. By choosing a file as the adapter, you can simulate network conditions for training or open other packet traces without being connected to an 802.11 WLAN network, or indeed without even having a supported NIC installed on your computer.

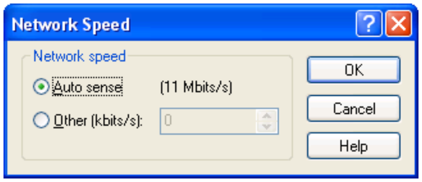
Note: If you have the separately purchased RFGrabber Analysis Module installed, you will also see a heading for that Module and, under it, choices for a *New Remote Adapter*, or previously used remote adapters. For details about RFGrabber, see Chapter 14, “RFGrabber Probe” on page 283.

In addition to showing the currently selected adapter and its *Media* type, the ***Adapter*** view of the **Capture Options** dialog shows the *Current address*, *Link speed*, and whether or not the *WildPackets driver* is installed for this adapter.

Tip You can return to the ***Adapter*** view of the **Capture Options** dialog by double-clicking on the current adapter, shown in the status bar at the bottom right of the Capture window. Alternatively, make the Capture window the active window, and choose **Capture Options...** from the **Capture** menu to open the **Capture Options** dialog for that Capture window, then click the *Adapter* tab to open the ***Adapter*** view.

Network speed

AiroPeek auto-senses the network speed of the network adapter you select for its use, by default. You may want to expressly set the network speed in certain cases. Some statistics are derived from calculations based in part on the network speed. You may wish to set a nominal network speed for a particular adapter within AiroPeek to insure consistent statistics reporting.



Network speed

● Auto sense (11 Mbits/s)

○ Other (kbits/s): 0

Figure 4.4 Network Speed dialog

To expressly set the network speed AiroPeek should use in performing calculations based on a particular adapter, open the ***Adapter*** view in either the **Monitor Options** or the **Capture Options** dialog. Right click on the adapter whose speed you wish to set, and choose **Network Speed…** from the context menu to open the **Network Speed** dialog (Figure 4.4) for that adapter. Click the radio button beside *Other (kbits/s)* and enter the speed in kilobits per second. Click **OK** to close the **Network Speed** dialog, and click **OK** again to close the parent dialog, accepting your changes.

Important! The same network speed is assigned for all uses of a particular adapter, whether it is selected for use by Monitor statistics, Capture window(s), or both. When you change the *Network speed*, it takes effect immediately for all uses of that adapter.

Default local adapter

The default choice in the ***Adapter*** view of the **Capture Options** dialog is the most recently selected adapter of any kind selected in the **Capture Options** dialog. (Creating a Capture window from a capture template does not affect the state of the **Capture Options** dialog, because the capture template bypasses the dialog, using its own stored options to create the new Capture window.) If there is no “most recently selected adapter” (you have never selected one, or the previously selected adapter is not found), the default adapter choice is the local NIC designated by AiroPeek as the “*default local adapter*.”

If you have only one supported 802.11 WLAN NIC installed on the local machine, then that NIC is the default local adapter. If you have more than one NIC installed, then the default local adapter is the first supported NIC in the list of those shown under *Local machine* in the ***Adapter*** view.

Capture options: 802.11

The ***802.11*** view of the **Capture Options** dialog lets you control channel selection or scanning and WEP (Wired Equivalent Privacy) decryption for the selected adapter.

Important! The ***802.11*** view is identical in either the **Monitor Options** or the **Capture Options** dialog. Changes made in the ***802.11*** view of either dialog take effect immediately for all uses of a particular adapter, whether it is selected for use by Monitor statistics, Capture window(s), or both.

For a detailed description of the ***802.11*** view and how to use it, please see “802.11 view” on page 21.

Capture options: triggers

The ***Triggers*** view of the **Capture Options** dialog lets you control the start and or stop of capture in a particular Capture window by watching for a user-specified time, network, or capture event. For a complete discussion of trigger functions and the ***Triggers*** view of the **Capture Options** dialog, please see “Triggers” on page 236.

Capture options: filters

The ***Filters*** view of the **Capture Options** dialog shows a list of all available filters and allows you to choose which filters to enable for the current Capture window by checking the checkbox next to that filter’s name. To choose how the filter(s) will be applied, use the **Accept Matching** or **Reject Matching** buttons at the top left of the ***Filters*** view. When you choose **Accept Matching**, only those packets which match the parameters of at least one of the enabled filters will be placed in the buffer. When you choose **Reject Matching**, only those packets which do not match any of the enabled filters will be entered in the buffer.

You can also set filters for a Capture window by using the ***Filters*** view of the Capture window itself.

Tip Use the ***Filters*** view of the **Capture Options** dialog to set the initial filter state for a new Capture window, or to build a capture template that includes filtering. Use the ***Filters*** view of the Capture window itself to make on-the-fly changes to filter settings. It's one click away, and the changes made there take effect immediately.

Double-click on any filter in any filter list in the program to open it in an **Edit Filter** dialog and change or simply verify its parameters. For more about filters and how to use them, see Chapter 11, "Filters" on page 207.

To apply filters to packets already captured to a buffer, either in a Capture window or a Packet File window, use the **Select…** command from the **Edit** menu. For more on how to use filters to select captured packets, see "Select dialog: filters, analysis modules and more" on page 313.

Capture options: statistics output

Use the ***Statistics Output*** view of the **Capture Options** dialog to control the periodic output of statistics while the Capture window is open. Choose from several groups of statistics in a variety of report and file output formats. Save the files to any location at an interval you specify. A similar dialog view with similar choices is used to control the periodic output of Monitor statistics, and a complete description of both views is provided in the "Statistics" chapter. Please see "Statistics output views" on page 188 for details.

Capture window views

The first time you launch AiroPeek, a new Capture window presents the ***Packets*** view in the view section by default. On subsequent start-ups, a new Capture window presents the view last seen in any Capture window. To move between views, click on the view tabs at the bottom of the Capture window.

When you click on a tab, it displays a different way of looking at the packets captured in this Capture window. The tab bar itself is not configurable and is the same for every Capture window. The appearance of individual views can be customized to a greater or lesser extent.

The views available in any Capture window, in order from left to right as they appear in the view tabs, are shown in Table 4.3.

Table 4.3 **Views available in Capture windows**

View	Description
Packets	This view shows a detailed list of all packets in the capture buffer, in the order they were received. This is the default view. You can choose which columns (what information) to display, as well as customize appearance. Packet Decodes are available.
Nodes	This view shows traffic aggregated by network node (physical address, logical address, and/or symbolic name). In the ***Hierarchical*** view, you can choose to show packets received, packets sent, or both. All views can limit display to highest traffic nodes. Customized appearance is available. Detailed views are available.
Protocols	This view shows traffic aggregated by protocol and sub-protocol using ProtoSpecs technology. It has a customizable appearance, and detailed views are available.
Summary	This view shows a synopsis of the activity on the network since capture began: number of nodes, traffic volumes by type, and other summary statistics supplied by AiroPeek and Analysis Modules.
Graphs	This view presents a variety of graphs displaying statistics from the current window in real time. All graphs, including the default set, are editable and configurable. (Default graphs include equivalents to the **Size** and **History** graphs found in Monitor statistics, for example.) You can add to, delete, rearrange, create, edit, export, and import graphs of nearly any form, each based on single or multiple statistics from the current Capture window.
Channels	This view shows traffic volumes, signal strength and more for every channel on which traffic is detected. The table has a large selection of user selectable columns.

Table 4.3 Views available in Capture windows (continued)

View	Description
Signal	This view shows the most recent signal data for each channel for which data is being collected by the current window. Graphically displays data in reference to user-defined thresholds. Can show Signal strength (% or dBm), Noise (% or dBm), or Signal:Noise, depending on user set-up and adapter capabilities.
Log	This view logs events such as the start of capture and shows messages, primarily from any enabled Analysis Modules.
Conversations **(AiroPeek standard only)**	Unique to AiroPeek standard, this view shows statistics for traffic arranged by conversations between pairs of nodes, as well as data about the individual nodes in each conversation.
Expert **(AiroPeek NX only)**	Unique to AiroPeek NX, this view shows conversations, including detailed expert analysis of potential problems, as identified in the Expert ProblemFinder settings.
Peer Map **(AiroPeek NX only)**	Unique to AiroPeek NX, this view shows a customizable graphical view of communications patterns between partners, based on the traffic in the current window.
Filters	This view shows a list of all available filters, showing which are enabled for this window. Enable and disable filters for the window in this view.

The rest of this section will take each of these views in order and describe their default appearance, any detailed views available, and any customizations that can be made to their appearance.

Packets view

The ***Packets*** view has three panes: the Packet List, Decode, and Hex view panes. You can display one, two, or all three of these panes in the ***Packets*** view at any time.

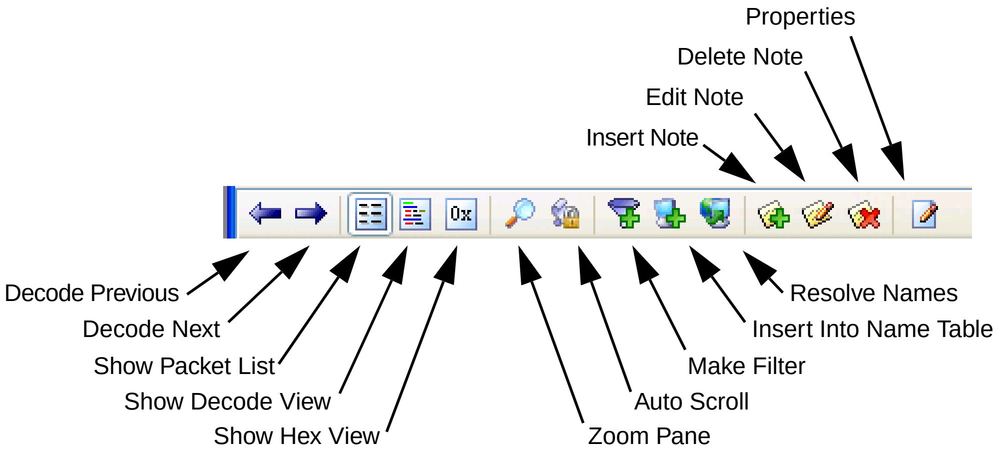
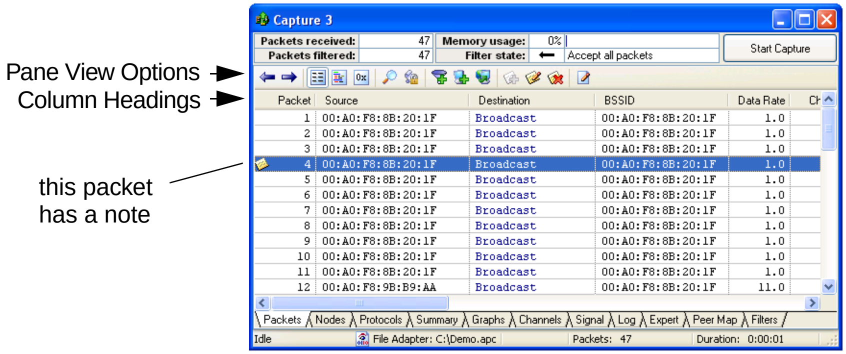


Figure 4.5 Detail of Pane View Options buttons in the Packets view

Use the Pane View Options buttons at the top of the ***Packets*** view (shown in detail in Figure 4.5) to select which panes will be visible. You can choose to **Show Packet List**, **Show Decode View**, and/or **Show Hex View** by toggling the appropriate button(s). The left and right arrow buttons step through the packets visible in the packet list backwards or forwards, respectively. You can use the function keys **F7** (previous) and **F8** (next), or use the keyboard combinations **Alt + left arrow** (previous) and **Alt + right arrow** to accomplish the same thing. When multiple panes are open, you can use the **Zoom Pane** button (or the **F4** function key) to toggle between viewing all panes (no zoom) or only the active pane (zoom). The active pane is the one in which you have highlighted some item.



Packets received: 47
Packets filtered: 47
Memory usage: 0%
Filter state: Accept all packets

Packet	Source	Destination	BSSID	Data Rate	Ch
1	00:A0:F8:8B:20:1F	Broadcast	00:A0:F8:8B:20:1F	1.0	
2	00:A0:F8:8B:20:1F	Broadcast	00:A0:F8:8B:20:1F	1.0	
3	00:A0:F8:8B:20:1F	Broadcast	00:A0:F8:8B:20:1F	1.0	
4	00:A0:F8:8B:20:1F	Broadcast	00:A0:F8:8B:20:1F	1.0	
5	00:A0:F8:8B:20:1F	Broadcast	00:A0:F8:8B:20:1F	1.0	
6	00:A0:F8:8B:20:1F	Broadcast	00:A0:F8:8B:20:1F	1.0	
7	00:A0:F8:8B:20:1F	Broadcast	00:A0:F8:8B:20:1F	1.0	
8	00:A0:F8:8B:20:1F	Broadcast	00:A0:F8:8B:20:1F	1.0	
9	00:A0:F8:8B:20:1F	Broadcast	00:A0:F8:8B:20:1F	1.0	
10	00:A0:F8:8B:20:1F	Broadcast	00:A0:F8:8B:20:1F	1.0	
11	00:A0:F8:8B:20:1F	Broadcast	00:A0:F8:8B:20:1F	1.0	
12	00:A0:F8:9B:B9:AA	Broadcast	00:A0:F8:8B:20:1F	11.0	

Idle | File Adapter: C:\Demo.apc | Packets: 47 | Duration: 0:00:01

Figure 4.6 Packet List in Packets view of a Capture window, with note

The Packet List pane is a table with user-configurable columns showing information about each packet on a single line. The next section, Packet list columns, describes each of the columns which can be used in the Packet List pane of the ***Packets*** view. For instructions on how to add or delete columns in a particular Packet List and how to change their order, please see “Customizing columns in the packet list” on page 82.

The Decode pane of the ***Packets*** view shows the information contained in a single packet, decoded and interpreted. The Hex view pane shows the information contained in a single packet as raw hexadecimal values on the left, and the same data expressed as ASCII characters on the right. The Decode and Hex panes of the ***Packets*** view are identical to the same views in the **Packet Decode** window. For a detailed description of the Decode and Hex view panes and how to use them, please see “The packet decode window” on page 318.

Tip AiroPeek produces live decodes of packets as they are captured, when either or both of the Decode and Hex panes are open and **Auto Scroll** is active. As each packet is captured, these panes are updated in real time with that packet’s information. The views are refreshed with the most recently captured packet, as long as **Auto Scroll** is enabled.

Packet list columns

Each column in the Packet List pane of the ***Packets*** view contains a particular type of information about the packet or a piece of information contained in the packet. Table 4.4 shows the columns available for use in the Packet List pane. Columns are included or excluded for a particular Capture window using the **Packet List Options** dialog. To open the **Packet List Options** dialog for a particular Packet List, click anywhere in the column headers of the list, or right-click in the display and choose **Packet List Options…** from the context menu.

The columns present by default when you use AiroPeek for the first time are shown in Table 4.4 with an **X** in the **Default** column. You can restore the default selection of columns at any time by clicking the **Defaults** button in the ***Columns*** view of the **Packet List Options** dialog.

Table 4.4 **Packet List Options columns, showing defaults**

Default	Column	Description
X	***Packet***	This column displays a packet number as determined by the time-sequential order in which the packets were captured.
X	***Source***	This column displays the source address. Depending upon the choice under **Display Format** in the **View** menu, this address may be a physical 802.11 WLAN address, a higher-level, logical address such as IP or AppleTalk, or a symbolic name.
	Source Logical	This column shows the logical address of the packet's source. Unlike the default ***Source*** column, this column's display is unaffected by any choice you make in **Display Format** under the **View** menu. This allows you to show different formats for a packet's source on a single line.
	Source Physical	This column shows the physical address of the packet's source. Unlike the default ***Source*** column, this column's display is unaffected by any choice you make in **Display Format** under the **View** menu. This allows you to show different formats for a packet's source on a single line.
	Source Port	This column displays the source port or socket, if any, in the notation appropriate for that protocol. For a definition of ports and sockets, please see "Ports and sockets" on page A-38.
X	***Destination***	This column displays the destination address. Like the source address, it may be shown as a numeric address or a Name Table entry.
	Destination Logical	This column shows the logical address of the packet's destination. Unlike the default ***Destination*** column, this column's display is unaffected by any choice you make in **Display Format** under the **View** menu. This allows you to show different formats for a packet's destination on a single line.

Table 4.4 **Packet List Options columns, showing defaults (continued)**

Default	Column	Description
	Destination Physical	This column shows the physical address of the packet's destination. Unlike the default ***Destination*** column, this column's display is unaffected by any choice you make in **Display Format** under the **View** menu. This allows you to show different formats for a packet's destination on a single line.
	Destination Port	This column displays the destination port or socket, if any, in the notation appropriate for that protocol. For a definition of ports and sockets, please see "Ports and sockets" on page A-38.
X	***BSSID***	This column displays the ID number of the access point or base station to whose traffic this packet belongs.This six byte hexadecimal number is typically formed from the station's MAC address.
	Transmitter	This column displays the physical address of the station identified in the packet header as the Transmitter, regardless of which address field may contain that information. A transmitter is typically the last hop on a relay through the DS (distribution system) and is distinguished from the original Source address.
	Receiver	This column displays the physical address of the station identified in the packet header as the Receiver, regardless of which address field may contain that information. A receiver is typically the first hop on a relay through the DS (distribution system) and is distinguished from the ultimate Destination address.
	Address 1	This column displays the physical address found in the first address field of the 802.11 WLAN MAC header, without reference to its type: destination, receiver, or BSSID.
	Address 2	This column displays the physical address found in the second address field of the 802.11 WLAN MAC header, without reference to its type: source, BSSID or transmitter.

Table 4.4 **Packet List Options columns, showing defaults (continued)**

Default	Column	Description
	Address 3	This column displays the physical address found in the third address field of the 802.11 WLAN MAC header, without reference to its type: source, destination, or BSSID.
	Address 4	This column displays the physical address found in the fourth address field of the 802.11 WLAN MAC header, without reference to its type. This address field is empty, except in packets relayed through the DS, in which it holds the source address.
X	***Flags***	This column contains flag characters indicating that a packet is of a certain type or condition. These are: management packets, control packets, CRC error, trigger packets, encrypted packets, and packets with decryption errors.The characters used for flags are assignable using the ***Flags*** view of the **Packet List Options** dialog, available by left-clicking in the column headers of the Packet List pane of the ***Packets*** view of any Capture window or Packet File window. The default assignments are shown in Table 4.5 below.
X	***Data Rate***	This column displays the data rate at which the body of this packet was transmitted.
X	***Channel***	This column displays the number of the channel on which the NIC was listening when the packet was captured.
X	***Signal***	This column displays the RSSI (Received Signal Strength Indicator) reported in the receipt of this packet, with RSSI normalized to a percentage value.
X	***Signal dBm***	This column displays the received signal strength reported in the receipt of this packet, in dBm (decibel milliWatts).
X	***Noise***	This column displays the noise detected on receipt of this packet, expressed as a percentage.
X	***Noise dBm***	This column displays the noise detected on receipt of this packet, expressed in dBm (decibel milliWatts).

Table 4.4 Packet List Options columns, showing defaults (continued)

Default	Column	Description
X	***Size***	This column displays the length of the packet in bytes, including the packet header.
	IP Length	This column displays the total length of the IP datagram, in bytes. It includes the length of the IP header and data.
	IP ID	This column displays the IP ID (Identifier) of the packet. The IP ID uniquely identifies each IP datagram sent by a host. It normally increments by one each time a datagram is sent.
	Date	This column shows the date the packet was received.
X	***Absolute Time***	This column displays the time-stamp assigned to each packet as the actual time of capture, according to the system clock of the computer on which AiroPeek is running. Use the ***Format*** view of the **Packet List Options** dialog to set the display units for all time-stamps to milliseconds or microseconds.
	Delta Time	This column shows the time-stamp of each packet as the elapsed time since the capture of the previous visible packet. (That is, if packets are hidden, the time shown is relative only to the previous *visible* packet.) Use the ***Format*** view of the **Packet List Options** dialog to set the display units for all time-stamps to milliseconds or microseconds.
	Relative Time	This column displays the time-stamp of each packet as the elapsed time since the start of the current AiroPeek session. You can set a particular packet as the "zero" time for all items in the Relative Time column. Packets captured before will show negative values, those after, positive values, all relative to the new zero time. To set a packet as the zero time by setting it as the Relative Packet, right click on the packet's line and choose **Set Relative Packet** from the context menu. Use the ***Format*** view of the **Packet List Options** dialog to set the display units for all time-stamps to milliseconds or microseconds.

Table 4.4 **Packet List Options columns, showing defaults (continued)**

Default	Column	Description
	Cumulative Bytes	If no Relative Packet is set, this column shows the total bytes represented by all the packets from the first packet in the list to the current packet, inclusive. If you have set a Relative Packet, this column shows the total bytes from the Relative Packet to the current packet, inclusive. To set a packet as the Relative Packet, right click on the packet's line and choose **Set Relative Packet** from the context menu.
X	***Protocol***	This column displays the protocol type of the packet. This may be shown as an LSAP value, a SNAP value, or a ProtoSpec. If you have established a symbolic name for a protocol otherwise unknown to ProtoSpecs, that name may be taken from the Name Table and displayed here.
	Filter	This column displays the name of the filter that allowed the packet to be entered into the capture buffer.
X	***Summary***	This column lists any information provided about the packet by enabled Analysis Modules.
	Analysis Module Name	This column displays the name of the Analysis Module that supplied the information on that packet that is displayed in the ***Summary*** column.
X (AiroPeek NX only)	***Expert***	Unique to AiroPeek NX, this column presents data collected about the packet by the Expert Analysis tools. Typically, this is a short description of the type of problem found in the packet, and may include a measurement (such as response time since another named packet) which caused this packet to be identified as a problem.

In order to see the right-most columns in the Packet List, you may need to use the scroll bars or resize the Capture window.

Making notes on packets and packet files

The Notes tools let you make notes on individual packets within the packet list, and the annotations will be preserved when you save the file as an AiroPeek packet file (*.apc) or compressed packet file (*.wpz). In addition, you can make notes on the packet file as a whole by adding comments to the **Properties** dialog. These too will be preserved when the file is saved in either AiroPeek format.

To make a note on an individual packet, select the packet in either the ***Packets*** view or in its own **Packet Decode** window and click the **Insert Note** button in the header section of the view or window. (See Figure 4.5 on page 69 for a detail of the header section of the ***Packets*** view of a Capture window, with all the buttons labeled.) This brings up the **Insert Note** dialog (Figure 4.7). An icon representing a note appears in the ***Packet*** column (the column showing packet numbers) of the ***Packets*** view for any packet with an associated note.

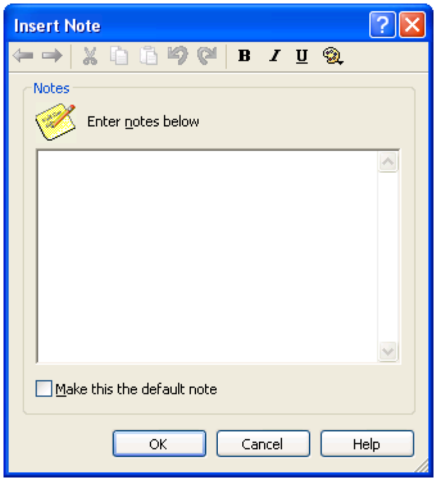
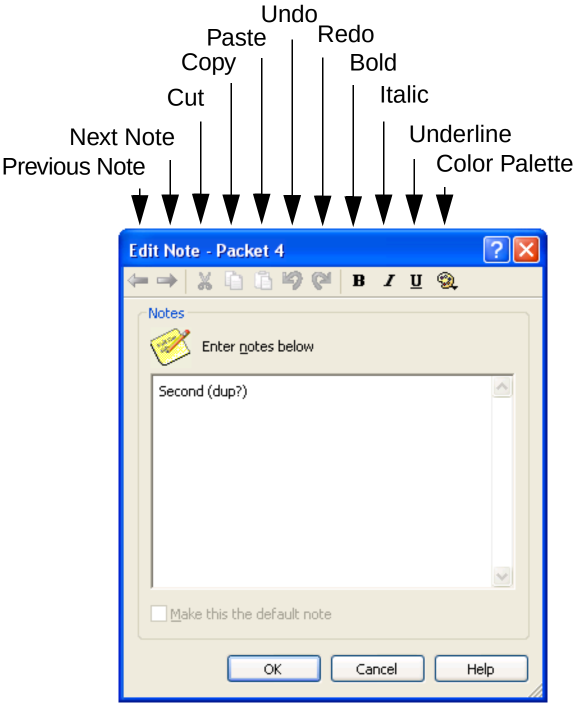


Figure 4.7 Insert Note dialog

You can assign the same note text to multiple packets in either of two ways. You can highlight multiple packets, click the **Insert Note** button, fill in the note text in the **Insert Note** dialog and click **OK**. This assigns the same note to all the selected packets at once. Alternatively, you can compose a note and check the checkbox labeled *Make this the default note*. While this option is checked, the same text will be entered for you in each **Insert Note** dialog you open. To add this exact note to one or more packets, highlight them, click the **Insert Note** button and accept the default text by clicking the **OK** button or using the **Enter** key.

Note: If you want a group of notes to have a character string in common, it is better to use the **Copy** and **Paste** buttons to insert this shared text into each note as it is created. When you uncheck the *Make this the default note* option, the program will not remember a previously chosen “default note” text.



Second (dup?)

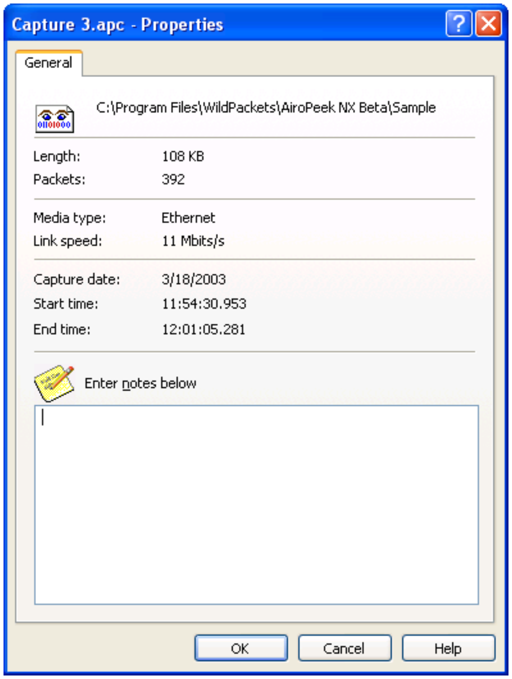
□ Make this the default note

Figure 4.8 Edit Note dialog

To view or edit the contents of a note, highlight the packet to which it belongs (or open the packet in the **Packet Decode** window) and click the **Edit Note** button to open the **Edit Note** dialog (Figure 4.8). In addition to a full range of editing features, the **Edit Note** dialog allows you to step through the packet notes. Use the **Next Note** and **Previous Note** buttons to steps forward or backward through the notes, in packet number order. As each note is presented in the **Edit Note** dialog, the packet to which it belongs becomes the selected (highlighted) packet in the Packet List pane of the ***Packets*** view.

To delete one or more notes, highlight the packet(s) to which they belong and click the **Delete Note** button.

You can also make a note on the contents of a Capture window or Packet File window as a whole by entering text in the **Properties** dialog. Click the **Properties** button in the header section of the ***Packets*** view to open the **Properties** dialog (Figure 4.9). In addition to providing a container for notes, the **Properties** dialog presents summary information, such as file size, number of packets, network type, and capture date and times. This information, along with any notes you have entered, will be saved and associated with the saved packet file.



Capture 3.apc - Properties

General

C:\Program Files\WildPackets\AiroPeek NX Beta\Sample

Length: 108 KB
Packets: 392

Media type: Ethernet
Link speed: 11 Mbits/s

Capture date: 3/18/2003
Start time: 11:54:30.953
End time: 12:01:05.281

Enter notes below

Figure 4.9 Properties dialog for a Packet File window

Statistical display views

Capture windows offer six different displays of statistics: ***Node***, ***Protocol***, ***Summary***, ***Channels***, ***Signal***, and ***Graphs***. In addition, Capture windows in AiroPeek standard offer the ***Conversations*** view.

Statistics in Capture windows are calculated based on all the packets that have been accepted to the buffer since capture was initiated. If continuous capture is enabled and the buffer has wrapped, this may mean that the statistics are based on many more packets than are present in the buffer. If you use the Hide functions to alter the apparent contents of the buffer, it will force a recalculation of all the statistics to match the changed visible contents, and you will lose all accumulated data.

The ***Graphs*** and ***Conversations*** views, unlike the other statistical views, have no direct equivalents in Monitor statistics. The other statistics views of a Capture window or a Packet File window are substantially the same as the Monitor statistics windows of the same names. The ***Signal*** view of a Capture window or Packet File window, for example, is identical in layout and capability to the ***Signal*** view of the **Channel Statistics** window in Monitor statistics. Please see Chapter 9, “Statistics” on page 147, for a detailed discussion of each of these types of statistical displays. For notes on important differences between Monitor statistics and statistics in Capture windows and Packet File windows, see “Statistics in capture windows” on page 180.

For a complete discussion of the ***Graphs*** view, see Chapter 10, “Graphs of Monitor and Capture Statistics” on page 193. For a complete discussion of the ***Conversations*** view, see “Conversations” on page 183. For information on saving and printing statistics from these windows, see “Saving reports from capture windows” on page 187. You can also save statistics from Capture windows at set intervals by using the ***Statistics Output*** view of the **Capture Options** dialog. Please see “Statistics output views” on page 188 for details.

Graphs view

The ***Graphs*** view presents a variety of graphs displaying statistics from the current window in real time. All graphs, including the default set, are editable and configurable. (Default graphs include equivalents to the **Size** and **History** graphs found in Monitor statistics, for example.) You can add to, delete, rearrange, create, edit, export, and import graphs of nearly any form, each based on single or multiple statistics from the current Capture window.

For a complete discussion of the ***Graphs*** view and all its functions, please see Chapter 10, “Graphs of Monitor and Capture Statistics” on page 193.

Log view

The ***Log*** view contains information, primarily generated by Analysis Modules, about the packets in the buffer of the Capture window or Packet File window. The ***Log*** view also notes such things as start capture times. Log messages are not saved with saved packet files, but rather are regenerated each time the buffer is renewed—by opening the file or by hiding or unhiding packets, for example.

Note: The ***Log*** view in a Capture window or a Packet File window is limited to 128k bytes. Older data will be discarded to make room for newer entries.

For more about Analysis Modules and the types of messages they can write to the ***Log*** view, please see Chapter 13, “Analysis Modules” on page 257.

Conversations view

Unique to AiroPeek standard, the ***Conversations*** view groups the traffic in a Capture window or Packet File window into conversations between pairs of nodes. The ***Conversations*** view presents information about each conversation in the upper Conversations pane and additional information about each partner in the lower Naming and Statistics pane.

For more about the ***Conversations*** view and how to use it, please see “Conversations” on page 183.

Expert view

Unique to AiroPeek NX, the ***Expert*** view provides expert analysis of delay, throughput and a wide variety of network problems in a conversation-centered view of traffic in a Capture window or Packet File window.

For more about the ***Expert*** view and the expert analysis it provides, please see Chapter 5, “Expert View and Expert ProblemFinder” on page 103.

Peer Map view

Unique to AiroPeek NX, the ***Peer Map*** view is a powerful tool for visualizing network traffic in a Packet File window or Capture window. The Peer Map displays the nodes in the current window around an elongated ellipse. Lines between communicating nodes (peers) represent the traffic. The line weight shows the volume of traffic between each pair of communicating peer nodes. The line color shows the protocol in use between each pair of nodes.

Like all other views of a Capture window or Packet File window, the ***Peer Map*** view is based on the packets that are visible in the ***Packets*** view. The ***Peer Map*** also contains its own independent tools to control the display of nodes and types of network traffic. This lets you quickly create a picture of all the traffic in a particular protocol, for example, or all the nodes sending or receiving multicast traffic.

For a detailed description of how to use the Peer Map and all the functions of the ***Peer Map*** view, please see Chapter 6, “Peer Map” on page 121.

Filters view

The ***Filters*** view of a Capture window shows a list of all available filters and allows you to choose which filters to enable for that Capture window by checking the checkbox next to that filter’s name. To choose how the filter(s) will be applied, use the **Accept Matching** or **Reject Matching** buttons at the top left of the ***Filters*** view. When you choose **Accept Matching**, only those packets which match the parameters of at least one of the enabled filters will be placed in the buffer. When you choose **Reject Matching**, only those packets which do not match any of the enabled filters will be entered in the buffer.

By double-clicking on any filter, you can open it in an **Edit Filter** dialog and change or simply verify its parameters. For more about filters and how to use them, see Chapter 11, “Filters” on page 207.

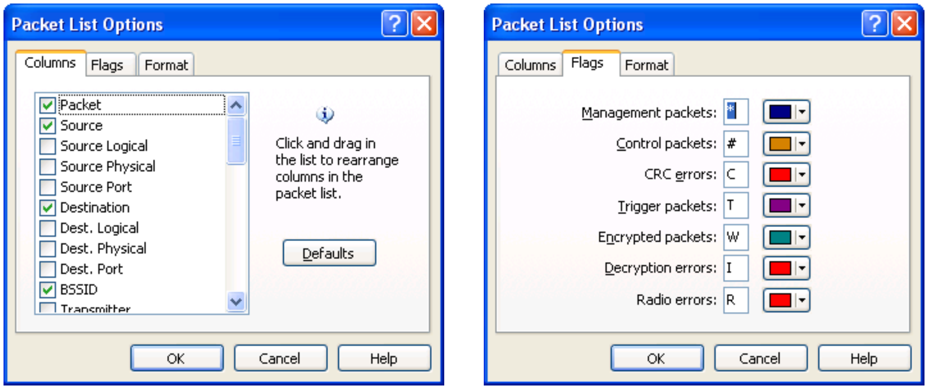
The ***Filters*** view only exists in Capture windows. To apply filters to packets already captured to a buffer, either in a Capture window or a Packet File window, use the **Select…** command from the **Edit** menu. For more on how to use filters to select captured packets, see “Select dialog: filters, analysis modules and more” on page 313.

Customizing views

You can customize the way in which certain types of information are displayed in the Packet List pane of the ***Packets*** view of Capture windows and Packet File windows using the **Packet List Options** dialog. Other data display characteristics can be customized in a way that affects the display of certain data in all windows, including Monitor statistics. These more general display parameters include the ***Fonts*** view of the **Options** dialog (available under the **Tools** menu) and the **Display Format** and **Color** submenus under the **View** menu. Each of these formatting tools is discussed in this section.

Packet list view options

The column content, color and format in which packet information is displayed in Capture windows and Packet File windows can be customized in the **Packet List Options** dialog. To open the **Packet List Options** dialog for a particular Packet List, click anywhere in the column headers of the list, or right-click in the display and choose **Packet List Options…** from the context menu.



☑ Packet
☑ Source
□ Source Logical
□ Source Physical
□ Source Port
☑ Destination
□ Dest. Logical
□ Dest. Physical
□ Dest. Port
☑ BSSID
□ Transmitter

Click and drag in the list to rearrange columns in the packet list.

Management packets: *
Control packets: #
CRC errors: C
Trigger packets: T
Encrypted packets: W
Decryption errors: I
Radio errors: R

Figure 4.10 Packet List Options dialog, Columns and Flags views

Customizing columns in the packet list

You can customize the information to be displayed about each packet in the Packet List pane of the ***Packets*** view by adding, deleting, or rearranging the columns. You can, for example, keep an inventory of the devices on a network segment which shows the physical, logical, and symbolic names for each device by creating a customized Capture window with only these columns.

Left-click anywhere in the Packet List column headings to bring up the **Packet List Options** dialog. Choose the ***Columns*** view (by clicking the labeled tab) to display a list of available column types. The columns currently used in the ***Packets*** view of the active Capture window will have a ✔ checkmark in the checkbox next to their entries in the scrollable list. Uncheck any you wish to remove and check any you wish to add to the Packet List of the active window. A descriptive list of all available column types is shown in Table 4.4.

When you save a packet file as a tab or comma-delimited file, the information is saved in the same column order as appears in the Packet List pane of the ***Packets*** view. You can rearrange the order of the columns in the Packet List pane using drag and drop in either the Packet List itself or in the list of columns shown in the ***Columns*** view of the **Packet List Options** dialog. To use drag and drop in the Packet List itself, click in the heading of the column you wish to move, and hold down the mouse button. You can drag the heading to any other position and drop it there by releasing the mouse button. You can use the same technique to rearrange the order of the column types in the ***Columns*** view of the

Packet List Options dialog, but in this case you must also click **OK** in the **Packet List Options** dialog for the changes to take effect.

Packet list flag options

The ***Flags*** view of the **Packet List Options** dialog defines both the flag character and the color associated with flagged packets. These are: *Management packets*, *Control packets*, *CRC error*, *Trigger packets*, *Encrypted packets*, and packets with *Decryption errors* or *Radio errors*. You can use the dialog to assign a flag character and/or color to any of these packet types.

Table 4.5 **Flag characters and colors, default values**

Flagged Packet Type	Character	Color
Management packets (authentication, association, synchronization,…)	*	(blue is default)
Control packets (RTS, CTS, ACK, and so forth)	#	(orange is default)
CRC error (corrupt data)	*C*	CRC Error color (red is default)
Trigger packets (match an enabled trigger)	*T*	Trigger color (purple is default)
Encrypted packets (WEP bit set)	*W*	(green is default)
Decryption errors	*I*	(red is default)
Radio errors	*R*	(red is default)

To assign a character, simply highlight the existing character and type over it. To assign a color, click on the color swatch to open a palette of alternative colors. If you choose **Flag** in **Color** under the **View** menu, the color associated with the packet type will be used for all information displayed about that type of packet.

Packet list format options

The ***Format*** view of the **Packet List Options** dialog allows you to set the *Time-Stamp format* to use *Milliseconds* or *Microseconds* as its units, by choosing one of these from the drop-down list. By checking the appropriate checkbox, you can choose to *Show an ellipsis for truncated items* in Packet List columns and/or *Prefix addresses and protocols with the type* appropriate to them and/or *Show port names*. You can also choose to *Use protocol color for summary column* by checking that checkbox. When checked, this option displays the information provided by Analysis Modules and shown in the ***Summary*** column in the color assigned to the relevant protocol by ProtoSpecs.

Tip The same font is used throughout the program to display information discovered by AiroPeek. This font is used in the packet list and all other views of Capture windows, Packet File windows, and Monitor statistics. You can globally change this font in the ***Fonts*** view of the **Options** dialog. Please see “Fonts view” on page 29 for details.

Node display format options

The **Display Format** submenu is available from the **View** menu. At a minimum, packets are identified by the **Physical Address** of the source and destination nodes. If you choose **Name Table Entry** and there is a Name Table entry for a node, AiroPeek will use the node’s name instead of its address whenever it encounters packets to or from that node. The **Logical Address** item causes AiroPeek to show logical instead of physical addresses, wherever logical addresses are available. Before a packet is displayed, AiroPeek checks its protocol type. If it is one of the types that AiroPeek recognizes, it can replace the physical address with its logical address according to the protocol type.

Color display options

The **Color** submenu of the **View** menu determines how colors *already assigned in other dialogs* will be used in displaying packets, as well as node and conversation statistics in all displays. There are four sources of color assignments for elements of network traffic in AiroPeek:

- The ***Flags*** view of the **Packet List Options** dialog (available by left-clicking anywhere in the Packet List pane headers) determines the color associated with error or trigger packets. You can also assign a color to 802.11 WLAN management packets and control packets, as well as to WEP encrypted packets and/or to packet with decryption errors. (These choices are not meaningful for statistics displays.)
- The **Edit Name** dialog in the **Name Table** can set the color for packets associated with a particular address (node), port, or protocol.

- ProtoSpecs assign colors to all the protocols they know how to identify, and their color choices cannot be overridden.
- The **Edit Filter** dialog can set the color for any filter you create or edit. (These choices are not meaningful for statistics displays.)

The **Color** sub-menu of the **View** menu uses the color information from these other sources, and applies it to the display of packets in ***Packets*** view in the ways described in the table below for each of the available choices. A ✔ checkmark appears beside the enabled choice.

Table 4.6 **View menu > Color menu choice items**

Color Menu Item	Description
Source	This choice causes packets sent out by a particular node to be displayed in the color assigned to that node in the Name Table.
Destination	This choice causes packets destined for a particular node to be displayed in the color assigned to that node in the Name Table.
Protocol	This choice causes packets to be displayed in the color assigned to protocols by ProtoSpecs. If ProtoSpecs cannot identify the protocol *and* the protocol is listed in the Name Table and has a color assigned there, then the color assigned in the Name Table will be used.
Filter	This choice causes packets that are captured through a filter to be displayed in the color assigned to that filter in the **Edit Filter** dialog. (This choice is not meaningful for statistics displays.)
Flag	This choice causes packets that are captured as a result of a network event to be displayed in the color assigned to trigger, error, and other flagged packet types in the **Packet List Options** dialog. (This choice is not meaningful for statistics displays.)
Independent	This choice causes each of the above items to display in its own assigned color.
No Color	This choice turns off all color coding.

Scroll during capture

When **Auto Scroll** is enabled, the most recently captured packet will always appear as the last packet in the Packet List pane of the ***Packets*** view. Use the **Auto Scroll** button at the top of the ***Packets*** view of the Capture window to toggle this feature.

When this option is disabled, the Packet List pane does not change as packets are added to the buffer. The window does change, however, when continuous capture is enabled. The scroll bar at the right of the pane will move to show that it is keeping the same relative position in the whole buffer. As the buffer fills, the scroll bar will move up. If you chose to *Discard all packets when wrapping*, the scroll bar will move to the top of the display the first time the buffer is emptied, then stay there. If you chose *Discard oldest packets first (use ring buffer)*, the scroll bar will move up and down, following the relative position of the initial “end of file” marker.

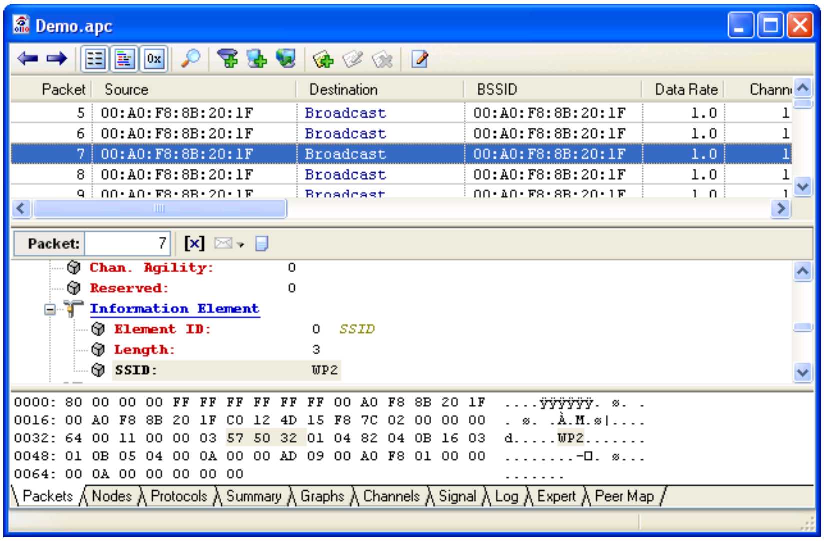
You may wish to make auto-scroll the default state for all Capture windows. Choose **Options…** from the **Tools** menu to open the **Options** dialog. In the ***Workspace*** view, click the checkbox beside *Resume auto-scroll in the packet lists after [number] seconds*, and enter the number of seconds. Auto scroll does use some processor resources. For this reason, the auto-scroll resume feature is not enabled by default.

Packet file windows

Packet files in AiroPeek format are loaded into their own individual Packet File windows.

A Packet File window is very similar in structure, function and layout to a Capture window. With the important exceptions noted below, everything described in this chapter about Capture windows is also true of Packet File windows.

The differences between them are due to their differences in function. There is no capture in a Packet File window and no loading of saved packets in a Capture window. The title of a Packet File window shows the name of the loaded file. The header section of the Packet File window shows no information relating to capture (no Progress section). It does, however, show a value for *Packets* (total packets in the file) in the window status bar. Figure 4.11 below shows the ***Packets*** view of a Packet File window with the Packet List, Decode and Hex panes all visible.



Packet	Source	Destination	BSSID	Data Rate	Chann
5	00:A0:F8:8B:20:1F	Broadcast	00:A0:F8:8B:20:1F	1.0	1
6	00:A0:F8:8B:20:1F	Broadcast	00:A0:F8:8B:20:1F	1.0	1
7	00:A0:F8:8B:20:1F	Broadcast	00:A0:F8:8B:20:1F	1.0	1
8	00:A0:F8:8B:20:1F	Broadcast	00:A0:F8:8B:20:1F	1.0	1
9	00:A0:F8:8B:20:1F	Broadcast	00:A0:F8:8B:20:1F	1.0	1

```
Packet: 7
  Chan. Agility:          0
  Reserved:               0
  Information Element
    Element ID:             0   SSID
    Length:                 3
    SSID:                   WP2
```

```
0000: 80 00 00 00 FF FF FF FF FF FF 00 A0 F8 8B 20 1F   ....ÿÿÿÿÿÿ. ø. .
0016: 00 A0 F8 8B 20 1F C0 12 4D 15 F8 7C 02 00 00 00   . ø. .À.M.ø|....
0032: 64 00 11 00 00 03 57 50 32 01 04 82 04 0B 16 03   d.....WP2.......
0048: 01 0B 05 04 00 0A 00 00 AD 09 00 A0 F8 01 00 00   ........-□. ø...
0064: 00 0A 00 00 00 00 00                               .......
```

Figure 4.11 AiroPeek NX Packet File window, 3-pane view

There are, of course, no triggers or use of filters for capture in a Packet File window, but you can use filters as tests for selecting packets, using the **Select** dialog. (Please see “Select dialog: filters, analysis modules and more” on page 313.) You can include a ***Filter*** column in the Packet List pane of the ***Packets*** view, even though no filter information is saved with AiroPeek packet files. If a Packet File window has this column and you make a selection in the **Select** dialog using a filter match as the test, the name of the filter that allowed each packet to be selected will show up in the ***Filter*** column.

Note: Statistics in a Packet File window are calculated based on packets visible in the buffer. If you hide or unhide packets (using the commands from the **Edit** menu), it will force a recalculation of the statistics to reflect the changed visible contents of the buffer.

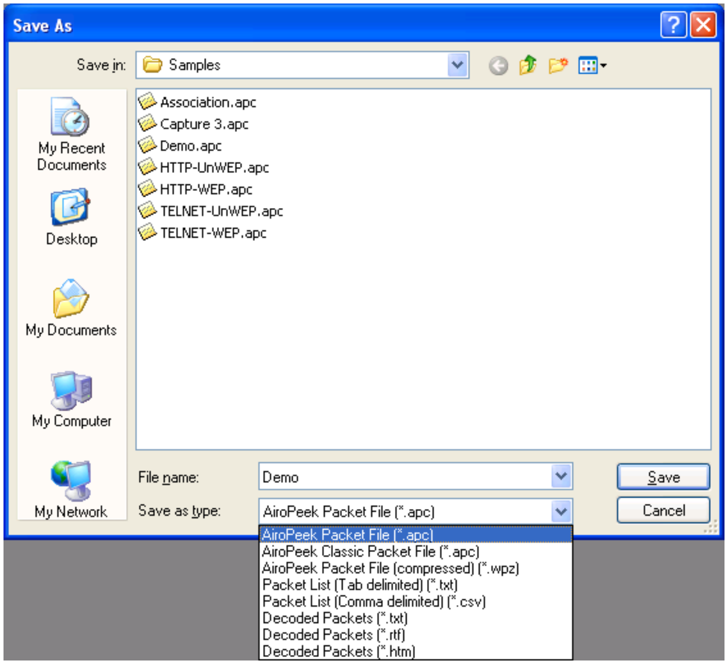
Saving, loading and printing captured packets

You can save the packets captured during an AiroPeek session for later examination and comparison. To save all captured packets, choose the **Save All Packets…** command in the **File** menu or type **Ctrl + S**.

To save only certain packets, select the ones you want, then choose the **Save Selected Packets…** command in the **File** menu. **Save Selected Packets…** saves only the packets currently highlighted in the active Capture window or Packet File window.

For more information about selecting packets, please see Chapter 15, “Post-capture Analysis” on page 305.

Choosing either of the above commands opens the **Save As** dialog:



Save in: Samples

File name: Demo

Save as type: AiroPeek Packet File (*.apc)

Figure 4.12 Saving packets as lists or as decoded packets

Save file formats

In this dialog, you can assign a file name and choose among six file formats:

- *AiroPeek Packet File (*.apc)*, the default choice, saves to the native AiroPeek file format, with a *.apc extension.
- *AiroPeek Classic Packet File (*.apc)*, saves to the older version of the AiroPeek packet file format, with a *.apc extension. Use this format to make files readable

by older programs, such as older versions of AiroPeek, NetSense, and ProConvert.

- *AiroPeek Packet File (compressed) (*.wpz)*, saves to the native AiroPeek file format, but using file compression to save disk space. Uses a *.wpz extension.
- *Packet List (Tab delimited) (*.txt)* creates a tab-delimited text file (*.txt) containing only the information visible in the ***Packets*** view of the active Capture window or Packet File window. For a complete description of this option, please read the section entitled “Saving as packet list (comma- or tab-delimited)” below.
- *Packet List (Comma delimited) (*.csv)* creates a comma-delimited text file (*.csv) containing only the information visible in the ***Packets*** view of the active Capture window or Packet File window. For a complete description of this option, please read the section entitled “Saving as packet list (comma- or tab-delimited)” below.
- *Decoded Packets (*.txt)* saves the decoded packets as a plain text file (*.txt).
- *Decoded Packets (*.rtf)* saves the packets in an RTF file (*.rtf) that preserves the text formatting and page layout of the same packets in the ***Decode*** view of an AiroPeek **Packet Decode** window. For a complete description of this option, please see “Saving as decoded packets (RTF or HTML)” below.
- *Decoded Packets (*.htm)* saves the packets in an HTML file (*.htm) that preserves the text formatting and page layout of the same packets in the ***Decode*** view of an AiroPeek **Packet Decode** window. For a complete description of this option, please see “Saving as decoded packets (RTF or HTML)” below.

Saving as packet list (comma- or tab-delimited)

When you choose to save packets as *Packet List (Comma-delimited)* or *Packet List (Tab-delimited)*, the output file contains only the information shown in the ***Packets*** view of the active Capture window or Packet File window. By changing the information displayed in that view (by adding or subtracting columns, re-ordering columns, hiding or unhiding packets, and so forth), you can fully tailor the output to either of these file types. Comma-delimited and tab-delimited files are widely supported interchange formats among spreadsheet and database programs.

Saving as decoded packets (RTF or HTML)

AiroPeek can save decoded packets to RTF (Rich Text Format) or HTML (HyperText Markup Language) formats. Either of these text plus mark-up formats will preserve the text formatting and page layout used to present the decoded packets on the screen (for example, in the ***Decode*** view of a **Packet Decode** window or the Decode pane of the ***Packets*** view of a Capture window or Packet File window).

Choosing to save packets in either of these formats provides you with a file that includes information similar to that displayed in the **Packet Decode** window for each packet saved.

Loading packets from a file

Packets saved in the AiroPeek file format (*.apc) or the compressed packet file format (*.wpz) can be opened in a Packet File window using the **Open…** command in the **File** menu. The file **Open** dialog allows you to open files of the following formats:

- *AiroPeek Packet File (*.apc, *.wpz)*: Files with the *.apc extension are created in AiroPeek by using the **Save All Packets…** or **Save Selected Packets…** commands from the **File** menu. The current version of AiroPeek can read files in either its own native format (*.apc), AiroPeek Classic format (also *.apc), or the compressed version of AiroPeek format (*.wpz).
- *NAI Sniffer Wireless File (*.cap, *.caz)*: These are files containing packets captured in the Sniffer Wireless® program. For AiroPeek to recognize these files, they must have an extension of *.cap or *.caz.

You can only load one file in a given Packet File window. You can use the PeekCat command line utility (located in the AiroPeek\Bin directory) to concatenate multiple AiroPeek packet files. Please see the PeekCat.txt file in the \Bin directory for more information.

Note: ProConvert, the WildPackets packet trace file conversion utility, can convert in either direction between a number of packet trace file formats, including AiroPeek Classic file format and the formats of other wireless and Ethernet analyzers and capture utilities. For more information on ProConvert, please visit the Product Information pages at http://www.wildpackets.com.

Printing packet lists and packet decode windows

To print the complete list of packets shown in the ***Packets*** view of the active Capture window or Packet File window, choose the **Print…** command from the **File** menu.

Printing lists of selected packets

If you would like to print only some of the list of packets in a Capture window or Packet File window, use the functions under the **Edit** menu to hide everything except what you wish to print. When you choose the **Print…** command from the **File** menu, only the listings for the visible packets will be printed. For more on selecting, hiding and unhiding packets, please see Chapter 15, “Post-capture Analysis” on page 305.

To print in landscape format or to use other standard printer options, choose the **Print Setup…** command in the **File** menu.

Printing packet decode windows

To print individual decoded packets, select the packets you would like to print and choose **Print Selected Packets…** from the **File** menu. This will print out a formatted text version of *only* the decode portion of the selected packets. This will print the packet decodes as a single document without page breaks between the packets.

Tip An alternative is to save the decoded packets as RTF or HTML and print them from another application that can read and print those file types. This alternative preserves the formatting of the **Packet Decode** window and allows multiple packets to be printed on individual pages.

AutoCapture

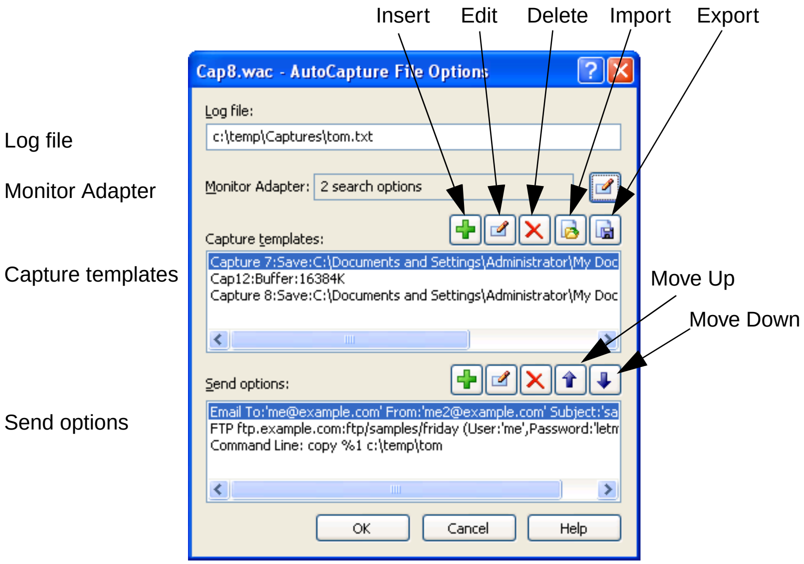
The AutoCapture feature allows the user to set AiroPeek to automatically start multiple Capture windows, each with its own buffer size, adapter selection settings, save options, triggers, and filters. When capture in all windows is completed, the AutoCapture function sends the resulting capture files by a user-specified method, then exits the application. AutoCapture settings are saved in a file which can be sent to a remote user. Remote users can double-click on the file to run it immediately, or schedule AiroPeek to run using the Windows Scheduler.

Creating and editing AutoCapture files

To create or edit AutoCapture (*.wac) files, choose the **Create New…** or **Edit Existing…** sub-menu choices under **AutoCapture** in the **File** menu. This brings up the **AutoCapture File Options** dialog (Figure 4.13). When editing an existing file, the name of the *.wac file is shown in the dialog title. When creating a new file, the dialog title appears as **New AutoCapture File Options**. There are four sections in the **AutoCapture File Options** dialog: *Log file*, *Adapter search*, *Capture templates*, and *Send options*. Each of these is described below.

Log file

You can optionally specify the name and location of a text log file for an AutoCapture file. All of the actions taken by the AutoCapture file will be appended to the end of the specified log file in text format.



Cap8.wac - AutoCapture File Options

Log file: c:\temp\Captures\tom.txt

Monitor Adapter: 2 search options

Capture templates:

```
Capture 7:Save:C:\Documents and Settings\Administrator\My Doc
Cap12:Buffer:16384K
Capture 8:Save:C:\Documents and Settings\Administrator\My Doc
```

Send options:

```
Email To:'me@example.com' From:'me2@example.com' Subject:'sa
FTP ftp.example.com:ftp/samples/friday (User:'me',Password:'letm
Command Line: copy %1 c:\temp\tom
```

Figure 4.13 AutoCapture File Options window

Monitor adapter and adapter search

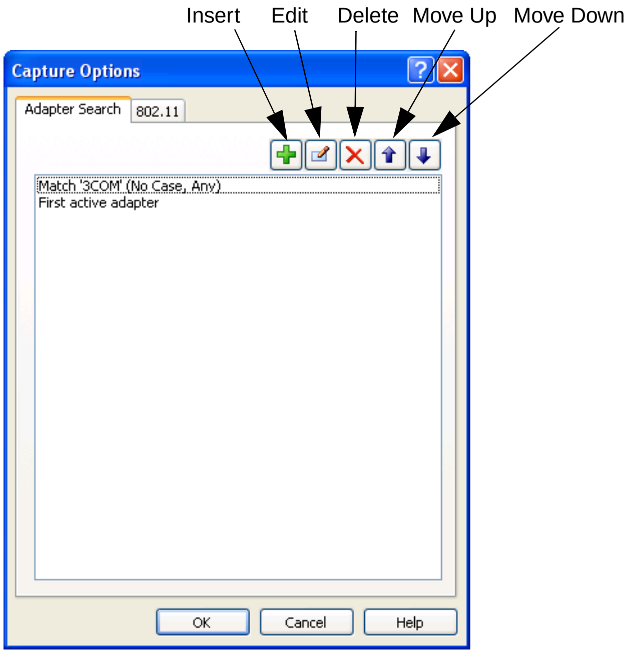
The AutoCapture file must be able to select an 802.11 WLAN adapter for AiroPeek to use in capturing packets. You can use the program’s default capture adapter, or you can specify one or more search methods for locating an adapter. The program’s default adapter is the most recent valid adapter (an actual NIC, not *File* or *None*) selected as the Monitor adapter in the **Monitor Options** dialog.

If you are unsure of the current default adapter for the target instance of AiroPeek, or if you want to specify the default adapter by setting your own choice for the Monitor Adapter on the target system, you can add one or more adapter search instructions to the

Monitor Adapter section of the **AutoCapture File Options** dialog. Click the **Edit** button beside the *Monitor Adapter* text display box to open the special AutoCapture version of the **Capture Options** dialog (Figure 4.14). In the ***Adapter Search*** view of this dialog you can **Insert**, **Edit**, or **Delete** adapter search routines using the named buttons, or use the **Move Up** and **Move Down** buttons to change the order of adapter search routines.

Each Adapter Search method can have its own options in the ***802.11*** view of the special AutoCapture version of the **Capture Options** dialog. Note that the ***802.11*** view in this dialog differs from all other such views in one respect. Lists of channels are not restricted in this ***802.11*** view, and any channel may be chosen. You must select channels appropriate to the adapter that will be chosen in order for capture to take place. For a detailed description of the ***802.11*** view and how to use it, please see “802.11 view” on page 21.

AiroPeek will attempt to select a Monitor adapter based on each search method, in the order specified in the *Adapter search* section of the **AutoCapture File Options** dialog. AiroPeek will use the first usable adapter it finds, and ignore any further search methods.



Match '3COM' (No Case, Any)
First active adapter

Figure 4.14 Adapter Search view of the special AutoCapture Capture Options dialog

Important! There are two levels of adapter search in an AutoCapture file. The settings in the *Monitor Adapter* section of the **AutoCapture File Options** dialog provide the default adapter for the AutoCapture file as a whole. The settings in the ***Adapter Search*** view of the **Capture Options** dialog for each separate capture template within the *.wac file define the method for selecting the adapter for the Capture window made from that template. The adapter selected for the AutoCapture file as a whole is treated as the default adapter by the ***Adapter Search*** settings of each individual capture template.

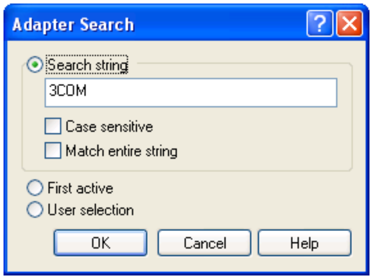
Note: After an AutoCapture (*.wac) file has been run successfully, it remembers the adapter it last used. The next time it is run, it first attempts to use that same adapter, regardless of any settings in the *Adapter search* section. If that attempt fails, it then runs through the choices, as if the AutoCapture file were being run for the first time. An AutoCapture file will only treat an actual NIC as the default adapter, never *File* or *None*.

Table 4.7 **Adapter search methods**

Search Method	Usage
Search string	Selects the first adapter whose description contains a match with the text in the user-supplied search string. You can constrain the search to be *Case sensitive* and/or to *Match whole string* by checking the checkbox beside either or both of those choices. You can see examples of the adapter descriptions over which this Adapter Selection method will search, in Windows **Device Manager** or in the adapter display in the Status Bar of the **AiroPeek** main program window.
First active	Selects the first active, usable 802.11 WLAN adapter in the list of adapters installed on the host computer.

Table 4.7 **Adapter search methods (continued)**

Search Method	Usage
User selection	Opens the **Select Adapter** dialog, from which a user must actively choose an 802.11 WLAN adapter. Note that if you use this method, AiroPeek will wait indefinitely for user input.
Default (blank)	If no specific adapter search method is listed in the *Adapter search* section of the **AutoCapture File Options** dialog, AiroPeek will attempt to use its default adapter. (The first time you run AiroPeek you must select an 802.11 WLAN adapter for the program's use. The last adapter used by AiroPeek becomes the default adapter for the program. Only an actual NIC can be the default adapter, never *File* or *None*.) If any explicit Adapter Search methods are listed in the *Adapter search* section, the AutoCapture file will attempt to use them first. That is, the search for the default adapter is always present, but is always last in the list of adapter search methods.



Adapter Search

● Search string

3COM

□ Case sensitive

□ Match entire string

○ First active

○ User selection

Figure 4.15 Adapter Search dialog

To define a new adapter search method, click the **Insert** button in the *Adapter search* section of the **AutoCapture File Options** dialog. This opens the **Adapter Search** dialog (Figure 4.15). Use the radio buttons to choose the adapter search method. Your choices are: *Search string*, *First active*, or *User selection*. Each of these methods is described in Table 4.7. When you have defined the new search method, click **OK** to add it to the list and close the dialog, or click **Cancel** to close the dialog without creating a new search method. New adapter search methods are added to the bottom of the list, and show as much of the method’s parameters as can be displayed on a single line in the *Adapter search* section of the **AutoCapture File Options** dialog.

To edit a search method, highlight its entry in the *Adapter search* section of the **AutoCapture File Options** dialog and click the **Edit** button to bring up the **Adapter Search** dialog with that method’s parameters displayed and ready to edit. Click **OK** to accept your changes or click **Cancel** to close the dialog without changing the adapter search method.

To delete a search method from the list, highlight its entry in the *Adapter search* section of the **AutoCapture File Options** dialog and click the **Delete** button.

AiroPeek uses the search methods in order from top to bottom as they appear in the *Adapter search* section of the **AutoCapture File Options** dialog. To change the list order, highlight a list item and use the **Move Up** or **Move Down** buttons to move the item.

Capture templates

AutoCapture files use capture templates to create Capture windows. Each template creates one Capture window. A single AutoCapture file can have multiple capture templates and create multiple Capture windows. You can use existing capture templates, or you can create or modify capture templates from within the **AutoCapture File Options** dialog.

A capture template specifies all the parameters found in the **Capture Options** dialog for a given Capture window. Although you can use capture templates created in other programs (AiroPeek, for example), capture templates used for AutoCapture have three special requirements:

- Because AutoCapture files are intended to be usable on remote machines, the ***Adapter*** view of an ordinary capture template is replaced by an ***Adapter Search*** view in the capture templates created in or imported into an AutoCapture file.
- You must save captured packets before they can be sent using the *Send options*. In practice, this means you should enable the *Continuous capture* and *Save to disk* options in the ***General*** view of the **Capture Options** dialog for each template.
- A stop trigger must be set for each capture template, or the capture will never terminate and no files will be sent. Capture must stop in *all* the Capture windows created by a given AutoCapture file before *any* files will be sent. Automatic saving of captured packets is only supported under the *Continuous capture* setting in the ***General*** view of the **Capture Options** dialog. Under the

Continuous capture setting, only active user intervention or a stop trigger will stop capture.

Note: The ***802.11*** view in these special AutoCapture versions of the **Capture Options** dialog cannot determine in advance which channels will be supported by the adapter ultimately selected through the Adapter Search process. For this reason, all channels are available. Your choices in the ***802.11*** view must be supported by the adapter ultimately selected for capture, in order for any capture to take place.

To create a new capture template, click the **Insert** button in the *Capture templates* section of the **AutoCapture File Options** dialog. This opens the **Capture Options** dialog (Figure 4.2), where you can specify the name, buffer usage, packet slicing, and other parameters for the Capture window created from this template. For a detailed discussion of the **Capture Options** dialog and how to use it, please see “Capture options dialog” on page 55. When you have specified the capture options for this template, click **OK** to add it to the list.

To add a previously saved capture template to the list, click the **Import** button to bring up a file **Open** dialog. Use the file **Open** dialog to navigate to the location of the capture template (*.ctf) file you wish to add. Choose the file and click **OK** to add it to the list.

To save a capture template from the *Capture templates* list as a free-standing capture template for later re-use, highlight its entry in the list and click the **Export** button. This brings up a **Save As** dialog which you can use to name the template and navigate to the location where you would like to save the capture template (*.ctf) file.

Note: When you use **Import** to add a previously existing capture template to an AutoCapture file, the template’s parameters are copied into the AutoCapture file. If you then modify these parameters from within the **AutoCapture File Options** dialog, only the AutoCapture file’s copy of the template parameters is modified. The original capture template remains unchanged. When you delete an imported capture template from the list, the template is removed from the AutoCapture file, but the original capture template (*.ctf) file is unaffected. Similarly, when you use **Export** to save a capture template, any further changes made to that template in the **AutoCapture File Options** dialog have no effect on the previously saved version.

To edit the capture options for a particular capture template, highlight the template in the *Capture templates* section of the **AutoCapture File Options** dialog and click the **Edit** button. This opens the **Capture Options** dialog with that template’s parameters displayed and ready to edit. When you have made your changes, click **OK** to close the dialog and accept your changes, or click **Cancel** to close the dialog without changing the template's parameters.

Tip AiroPeek will automatically import a similarly named filter file found in the same location as the AutoCapture (.wac) file when starting an AutoCapture session. For example, if the AutoCapture file is named Agincourt.wac, AiroPeek will look in the same directory for a filter file named Agincourt.flt from which to import filters. AiroPeek adds the filters to the existing list, rather than replacing it. Duplicates of existing filters will be ignored if they have identical parameters as well as identical names. Filters with the same name but different parameters will be added with "*Copy of*" added to their names.

To delete a capture template from the list, highlight the listing for that template in the *Capture templates* section of the **AutoCapture File Options** dialog and click the **Delete** button.

Send options

When capture is stopped in all Capture windows, AiroPeek attempts to send a single capture file using the first send option listed in the *Send options* section of the **AutoCapture File Options** dialog. If the first send option fails, AiroPeek tries any remaining send options in the order in which they are listed in the *Send options* section. All capture files are sent using the first send option that succeeds, and any remaining send options are ignored. If no send option succeeds, no capture files are sent. There are three types of send option:

- *Email*
- *FTP*
- *Command line*

You can create multiple instances of the same basic type (for example, multiple Email send options, each using a different server), but only the first successful send option will actually be used by AiroPeek.

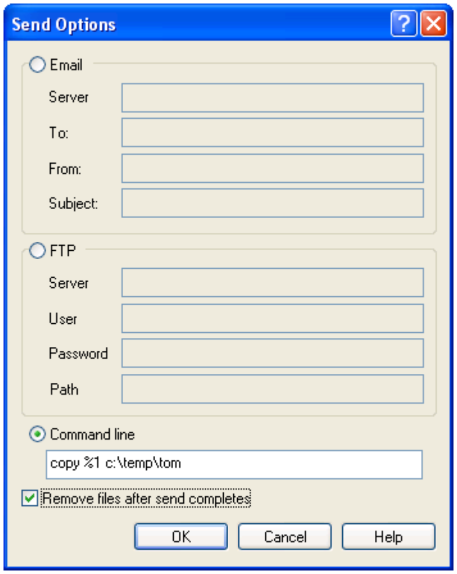
To create a new send option, click the **Insert** button in the *Send options* section of the **AutoCapture File Options** dialog. This brings up the **Send Options** dialog (Figure 4.16). Use the radio buttons to choose the type of option. Your choices are *Email*, *FTP* or *Command line*. Fill in the required information and any optional information for the chosen method, using the instructions in Table 4.8. Click **OK** to create the specified send option and close the dialog, or click **Cancel** to close the dialog without creating a new send option. New send options are added to the bottom of the list, and show as much of the option’s parameters as can be displayed on a single line in the *Send options* section of the **AutoCapture File Options** dialog.

Note: The *Remove files after send completes* option is enabled or disabled for each send option individually. The files are only removed if this option is enabled (checked) in the particular send option ultimately used to send the files, and is ignored when it is enabled in a send option that is not used.

Table 4.8 **Send option usage**

Option	Usage
Email	Sends the capture (*.apc) files as attachments in email, one file per email. You must specify a valid email *Server*, and valid email addresses in the *To* and *From* edit boxes. The *Subject* line is optional.
FTP	Copies the capture (*.apc) files to the specified *Path* (directory) using FTP. You must specify a valid FTP *Server*, a valid *User* name and *Password* for that server, and the *Path* to a valid directory on that server. Note: because capture (*.apc) files include a time signature in the file name, it is highly unlikely any two will ever have the same name, but not strictly impossible. In the unlikely event of identical file names, files will be overwritten only if the permissions for the *User* allow it.
Command line	Executes the specified command line instruction on each capture (*.apc) file in turn. Enter a valid command line in the text entry box, using the string `%1` as a substitute for the file names of the capture files. For example, to copy the files to the C:\temp\ directory, the command line would be: `copy %1 C:\temp\`
Remove files after send completes	The *Remove files after send completes* option removes each file after it is sent. Check to enable, uncheck to disable.

To edit a send option, highlight its entry in the *Send options* section of the **AutoCapture File Options** dialog and click the **Edit** button to bring up the **Send Options** dialog with that option’s parameters displayed and ready to edit. Click **OK** to accept your changes or click **Cancel** to close the dialog without changing the send option.



Send Options

○ Email

Server

To:

From:

Subject:

○ FTP

Server

User

Password

Path

● Command line

copy %1 c:\temp\tom

☑ Remove files after send completes

Figure 4.16 Send Options dialog

To delete a send option from the list, highlight its entry in the *Send options* section of the **AutoCapture File Options** dialog and click the **Delete** button.

AiroPeek tries the send options in order from top to bottom as they appear in the *Send options* section of the **AutoCapture File Options** dialog. To change the list order, highlight a list item and use the **Move Up** or **Move Down** buttons to move the item.

Using an AutoCapture file

To execute an AutoCapture, double-click on an AutoCapture (*.wac) file or specify the file on the command line. For example:

```
Peek.exe c:\temp\Poitiers.wac
```

When launched with an AutoCapture file as its object, AiroPeek will:

1. Establish a log file, if one is specified for the AutoCapture file.
2. Search the directory where the AutoCapture (*.wac) file is located, looking for a file of the same name but with the filter (*.flt) file extension. If it finds such a filter file in that directory, it will import it into the **Filters** window.

3. Run through the adapter search methods in the *Adapter search* section of the AutoCapture file to select a valid adapter. If multiple methods are enabled, they will be tried in the order specified, and the first successful selection will set the adapter. If no adapter is selected, AiroPeek will exit.

4. Create the Capture window(s) specified by the capture template(s), executing the *Adapter search* methods (if any) specified by each individual capture template. The adapter found by the methods specified in the *Adapter search* section of the AutoCapture file as a whole will become the fall-back or default adapter for each of these individual adapter searches.

5. Start capture or set the start/stop triggers for each Capture window.

6. Wait for all Capture windows to stop capturing.

Important! Be sure to enable the *Continuous capture* and *Save to disk* options and set a Stop Trigger for every capture template in the AutoCapture file. No files will be sent until capture is stopped in all Capture windows. Packets must be saved before they can be sent.

7. Run through the *Send options* to send or save any capture files. The first successful send option will be used to send all of the files.

8. Remove the sent or saved files if *Remove files after send completes* is selected for the Send Option used.

9. Exit AiroPeek.

AiroPeek can also be scheduled with the Windows Task Scheduler, available by choosing **Start** > **Settings** > **Control Panel** > **Scheduled Tasks**. The easiest way to use AiroPeek with an AutoCapture file as a scheduled task is to create a batch file (*.bat) with the desired command line, then schedule the batch file to run at a specified time in the Task Scheduler. For more about the command line, please see “Starting AiroPeek from the command line” on page 31.

Expert View and Expert ProblemFinder

Unique to AiroPeek NX, the ***Expert*** view provides expert analysis of delay, throughput and a wide variety of network problems in a conversation-centered view of traffic in a Capture window or Packet File window.

The Expert ProblemFinder scans traffic in a Capture window or Packet File window, looking for trouble. You can configure the Expert ProblemFinder to be as narrowly or as broadly focused as you like. The ProblemFinder's 113 separate diagnostics check for anomalies and sub-optimal performance at all layers of the network from application to physical. They monitor Client/Server delay and throughput as well.

You can enable and disable each diagnostic individually. In addition, many of the diagnostics have user-defined settings and thresholds, allowing you to fine-tune this Expert system to precisely fit your needs. You can save and reload Expert ProblemFinder settings for use in particular environments.

The ***Expert*** view provides aggregate ProblemFinder results, but it also provides a detailed view of every transaction, noting any problems encountered in each individual conversation or flow.

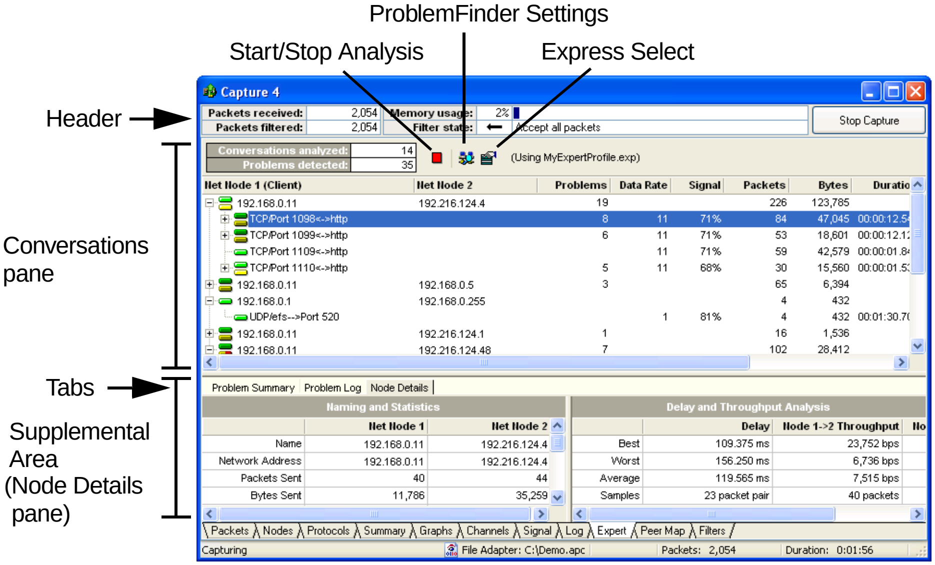
You can use the **Express Select** button to instantly highlight the packets associated with a particular problem, or with any conversation in the ***Expert*** view.

The Expert ProblemFinder not only helps identify problems, but it also helps you understand the meaning, the typical causes, and the typical solutions to the problems it uncovers. Detailed information is only a click away.

In this Chapter:

Expert view

The ***Expert*** view has a header section and two data areas: the Conversations pane of the ***Expert*** view above and a supplemental area below. The Conversations pane displays conversations or flows, nested under the address or name of the client node. The supplemental area can display one of three additional panes, accessible by clicking the labeled tabs. The tabs are: ***Problem Summary***, ***Problem Log***, and ***Node Details***. Each of these elements of the ***Expert*** view is described in turn below.



Packets received:	2,054	Memory usage:	2%
Packets filtered:	2,054	Filter state:	Accept all packets

Conversations analyzed:	14
Problems detected:	35

(Using MyExpertProfile.exp)

Net Node 1 (Client)	Net Node 2	Problems	Data Rate	Signal	Packets	Bytes	Duratio
192.168.0.11	192.216.124.4	19			226	123,785	
TCP/Port 1098<->http		8	11	71%	84	47,045	00:00:12.5
TCP/Port 1099<->http		6	11	71%	53	18,601	00:00:12.1
TCP/Port 1109<->http			11	71%	59	42,579	00:00:01.8
TCP/Port 1110<->http		5	11	68%	30	15,560	00:00:01.5
192.168.0.11	192.168.0.5	3			65	6,394	
192.168.0.1	192.168.0.255				4	432	
UDP/efs-->Port 520			1	81%	4	432	00:01:30.7
192.168.0.11	192.216.124.1	1			16	1,536	
192.168.0.11	192.216.124.48	7			102	28,412	

Naming and Statistics

	Net Node 1	Net Node 2
Name	192.168.0.11	192.216.124.4
Network Address	192.168.0.11	192.216.124.4
Packets Sent	40	44
Bytes Sent	11,786	35,259

Delay and Throughput Analysis

	Delay	Node 1->2 Throughput	No
Best	109.375 ms	23,752 bps	
Worst	156.250 ms	6,736 bps	
Average	119.565 ms	7,515 bps	
Samples	23 packet pair	40 packets	

Capturing | File Adapter: C:\Demo.apc | Packets: 2,054 | Duration: 0:01:56

Figure 5.1 AiroPeek NX Expert view, showing Node Details pane

Important! The ***Expert*** view and its ability to write to the ***Expert*** column of the ***Packets*** view must be enabled in the ***Analysis Modules*** view of the **Options** dialog in order to function. The ***Expert*** view is enabled by default. To open the ***Analysis Modules*** view, choose **Options…** from the **Tools** menu to open the **Options** dialog and click the *Analysis Modules* item in the navigation pane.

Expert view header

The header section of the ***Expert*** view shows the number of *Conversations Analyzed* and the *Problems Detected*. To the right of this information are three buttons: **Start/Stop**

Analysis, **ProblemFinder Settings**, and **Express Select**. The **Start/Stop Analysis** button displays as either a red square (click to stop) or a green arrow (click to start), depending on the current state of analysis. Click the **ProblemFinder Settings** button to open the **Expert ProblemFinder Settings** window, where you can configure the individual Expert diagnostics. Click the **Express Select** button to use the currently selected flow in the Conversations pane below as the basis for a **Select Related Packets** selection in the ***Packets*** view.

Expert view conversations pane

The Conversations pane of the ***Expert*** view shows the current conversations, with information about each conversation displayed in a user-definable set of columns. Right-click in the Conversations pane to open the context menu and choose **Visible columns…** to select the columns you wish to display. Use drag and drop to change column order. To use drag and drop, click on a column heading, then drag the ghost image of the column heading to a new location and release the mouse button. The columns available in the Conversations pane of the ***Expert*** view are shown in Table 5.1. Columns present in the default Conversations pane layout show an **X** in the **Default** column of Table 5.1.

Table 5.1 Expert view, conversations pane columns

Default	Column	Description
X	***Net Node 1 (Client)***	The client or first peer in the selected conversation.
X	***Net Node 2***	The server or second peer in the selected conversation.
X	***Problems***	Total number of problems identified by the Expert ProblemFinder. Note that count of problems is rolled up when the view is collapsed, such that higher levels of aggregations show totals for all sub-elements.
	Protocol	The protocol under which the packets in this conversation were exchanged.
	Hops	Number of hops separating the two end points of this conversation.

Table 5.1 Expert view, conversations pane columns (continued)

Default	Column	Description
	Channel	The channel reported in the packets making up this conversation. This is sometimes distinct from the channel on which the traffic was detected.
X	***Data Rate***	The data rate reported in the packets in this conversation.
X	***Signal***	The signal strength reported by the 802.11 WLAN NIC when this packet was captured.
X	***Packets***	The number of packets in the selected exchange. Note that packet totals are rolled up when the view is collapsed, such that higher levels of aggregations show totals for all sub-elements.
X	***Bytes***	The total bytes represented by the packets which were a part of the selected conversation.
X	***Duration***	The elapsed time, from the first to the last packet of the selected exchange, represented in the form Hours:Minutes:Seconds:Milliseconds.
X	***Avg Delay***	For exchanges in which this parameter is relevant, shows the arithmetic average of all client/server response times or of latencies for the selected pair of nodes.
X	***TCP Status***	For exchanges that represent TCP transactions, notes whether the session is *Open* or *Closed*.

The Conversations pane of the ***Expert*** view of a Capture window or Packet File window provides a hierarchical view of all conversations contained in the visible packets in the buffer of the window. Each highest-level item in the display represents a single node acting as the Client or first peer in a particular conversation. When a group of conversations differ only in port number, they are ranged below the Client node in order by port number. Any events diagnosed by the Expert ProblemFinder are shown in the next level of hierarchy below this one.

Note: The terms “conversation” or “flow” are equivalent, and have a precise meaning in the ***Expert*** view. For IP, the end-to-end IP address, and UDP or TCP ports form a unique conversation or flow for a given application. For IPX, the end-to-end IPX address, socket number, and connection IDs form a unique conversation or flow for a given application.

Important! In order to analyze and display conversations, AiroPeek NX interprets higher level protocol data, such as IP and IPX. If this data is unavailable (either because packet slice values were set too low or because traffic is encrypted and AiroPeek NX does not have the correct WEP keys to decrypt the data portion of the packets), then no conversations will appear in the Conversations pane. The ***Expert*** view can diagnose a range of potential security and performance problems regardless of encryption. These diagnoses are shown in the supplemental information panes, below the Conversations pane.

Items in the Conversations pane are color coded for easy scanning. When a conversation is still active, the color block beside that item is bright green. When the conversation is completed, the color block is dull green. When a problem has been identified as being associated with that particular conversation, a yellow color block appears beside the Client node. If some of the problems identified are classified as Major or Severe, the block will show part red and part yellow. If all of the problems are Major or Severe, the whole block will be red.

Click on the **+** (plus) or **-** (minus) signs at the left margin to expand or collapse individual elements of the display. Alternatively, you can right-click anywhere in the Conversations pane to open the context menu and choose either **Expand All** or **Collapse All**.

Forcing server identification

The Expert makes its best attempt to determine which node is the client and which the server in each conversation. You can override this behavior by making entries in the Name Table telling the ***Expert*** view to always identify certain nodes as the server, regardless of the context. If a node is identified in the ***Expert*** view as a client and you wish to have that IP address always treated as a server, you can make an entry in the Name Table as follows:

1. In the Conversations pane of the ***Expert*** view, right-click on the conversation in which the node is identified as a client and choose **Insert Net Node 1 into Name Table…** from the context menu.
2. In the **Add Name** or **Edit Name** dialog which appears, accept the other entries, but set the *Node type* entry to *Server* by choosing from the drop-down list.
3. Click **OK** to make the change to the Name Table.

4. The Expert checks the Name Table to identify nodes, and your changes will be reflected in subsequent captures or on re-reading this captured file or doing post capture analysis.

   When you designate a node as a *Server* in the Name Table, all connections to that IP address will identify this address as a server, regardless of other contextual clues. To once again allow the Expert to determine from context whether this node is acting as the client or server, delete the node's entry from the Name Table or change its *Node type* to *Workstation* or *Unknown*.

Expert view supplemental information panes

The supplemental information area at the bottom of the ***Expert*** view provides summary counts of problems and additional detail about the problems and the participants in the conversations shown in the Conversations pane above it. The supplemental information area can show one of three panes, accessible by clicking on the labeled tabs.

The panes, and the data tables they contain, are:

Problem Summary	***Problem Log***	***Node Details***	
Problem Summary table	*Problem Log*	*Naming and Statistics* table	*Delay and Throughput Analysis* table

Problem summary pane

The Problem Summary pane contains the *Problem Summary* table, showing the number of times each type of problem was encountered. The header area of the Problem Summary pane shows the *Total* number of problems identified. The *Problem Summary* table has four columns, as shown in Table 5.2. You can sort by any column by clicking in the column header. An arrow shows the direction of the sort for the column.

Table 5.2 **Problem Summary columns**

Column	Description
Severity Icon	The severity of the event, as set in the **Expert ProblemFinder Settings** window.
Layer	The network layer to which events of this type belong.
Event	The ProblemFinder problem event diagnosis which identified this packet as a problem (for example, *TCP Transport Retransmission*).
Count	The number of events of this type seen so far.

Right-click on any item in the *Problem Summary* and choose **ProblemFinder Setting** from the context menu to open the **Expert ProblemFinder Settings** window with that particular event highlighted and its setting displayed. The **Expert ProblemFinder Settings** window shows a description of the problem and a brief discussion of possible causes and possible remedies.

The context menu also allows you to save the *Problem Summary* table, or individual lines from it, to a text file, or to copy them to the clipboard.

When you highlight a type of event in the *Problem Summary* which is associated with conversations, the related conversations or flows in the Conversations pane are highlighted. From the *Problem Summary* table, you can also choose **Select Related Packets** > **By Problem Type** from the context menu (right click).

Tip To see a list of all the individual instances of a problem of a given type, switch to the Problem Log pane and sort the *Problem Log* by its ***Event*** column. You can then scroll to find the problem of the specific type.

Problem log pane

The Problem Log pane (shown in Figure 5.2) contains the *Problem Log*. The *Problem Log* has a header area, and a table.

The header area of the Problem Log pane shows a count of total *Entries* in the log, and counts of problems classified by their level of severity. The counts by level of severity are shown beside the icon for each level of severity. In order from left to right, these are: Informational, Minor, Major, and Severe. Click on these icons to toggle the display of problems in the table below. The counts will continue to update, even if you choose not to display problems of a particular severity.

The *Problem Log* table shows the individual packets which generated a problem notice, based on the settings in the **Expert ProblemFinder Settings** window. It shows one packet per line. The *Problem Log* presents information for each packet in the columns shown in Table 5.3. You can sort the *Problem Log* by any column by clicking in the column header. A triangle in the column header shows the order of the sort, ascending or descending. Click again to change the sort order.

Table 5.3 Problem Log columns

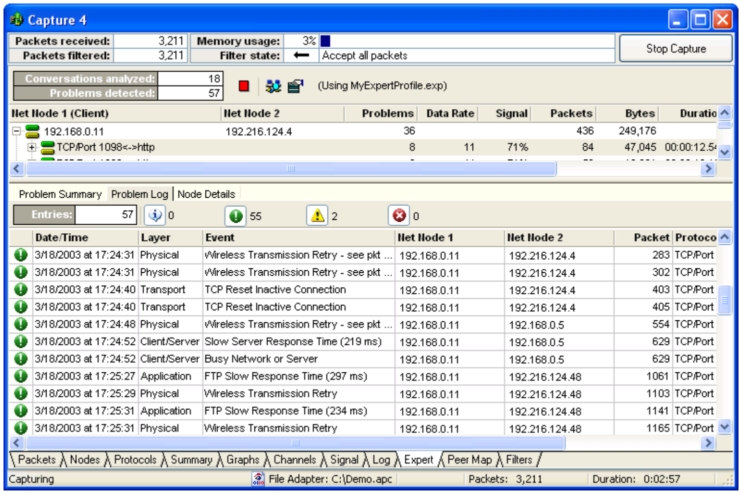
Column	Description
Severity Icon	The severity of the problem, as set in the **Expert ProblemFinder Settings** window.
Date/Time	The date and time of capture for the packet, shown to the nearest whole second.
Layer	The network layer to which events of this type belong.
Event	The ProblemFinder problem event diagnosis which identified this packet as a problem (for example, *TCP Transport Retransmission*). The description may be modified to show additional information. For example, a packet which was identified as a problem by the Expert ProblemFinder item called *TCP Reset Connection* might have an entry in the ***Event*** column of the *Problem Log* such as *TCP Connection Reset by Client*. For packets identified by Expert ProblemFinder items having a user-definable *Setting* value, the description may be followed by the actual measurement which identified this packet as having a problem (for example *Low Server-to-Client Throughput (1,850 bps)*).
Net Node 1	The client in the transaction or the initiating node in a peer to peer conversation. The node is identified by its logical address or by the symbolic name for that address if one exists in the Name Table.

Table 5.3 **Problem Log columns (continued)**

Column	Description
Net Node 2	The server or second peer in the transaction. The node is identified by its logical address or by the symbolic name for that address if one exists in the Name Table.
Packet	The packet number, as assigned in the ***Packets*** view of the Capture window or Packet File window. These numbers are assigned in sequence as the packets are captured into the buffer.
Protocol/App	The protocol and application represented by this packet. If the port used is other than the standard port for the application (or if there is no standard port), then port information is also shown. For example, *ICMP Echo (Ping) Reply* or *TCP/Port 10117<->Port 5003*.

Click on an entry in the *Problem Log* to display and highlight that same problem in the Conversations pane. If the display of the Conversations pane is collapsed, clicking on a *Problem Log* entry will expand the correct part of the Conversations pane to show the selected problem.

Note: If the entry in the *Problem Log* does not apply to any particular conversation, there will be no conversation to highlight. For example, *Wireless Channel Overlap* is a problem that is not associated with a particular conversation.



Packets received: 3,211
Packets filtered: 3,211
Memory usage: 3%
Filter state: Accept all packets

Conversations analyzed: 18
Problems detected: 57
(Using MyExpertProfile.exp)

Net Node 1 (Client)	Net Node 2	Problems	Data Rate	Signal	Packets	Bytes	Duratio
192.168.0.11	192.216.124.4	36			436	249,176	
TCP/Port 1098<->http		8	11	71%	84	47,045	00:00:12.5

Entries: 57 0 55 2 0

Date/Time	Layer	Event	Net Node 1	Net Node 2	Packet	Protoco
3/18/2003 at 17:24:31	Physical	Wireless Transmission Retry - see pkt ...	192.168.0.11	192.216.124.4	283	TCP/Port
3/18/2003 at 17:24:31	Physical	Wireless Transmission Retry - see pkt ...	192.168.0.11	192.216.124.4	302	TCP/Port
3/18/2003 at 17:24:40	Transport	TCP Reset Inactive Connection	192.168.0.11	192.216.124.4	403	TCP/Port
3/18/2003 at 17:24:40	Transport	TCP Reset Inactive Connection	192.168.0.11	192.216.124.4	405	TCP/Port
3/18/2003 at 17:24:48	Physical	Wireless Transmission Retry - see pkt ...	192.168.0.11	192.168.0.5	554	TCP/Port
3/18/2003 at 17:24:52	Client/Server	Slow Server Response Time (219 ms)	192.168.0.11	192.168.0.5	629	TCP/Port
3/18/2003 at 17:24:52	Client/Server	Busy Network or Server	192.168.0.11	192.168.0.5	629	TCP/Port
3/18/2003 at 17:25:27	Application	FTP Slow Response Time (297 ms)	192.168.0.11	192.216.124.48	1061	TCP/Port
3/18/2003 at 17:25:29	Physical	Wireless Transmission Retry	192.168.0.11	192.216.124.48	1103	TCP/Port
3/18/2003 at 17:25:31	Application	FTP Slow Response Time (234 ms)	192.168.0.11	192.216.124.48	1141	TCP/Port
3/18/2003 at 17:25:31	Physical	Wireless Transmission Retry	192.168.0.11	192.216.124.48	1165	TCP/Port

Capturing File Adapter: C:\Demo.apc Packets: 3,211 Duration: 0:02:57

Figure 5.2 AiroPeek NX Expert view, showing Problem Log pane

When one or more log entries are highlighted, you can use the context menu to **Select Related Packets** in a number of different ways by choosing from the sub-menu. These methods and their results are described in Table 5.4.

Table 5.4 Select Related Packets in the Expert Problem Log

Parameter	Action
By Source and Destination	Chooses packets with matching source and destination addresses.
By Conversation	Chooses packets sent between two nodes (in either direction), using the matching protocol and port.

Table 5.4 Select Related Packets in the Expert Problem Log (continued)

Parameter	Action
Selected Entries	Chooses only the individual packet identified with each highlighted entry in the Problem Log. The Problem Log shows one packet with one problem in each log entry. Multiple log entries may be highlighted at once.
Selected Entries + "See" or "From Pkt"	Chooses the individual packet identified with each highlighted entry in the Problem Log, plus any packet referred to in the log entry in a phrase which begins "*See Packet…*" or "*From Packet….*" These log entries refer to another packet in the same conversation, such as a response or request packet, for example.

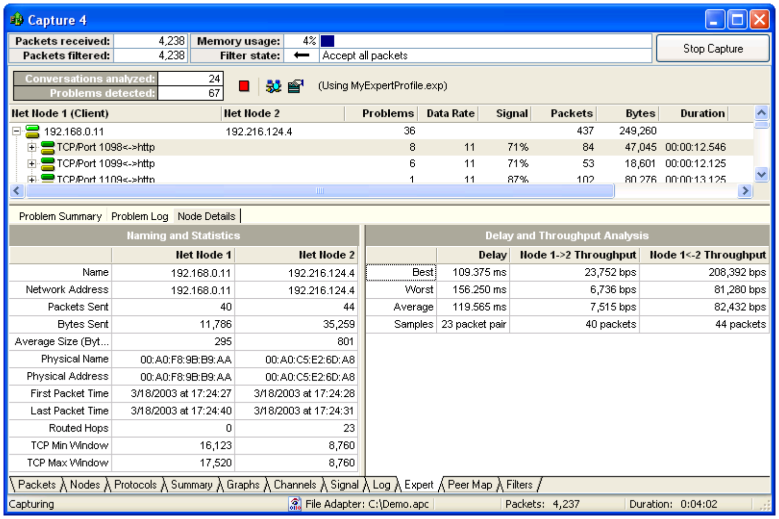
Right-click on any item in the *Problem Log* and choose **ProblemFinder Setting** from the context menu to open the **Expert ProblemFinder Settings** window with the diagnostic for that particular problem highlighted and its setting displayed. The **Expert ProblemFinder Settings** window shows a description of the problem event and a brief discussion of possible causes and possible remedies.

The context menu also allows you to save the *Problem Log* or individual lines from it to a text file, or to copy either the whole log or selected items to the clipboard.

Node details pane

The Node Details pane (shown in Figure 5.3) contains two tables:

- the *Naming and Statistics* table (on the left)
- the *Delay and Throughput Analysis* table (on the right)



Packets received: 4,238
Packets filtered: 4,238
Memory usage: 4%
Filter state: Accept all packets

Conversations analyzed: 24
Problems detected: 67
(Using MyExpertProfile.exp)

Net Node 1 (Client)	Net Node 2	Problems	Data Rate	Signal	Packets	Bytes	Duration
192.168.0.11	192.216.124.4	36			437	249,260	
TCP/Port 1098<->http		8	11	71%	84	47,045	00:00:12.546
TCP/Port 1099<->http		6	11	71%	53	18,601	00:00:12.125
TCP/Port 1109<->http		1	11	87%	102	80,276	00:00:13.125

Naming and Statistics

	Net Node 1	Net Node 2
Name	192.168.0.11	192.216.124.4
Network Address	192.168.0.11	192.216.124.4
Packets Sent	40	44
Bytes Sent	11,786	35,259
Average Size (Byt...	295	801
Physical Name	00:A0:F8:9B:B9:AA	00:A0:C5:E2:6D:A8
Physical Address	00:A0:F8:9B:B9:AA	00:A0:C5:E2:6D:A8
First Packet Time	3/18/2003 at 17:24:27	3/18/2003 at 17:24:28
Last Packet Time	3/18/2003 at 17:24:40	3/18/2003 at 17:24:31
Routed Hops	0	23
TCP Min Window	16,123	8,760
TCP Max Window	17,520	8,760

Delay and Throughput Analysis

	Delay	Node 1->2 Throughput	Node 1<-2 Throughput
Best	109.375 ms	23,752 bps	208,392 bps
Worst	156.250 ms	6,736 bps	81,280 bps
Average	119.565 ms	7,515 bps	82,432 bps
Samples	23 packet pair	40 packets	44 packets

Capturing | File Adapter: C:\Demo.apc | Packets: 4,237 | Duration: 0:04:02

Figure 5.3 AiroPeek NX Expert view, showing Node Details pane

Note: Unlike the Problem Summary and the Problem Log panes, the information in the Node Details pane applies only to the currently selected conversation or flow, or to the item currently selected in the Conversations pane of the ***Expert*** view.

The *Naming and Statistics* table shows additional details for the participants in the selected conversation, identified as ***Net Node 1*** and ***Net Node 2***. The *Naming and Statistics* table shows the characteristics described in Table 5.5 for both Net Node 1 and Net Node 2.

Table 5.5 Naming and Statistics table parameters

Parameter	Description
Name	The name (or address) of each node. The node is identified by its logical address or by the symbolic name for that address if one exists in the Name Table.
Address	The logical address, in a format appropriate to the protocol of the conversation.

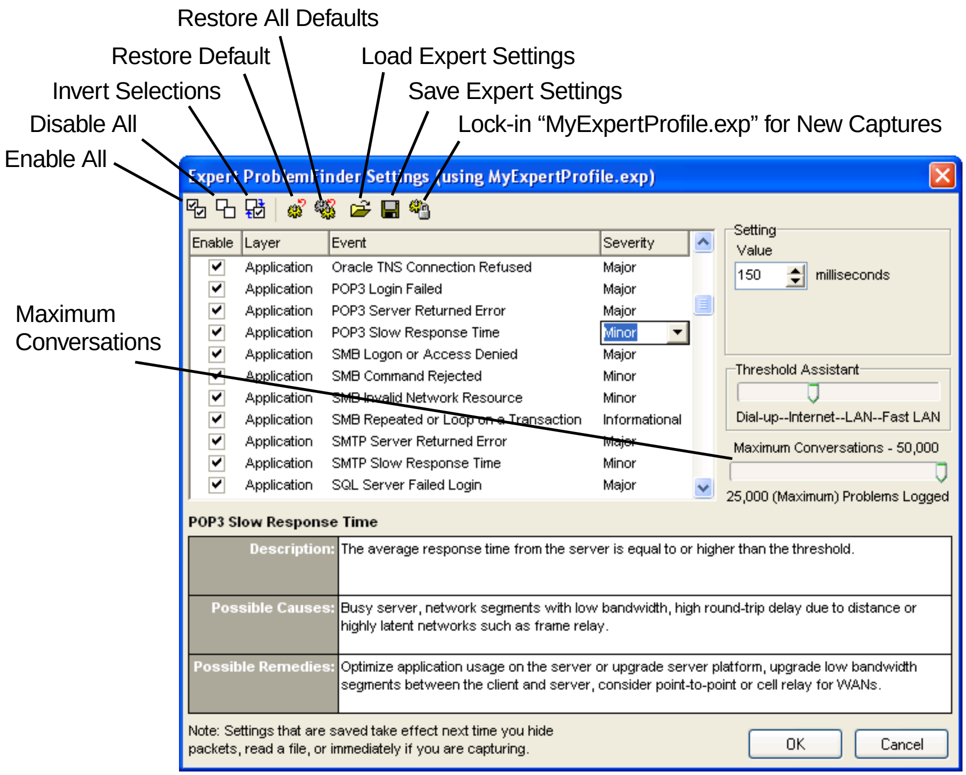
Table 5.5 **Naming and Statistics table parameters (continued)**

Parameter	Description
Packets Sent	The total number of packets sent by this node as a part of this conversation.
Bytes Sent	The total number of bytes sent by this node as a part of this conversation.
Average Size	The average size of the packets sent by this node as a part of this conversation, in bytes.
Physical Name	The name (if any) associated with the physical address of this node. An example might be a WINS or NetBIOS name. If no such name is discovered in the traffic itself or found in the Name Table, the MAC address of the node will appear here.
Physical Address	The physical address of the node. Its MAC address.
First Packet Time	The date and time of capture (to the nearest second) of the first packet for this node in the current conversation.
Last Packet Time	The date and time of capture (to the nearest second) of the last packet for this node in the current conversation.
Routed Hops	The number of intervening router hops separating Net Node 1 and Net Node 2 in this conversation.
TCP Min Window	The minimum size of the TCP window during the course of this conversation.
TCP Max Window	The maximum size of the TCP window during the course of this conversation.

The *Delay and Throughput Analysis* table shows the *Best*, *Worst*, and *Average* measures of delay and throughput for the selected conversation, along with the number of *Samples* on which these figures are based. The table shows data in three columns: ***Delay*** (server response time, network latency, and so forth), ***Node 1->Node 2 Throughput*** (peer one to peer two, or client to server throughput), and ***Node 1<-Node 2 Throughput*** (peer two to peer one, or server to client throughput). Delay is shown in milliseconds. To set the units for throughput, choose **Throughput** from the context menu (right-click) and select one of the three sub-menu choices: **Bits/Second (bps)**, **kBits/Second (kbps)**, or **kBytes/Second (kBps)**. The current choice has a dot beside it.

Expert ProblemFinder

The **Expert ProblemFinder Settings** window lets you enable or disable any of the 113 Expert ProblemFinder diagnostics individually or all together. Many of these diagnostics have user definable settings which can be customized to match particular tasks or environments. Where settings are related to network bandwidth, the *Threshold Assistant* can help you choose the best setting. In addition, the **Expert ProblemFinder Settings** window shows the *Description*, *Possible Causes*, and *Possible Remedies* for each problem it can diagnose.



Enable	Layer	Event	Severity
☑	Application	Oracle TNS Connection Refused	Major
☑	Application	POP3 Login Failed	Major
☑	Application	POP3 Server Returned Error	Major
☑	Application	POP3 Slow Response Time	Minor
☑	Application	SMB Logon or Access Denied	Major
☑	Application	SMB Command Rejected	Minor
☑	Application	SMB Invalid Network Resource	Minor
☑	Application	SMB Repeated or Loop on a Transaction	Informational
☑	Application	SMTP Server Returned Error	Major
☑	Application	SMTP Slow Response Time	Minor
☑	Application	SQL Server Failed Login	Major

Setting

Value 150 milliseconds

Threshold Assistant

Dial-up--Internet--LAN--Fast LAN

Maximum Conversations - 50,000

25,000 (Maximum) Problems Logged

POP3 Slow Response Time

Description:	The average response time from the server is equal to or higher than the threshold.
Possible Causes:	Busy server, network segments with low bandwidth, high round-trip delay due to distance or highly latent networks such as frame relay.
Possible Remedies:	Optimize application usage on the server or upgrade server platform, upgrade low bandwidth segments between the client and server, consider point-to-point or cell relay for WANs.

Note: Settings that are saved take effect next time you hide packets, read a file, or immediately if you are capturing.

Figure 5.4 AiroPeek NX Expert ProblemFinder Settings window

Configuring expert diagnostics

The **Expert ProblemFinder Settings** window shows all of the available diagnostics in a table in the upper left of the window. When you select an item in this table, the rest of the window changes to display the relevant characteristics for that item, including the descriptive and troubleshooting information and any settings. The table has four columns: ***Enable***, ***Layer***, ***Event***, and ***Severity***.

Check the checkbox in the ***Enable*** column to enable the diagnostic. You can also use the buttons at the top of the window to globally **Enable All** or **Disable All** diagnostics at once. To reverse the state of all diagnostics, enabling those currently disabled and disabling those currently enabled, click the **Invert Selections** button.

The ***Layer*** column groups the diagnostics into classes according to the type of traffic they examine. These layers are based on the OSI seven-layer model of networking. From top (closest to user interaction) to bottom (closest to the electrical impulses), the seven layers used by the Expert are: *Client/Server, Application*, *Session*, *Transport*, *Network*, *Data Link*, and *Physical*.

The ***Event*** column shows the name of the diagnostic, expressed as a short description of the type of network problem event for which it tests.

The ***Severity*** column shows the level of severity of notification this item will send when it encounters a matching problem event. Click on the entry in the ***Severity*** column for any diagnostic to open a drop-down list where you can set the level of severity of these notifications. For more on notifications and their levels of severity, please see "Notifications" on page 248.

Tip Click in any column heading to sort the display by that column. An arrow appears in the header of the column by which you have sorted the display, indicating the sort order. Click again to toggle the sort order between ascending and descending.

Diagnostic settings

The *Setting* area to the right of the diagnostic table shows the *Value* and units that mark the threshold of the problem condition for the selected diagnostic item. In Figure 5.4, for example, the selected diagnostic, *POP3 Slow Response Time*, shows a *Setting Value* of *150 milliseconds*. When this diagnostic item is enabled, it will diagnose any POP3 response time greater than 150 milliseconds as a problem. Note that not all diagnostics require a setting value. Some, such as *NCP Server Busy Reply*, simply check for a particular event or packet type.

Threshold assistant

Many ProblemFinder diagnostics look at characteristics of network traffic that can be expected to vary with network bandwidth. The Threshold Assistant helps you choose the right settings for these diagnostics in an intuitive way. In the example in Figure 5.4, the *Setting* for *POP3 Slow Response Time* is set to *150 milliseconds*. The *Threshold Assistant* slider bar is aligned under the *Internet* marker, and the setting value of 150 milliseconds is appropriate for POP3 connections over the Internet. If you move the slider bar to the left, the setting value increases, allowing for the slower POP3 response times that you would expect over, for example, a *Dial-up* connection. If you move the slider bar to the right, the *Value* decreases, reflecting the faster POP3 response times you would expect over a *LAN* or, further to the right, a *Fast LAN*. You can, of course, make changes to settings independent of the Threshold Assistant, but it often provides the quickest way to align several related diagnostics for optimum sensitivity and test accuracy.

Maximum conversations - expert resource limits

You can set an upper limit on the system resources (such as memory) available to Expert Analysis functions by using the *Maximum Conversations* slider bar, which appears in the *Setting* section of any ProblemFinder diagnostic item. When the maximum number of conversations is reached, the Expert will stop processing packets.

Note: Setting *Maximum Conversations* to a high value does not reserve resources, but the more conversations the Expert analyzes, the more memory is required. If you set high limits and those limits are reached, it may affect the performance of AiroPeek NX or of other open applications.

By default, *Maximum Conversations* is set at a level calculated to permit continued smooth operation, even when the maximums are repeatedly reached.

Move the *Maximum Conversations* slider bar to the left for fewer resources or to the right for more. Above and below the slider bar, respectively, you will see the *Maximum Conversations (number)* and the *(number) (Maximum) Problems Logged* which the chosen resource level will permit. The *Maximum Conversations* slider bar sets the limits for all instances of the Expert Analysis function globally.

Restoring defaults and accepting changes

To restore the default setting values for an individual diagnostic item, select that diagnostic in the table and click the **Restore Default** button at the top of the **Expert**

ProblemFinder Settings window. To restore the default values to all the diagnostic items, click the **Restore All Defaults** button.

You can also save and restore the entire collection of Expert ProblemFinder settings. To save the current Expert ProblemFinder settings under a new name for future use, click the Save Expert Settings button at the top of the window. This opens a Save As dialog in which you can name and choose a location for the saved settings file with its *.exp extension. To restore a previously saved group of settings, click the Load Expert Settings button at the top of the display. This opens a file Open dialog in which you can navigate to the location of and choose a settings file with a *.exp extension. You can load an alternative Expert ProblemFinder settings file and still use the default expert settings for all new Capture windows. Click the **Lock-in "MyExpertProfile.exp" for New Captures** button.

When you have made your changes to items in the **Expert ProblemFinder Settings** window, click the **OK** button to accept, or the **Cancel** button to reject your changes and close the window.

Peer Map

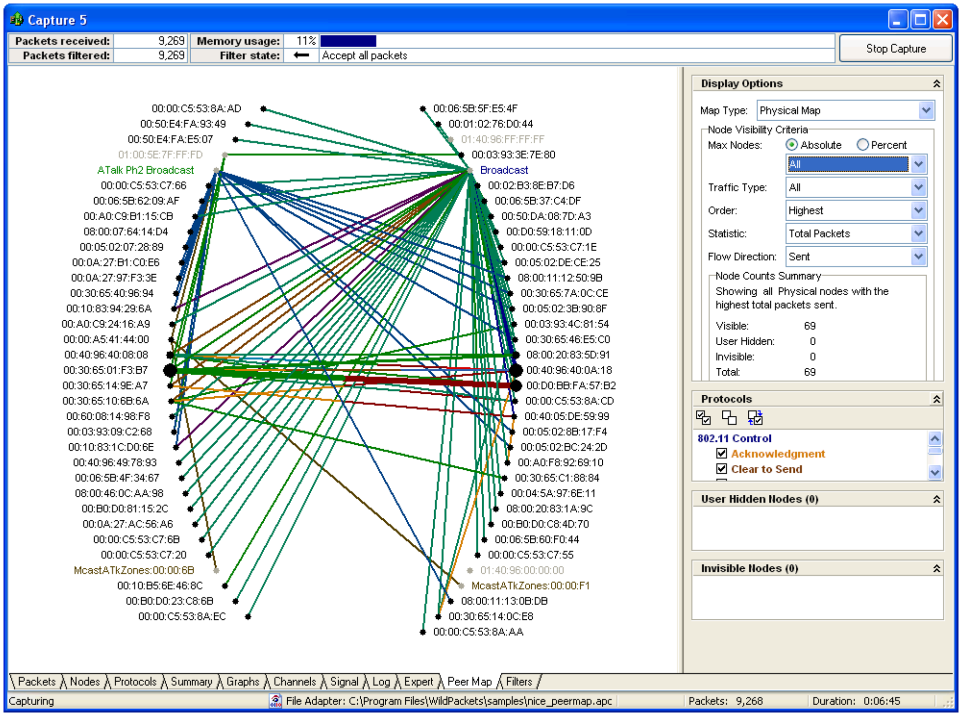
Unique to AiroPeek NX, the ***Peer Map*** view is a powerful tool for visualizing network traffic in a Packet File window or Capture window. The Peer Map uses line weight to show the volume of traffic between nodes, and uses line color to show the protocol in use between nodes. The nodes themselves can be color-coded and show icons for node type, based on Name Table data.

The ***Peer Map*** view contains its own tools to control the display of nodes and types of network traffic. This lets you quickly create a picture of all the traffic that is using a particular protocol, for example, or all the nodes sending or receiving multicast traffic.

The Peer Map displays the nodes around an elongated ellipse. Communications are shown by a line connecting each two peers. The color of the line denotes the protocol. The thickness of the line denotes the volume of traffic. When you drag nodes to new positions, the lines rubber-band.

Nodes are labeled with their physical or logical address, depending on the layer you choose to view. You can optionally show nodes with their symbolic names and/or use icons to represent node types stored in the Name Table.

In this Chapter:



Packets received: 9,269
Packets filtered: 9,269
Memory usage: 11%
Filter state: Accept all packets

Display Options

Map Type: Physical Map

Node Visibility Criteria

Max Nodes: ● Absolute ○ Percent

All

Traffic Type: All

Order: Highest

Statistic: Total Packets

Flow Direction: Sent

Node Counts Summary

Showing all Physical nodes with the highest total packets sent.

Visible: 69
User Hidden: 0
Invisible: 0
Total: 69

Protocols

802.11 Control

☑ Acknowledgment

☑ Clear to Send

User Hidden Nodes (0)

Invisible Nodes (0)

Capturing | File Adapter: C:\Program Files\WildPackets\samples\nice_peermap.apc | Packets: 9,268 | Duration: 0:06:45

Figure 6.1 Peer Map view of an AiroPeek NX Capture window

The ***Peer Map*** view shows the Peer Map itself on the left and a series of panes on the right used to control the display of the Peer Map. The panes on the right, from top to bottom, are: *Display Options*, *Protocols*, *User Hidden Nodes*, and *Invisible Nodes*. You can collapse or expand the view of any of these panes by clicking the chevron (the double arrow) in the upper right-hand corner of the pane. You can also drag the edges of the whole area, or drag the bottom edge of any pane to resize. Each of the panes with its features and functions is described below.

Display options pane

The *Display Options* pane sets the basic parameters of the Peer Map. The *Map Type* drop-down list lets you choose whether to display nodes as a *Physical Map* (containing only physical addresses), an *IP Map* (containing only IP addresses), or an *IPX Map* (containing only IPX addresses). Note that the *Map Type* also limits the protocols which can be displayed, and changes the options in the *Protocols* pane as well. For example, choosing *IPX Address* in the *Map Type* drop-down list will display only the nodes, traffic and protocols using IPX.

The *Node Visibility Criteria* section contains drop-down lists and checkboxes controlling what part of the traffic in the window's buffer will be displayed in the Peer Map. The drop-down lists can be thought of as creating a simple description of the nodes to be displayed. In fact, such a description appears at the top of the *Node Counts Summary* section, immediately below the drop-down lists. You may see descriptions such as *Showing up to 50 unicasting IP addresses with the highest total bytes received*. The *Node Counts Summary* section also shows the number of nodes in the current view which are *Visible*, *User Hidden*, or *Invisible*, and gives the *Total*.

The *Max Nodes* text entry box lets you limit the display to no more than the specified number of nodes, expressed as an *Absolute* number or as a *Percent* of all nodes included in the Map Type for this buffer. The other parts of the *Node Visibility Criteria* section determine whether these are the nodes with the highest or the lowest values, and what aspects of network traffic to use as the test for inclusion.

The *Traffic Type* drop-down list lets you choose whether to show *All* nodes matching the other criteria, only those sending or receiving *Unicast* traffic, only those involved in *Multicast* traffic, only nodes with *Broadcast* traffic, or those with both *Multi- & Broadcast* traffic. When you choose any value other than *All* from the *Traffic* drop-down list, the nodes removed from the Peer Map are listed in a separate pane at the lower right of the ***Peer Map*** view called *Invisible Nodes*. If you choose *Multicast* from the *Traffic* drop-down list, for example, this pane will contain a list of all the nodes which neither sent nor received multicast traffic. That is, the *Invisible Nodes* section will include all nodes which sent or received only broadcast, unicast, or a combination of the two.

The *Order* drop-down list lets you choose whether you want the *Max Nodes* to represent the *Highest* or the *Lowest* values in the sample.

The *Statistic* drop-down list lets you choose the units to use when evaluating the *Max Nodes* and *Order* criteria, set above. You can choose to evaluate nodes based on their *Total Packets* or *Total Bytes*.

The last item in the *Node Visibility Criteria* section, the *Flow Direction* drop-down list, lets you choose whether to count the bytes or packets *Sent*, or those *Received*.

The three checkboxes in the *Node Appearance* area control the way in which nodes are displayed in the Peer Map. These choices are enabled when checked and disabled when unchecked.

Show Names replaces physical or logical addresses with symbolic names found in the Name Table.

Show Type Icons adds the icon appropriate to that node type (workstation, router, and so forth) to the display of any node that has a Type listed for it in the Name Table.

Use Colors uses Name Table entries to color code node names and addresses.

Protocols pane

The *Protocols* pane controls the display of the lines between the various peers in the Peer Map, which represent traffic in a particular protocol.

The *Protocols* pane shows a hierarchical list of protocols found in the Peer Map which use the address type chosen in the *Map Type* drop-down list in the *Display Options* pane above. Each of the protocols and sub-protocols has a checkbox beside it which lets you enable and disable the display of traffic in each protocol or sub-protocol independently. Each protocol has a color associated with it in ProtoSpecs. Both the entry in the *Protocols* pane and the traffic lines in the Peer Map use the same ProtoSpecs-assigned color to display each particular protocol.

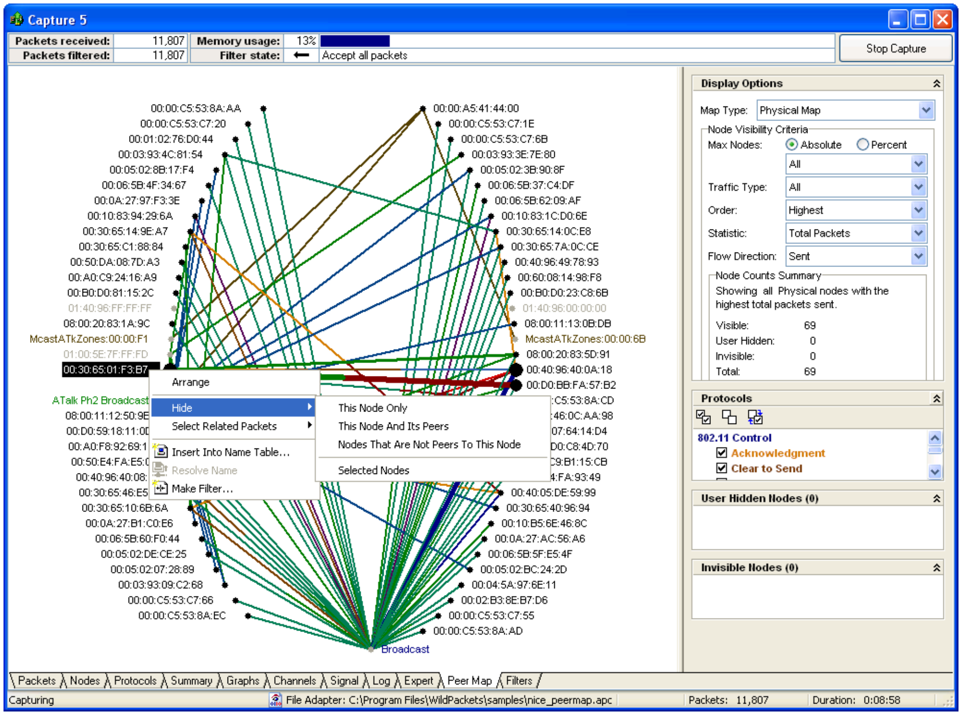
At the top of the *Protocols* pane are three buttons: **All On**, **All Off**, and **Invert All**. Click the **All On** button to enable the display of all protocols. Click the **All Off** button to disable the display of all protocols. Click the **Invert All** button to reverse the current enable/disable choices, enabling any that were disabled and disabling any that were enabled.

Note: Some traffic, while clearly belonging to a particular network protocol such as IP, may not be assigned a sub-protocol under ProtoSpecs. When traffic of this type is present, the *Protocols* hierarchy will show an item called *Other* which includes all such sub-protocols.

User hidden nodes pane

You can temporarily remove individual nodes from the Peer Map by hiding them. The *User Hidden Nodes* pane shows a list of nodes you have removed. The number of hidden nodes is shown in the header of this pane in parentheses. From this pane, you can restore the selected (highlighted) nodes to the Peer Map by right-clicking in the pane and choosing **Show Selected Nodes** from the context menu, or restore all the hidden nodes by choosing **Show All Nodes**.

There are several ways to hide nodes. You can select one or more nodes and drag them to the *User Hidden Nodes* pane. Alternatively you can highlight one or more nodes and right-click to bring up the context menu. From the context menu, you can choose **Hide** and make a choice from the submenu, as shown in Figure 6.2. The submenu gives you the option to hide only the named node, to hide the named node and all its peers, to hide only nodes which are *not* peers of the named node, or to hide only the selected nodes.



Capture 5

Packets received: 11,807 | Memory usage: 13%
Packets filtered: 11,807 | Filter state: Accept all packets

Display Options

Map Type: Physical Map

Node Visibility Criteria
Max Nodes: ● Absolute ○ Percent
All
Traffic Type: All
Order: Highest
Statistic: Total Packets
Flow Direction: Sent

Node Counts Summary
Showing all Physical nodes with the highest total packets sent.
Visible: 69
User Hidden: 0
Invisible: 0
Total: 69

Protocols
802.11 Control
☑ Acknowledgment
☑ Clear to Send

User Hidden Nodes (0)

Invisible Nodes (0)

Capturing | File Adapter: C:\Program Files\WildPackets\samples\nice_peermap.apc | Packets: 11,807 | Duration: 0:08:58

Figure 6.2 AiroPeek NX Peer Map view showing Hide context menu submenu choices

Note: When more than one node is selected, only the node from which the context menu was invoked is named in the **Hide** submenu. That is, only the node over which the cursor was positioned when the right-click was made can be used as the basis for hiding …**Peers** or …**Not Peers**. Alternatively, you can choose **Hide All Nodes** from the background context menu. Right click in the open area, away from all nodes, to open the background context menu. The Peer Map background context menu allows you to **Hide All Nodes**, **Arrange All Nodes**, **Resolve Names for All Nodes** (when available), or to copy the Peer Map to the clipboard.

Invisible nodes pane

The *Invisible Nodes* pane lists the nodes which have been temporarily hidden or removed from the Peer Map because they do not match the settings in the *Display Options* pane. Unlike the *User Hidden Nodes*, you cannot restore these nodes directly from the *Invisible Nodes* display. The header of the *Invisible Nodes* pane shows the number of invisible nodes in parentheses.

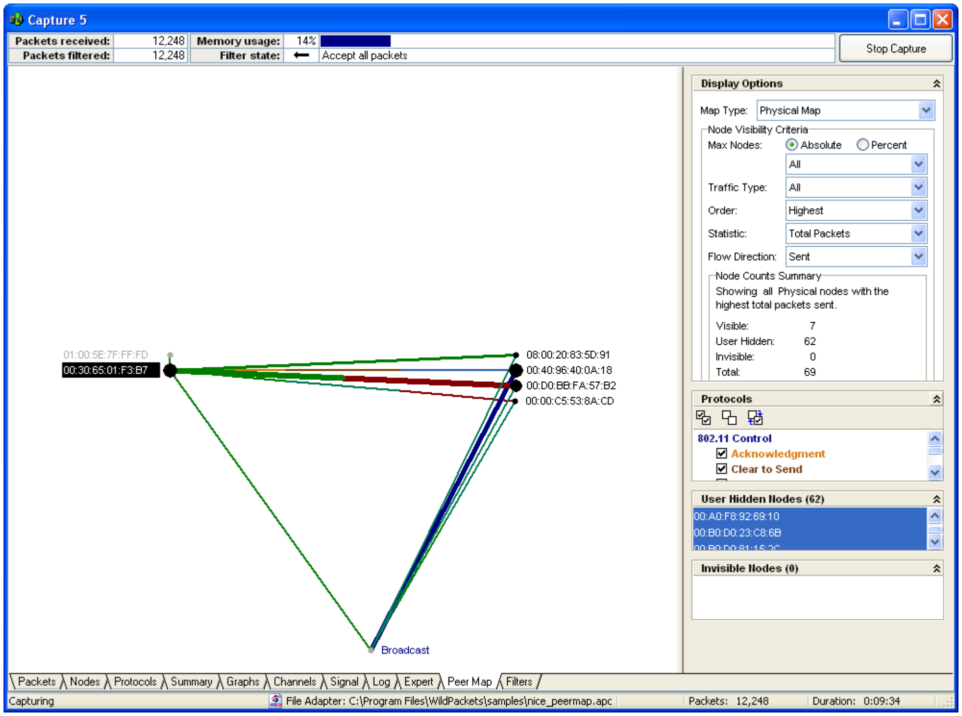
Using the peer map

The Peer Map is based on all the visible packets in the buffer of the Capture window or Packet File window, as further modified by the controls within the ***Peer Map*** view itself.

The tools for hiding and unhiding nodes described above in this chapter are particular to the Peer Map and have no effect on the ***Packets*** view or any of the other views.

Because the Peer Map reflects only the packets visible in the ***Packets*** view, you may also find it useful to switch back and forth between the ***Peer Map*** view and other views, hiding and unhiding packets to refine your picture of network traffic. When you right-click on a node in the Peer Map, the context menu allows you to **Select Related Packets**, using the current node **as Source**, **as Destination**, or **as Source or Destination**. These selection results are shown in the ***Packets*** view, as with any other Select Related operation.

Each dot on the Peer Map represents a particular node. The size of the dot represents the packets sent from that node, as a percentage of total packets in the window. The lines between nodes represent the traffic between them. The color of the line represents the protocol. This matches the color shown for each protocol in the *Protocols* pane at the right of the ***Peer Map*** view. The thickness of the line represents the volume of the traffic. Specifically, the thickness of the line represents the volume in bytes of the traffic between two nodes, expressed as a percent of all the traffic in the buffer.



Capture 5

Packets received: 12,248 Memory usage: 14%
Packets filtered: 12,248 Filter state: Accept all packets

Display Options

Map Type: Physical Map

Node Visibility Criteria

Max Nodes: ● Absolute ○ Percent

All

Traffic Type: All

Order: Highest

Statistic: Total Packets

Flow Direction: Sent

Node Counts Summary

Showing all Physical nodes with the highest total packets sent.

Visible:	7
User Hidden:	62
Invisible:	0
Total:	69

Protocols

802.11 Control
☑ Acknowledgment
☑ Clear to Send

User Hidden Nodes (62)

00:A0:F8:92:69:10
00:B0:D0:23:C8:6B

Invisible Nodes (0)

Capturing File Adapter: C:\Program Files\WildPackets\samples\nice_peermap.apc Packets: 12,248 Duration: 0:09:34

Figure 6.3 AiroPeek NX Peer Map, showing the results of hide non-peers from figure 6.2

Where screen space is limited, users may find the Peer Map is most useful when a smaller number of the most relevant nodes are displayed. Switching back and forth between various settings in the *Protocols* pane and choosing different *Traffic* options allows you to display the most interesting traffic quickly. Using the **Hide** functions from the context menu, you can further reduce the picture to only the most relevant nodes and traffic. At any time you can right-click in the white space of the Peer Map and choose **Arrange All Nodes** to restore the elliptical layout.

You can also drag nodes to clarify the picture of network traffic. You can drag a single node, or you can highlight multiple nodes and drag them all together. Use **Ctrl + Click** or **Shift + Click** to add unselected nodes to the selection, or to remove selected nodes from it. To move a single node back into the ellipse, select it and choose **Arrange** from the context menu. You can drag nodes to make any shape that suits your purpose, as shown in Figure 6.3.

Information about particular nodes

When you move the cursor over a particular node in the Peer Map, a tooltip appears containing information about that node.

Node	The label for this node in the current Peer Map. If the label is a symbolic name, the logical address is also shown in parentheses.
Type	The node type, as defined in the Name Table. For example, *Router*, *Workstation*, and so forth.
Protocols	All the protocols associated with this node in the current Map Type.
Packets Sent	Total, and percent of all packets this represents.
Packets Received	Total, and percent of all packets this represents.
Bytes Sent	Total, and percent of all traffic this represents.
Bytes Received	Total, and percent of all traffic this represents.
Identities	Other names and addresses by which this node is known.

To add any node in the Peer Map to the Name Table, right-click on the node and choose **Insert into Name Table…** from the context menu to open an **Edit Name** dialog with that node's characteristics already entered. To open an **Edit Name** dialog for any node in the Peer Map which already has a Name Table entry, choose **Edit Name…** from the context menu. When name resolution services are available, you can also choose **Resolve Name** from the context menu. For more about names, the Name Table and name resolution, see “Name table” on page 130.

To create a filter based on any node in the Peer map, right click and choose **Make Filter** from the context menu.

7

Name Table

This chapter describes the Name Table in AiroPeek and its powerful tools for constructing and maintaining symbolic names for network devices and processes.

When you first start capturing packets, devices on your network will typically be identified in ***Packets*** views or in statistical displays by their logical or physical addresses. The Name Table lets you assign your own symbolic names to addresses, ports and protocols.

It is easy to create and update Name Table entries in AiroPeek. You can also save and restore (export and import) the contents of the Name Table. This allows you to keep separate Name Tables for different network segments or office locations.

AiroPeek can scan all traffic, searching for logical and symbolic names in the contents of passing packets. You can control how and whether AiroPeek adds these passively discovered names to the Name Table, and tell it how to automatically age these entries, deleting those that remain unused after a certain time.

Providing names in place of logical or physical addresses makes the task of identifying packets of interest much simpler.

In this Chapter:

Name table

The Name Table lets you assign your own symbolic names to addresses, ports and protocols. This is a simple but powerful way to make packet-related information immediately familiar and intelligible.

In AiroPeek NX only, the Name Table also lets you assign a trust value to any address. By default, all addresses are Unknown, but you can classify individual nodes as either Known or Trusted. This can make security scanning, both manual and automated, far easier and far more effective.

Tip You can easily create a filter based on any entry in the Name Table. Highlight the entry and click the **Make Filter** button, or right click and choose **Make Filter…** from the context menu. For more on creating and using filters, please see Chapter 11, “Filters” on page 207.

Adding entries to the name table

AiroPeek is shipped with a default Name Table. There are several ways to create Name Table entries for your network devices. You can:

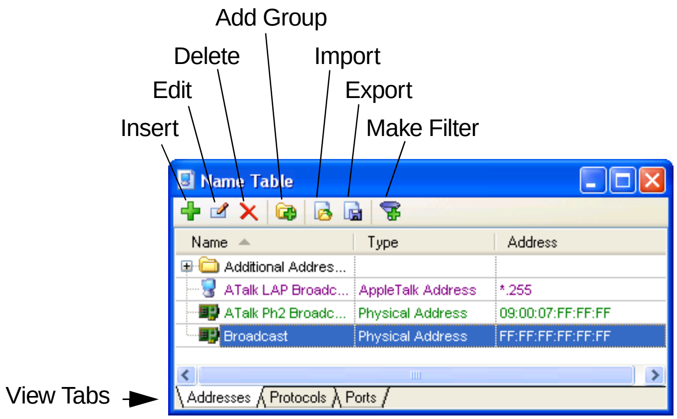
- Add names manually using the **Edit Name** dialog, displayed when you click the **Insert** button from the **Name Table** window.
- Highlight items in other views and click the **Insert Into Name Table** button, or right-click and use the **Insert Into Name Table…** command from the context menu.
- Highlight one or more items in other views and click the **Resolve Names** button, or right-click and use the **Resolve Names…** command from the context menu.
- Invoke the *Enable passive name resolution* function in the ***Name Resolution*** view of the **Options** dialog under the **Tools** menu to add WINS/NetBIOS, AppleTalk and IP names whenever AiroPeek encounters them in network traffic. This function is enabled by default.
- Use the **Import** button in the **Name Table** window to load previously saved versions of the Name Table, or to load a list of NIC vendor IDs supplied with AiroPeek to substitute the manufacturer’s name for the MAC address (physical address) of each device on the network.

Figure 7.1 below shows the ***Addresses*** view of a Name Table set up with groups.

Important! Name Table entries are used in displaying packets and statistics only if **Name Table Entry** is enabled in the **Display Format** submenu of the **View** menu. A checkmark precedes the entry when it is enabled, which is the default state for this option.

The name table window

The **Name Table** window has three views, accessed by clicking on the labeled tabs at the bottom of the window. The three views are: ***Addresses***, ***Protocols***, and ***Ports***.



Name	Type	Address
Additional Addres...		
ATalk LAP Broadc...	AppleTalk Address	*.255
ATalk Ph2 Broadc...	Physical Address	09:00:07:FF:FF:FF
Broadcast	Physical Address	FF:FF:FF:FF:FF:FF

Figure 7.1 Name Table window showing a Group

Each of these views has three columns: ***Name***, ***Type***, and a third column that corresponds to the view: ***Address***, ***Protocol***, or ***Port***, respectively. ***Name*** is the symbolic name you assigned. ***Type*** is the type of address, type of port, or type of protocol. The third column shows the discriminator AiroPeek is looking for in order to apply your symbolic name to a packet. This is written in the format of the specified type. As examples, an address of the ***Type*** *IP* will show a dotted decimal number in the ***Address*** column and a protocol of the ***Type*** *LSAP* will show the one-byte hexadecimal discriminator in the ***Protocol*** column.

Tip The Name Table allows you to sort entries in the table by the values in any column by clicking on the column headings in the **Name Table** window. A triangle appears in the column header to indicate that the display is being sorted by that column. The triangle points up if the sort is in ascending order and points down if the sort is in descending order.

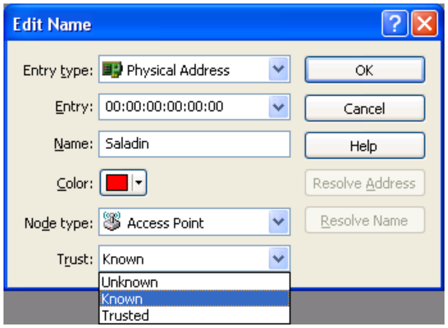
The **Name Table** window shows seven buttons. From left to right, their descriptions are shown in Table 7.1 below.

Table 7.1 Name Table buttons

Button	Description
Insert	This button opens the **Edit Name** dialog, in which you can enter all the parameters for the new name to be inserted in the Name Table.
Edit	When a name is highlighted, this button opens the **Edit Name** dialog with the details of the selected entry, ready to edit. When a Group is highlighted, it brings up the **Edit Group** dialog with the name of the highlighted Group ready to edit.
Delete	This button deletes the selected entry.
Add Group	This button opens the **Edit Group** dialog, in which you can name and create a new group. You can drag entries into and out of group folders. You can collapse or expand the view of group folder contents using the “+” in the left margin next to the folder icon.
Import	This button opens a dialog in which you can specify the Names file to load into the Name Table.
Export	This button opens a **Save** dialog allowing you to save the contents of the Name Table.
Make Filter	This button opens the **Edit Filter** dialog with an untitled filter matching the information in the selected Name Table entry.

Adding and editing name table entries manually

While AiroPeek offers many time-saving ways to populate the Name Table, some entries will always need to be entered by hand. Examples include symbolic names for routers and bridges, multicast addresses, loopback addresses, not well known ports, and protocols for which no ProtoSpec exists.



Entry type: Physical Address

Entry: 00:00:00:00:00:00

Name: Saladin

Color: 🟥

Node type: Access Point

Trust: Known

Figure 7.2 Edit Name dialog in AiroPeek NX, showing Trust options

Choose **Name Table** from the **View** menu to open the **Name Table** window. To add a new entry, click the **Insert** button in the **Name Table** window. This opens the **Edit Name** dialog. To edit an existing entry, select the entry you wish to edit and click the **Edit** button. Both the **Insert** and **Edit** buttons open the **Edit Name** dialog.

To enter the complete device or protocol entry manually:

1. Open the **Edit Name** dialog.
2. Use the *Entry type* drop-down list to select the type of entry you want to add to the Name Table.

Note: The only wildcard is the asterisk (*), and it stands for zero or more alphanumeric characters. It cannot substitute for any form of punctuation.

3. Enter the numeric designation for the entity you wish to add to the Name Table in the *Entry* edit field.
4. Enter a name in the *Name* field or, if you have entered an IP address, you can use the **Resolve Address** button in this dialog to query domain name services for a name for your specified address. Alternatively, you can specify a symbolic name and AiroPeek will attempt to resolve the name to find its address if you click the **Resolve Name** button.

Important! Active name resolution and notifications using the email action require an active network connection. Because AiroPeek puts the NIC into a “listen only” mode when the network adapter is selected, network access while AiroPeek is running requires that a second network adapter must be installed for use by network services. Alternatively, selecting either *None* or *File* as the adapter can free the NIC for network services, if the card supports this functionality. Please see our website at http://www.wildpackets.com/support for details about specific cards.

5. Assign a new color for your Name Table entry, if you wish, by clicking in the color swatch.
6. Use the *Node Type* drop-down list to set the node type for this entity, if you wish. Your choices are: *Unknown*, *Workstation*, *Server*, *Router*, *Switch*, *Repeater*, *Printer*, or *Access Point*.

Note: If a device is labeled as a *Router*, AiroPeek will suppress duplicate address notifications associated with this node.

7. In AiroPeek NX only, you can also set a value for a parameter called *Trust* for any entry in the ***Addresses*** view of the Name Table. All entries are assigned the lowest level of trust, *Unknown*, by default. You can optionally change the level of trust assigned to any node to *Known*, or to the highest level, *Trusted*. The Alarms feature can make use of this trust information in AiroPeek NX to help distinguish friend from foe.
8. Click **OK** to add the entry to the Name Table and close this dialog.

Example: adding a protocol name

To add a protocol to the Name Table:

1. Select the type of entry you want to add to the Name Table from the *Entry type* drop-down list. For example, choose *802.2 SNAP ID* to add an entry for the DECnet DNA Naming Service protocol.
2. Enter the hexadecimal representation of that protocol, *08-00-2B-80-3C,* in the *Entry* edit field.
3. Enter the name *DECnet DNA Naming Service* for the protocol in the *Name* field.
4. Assign a new color for your Name Table entry, if you wish.
5. Click **OK** to add the entry to the Name Table and close this dialog.

Note: Symbolic names assigned to protocols in the Name Table will *not* override names provided by ProtoSpecs.

Adding names from other windows

You can add to the Name Table or change name assignments for addresses by choosing device and protocol entries from a variety of other displays in AiroPeek. Basically, any window that can show individual devices can be used as a source of names for the Name Table. This includes the **Node Statistics** window, as well as the ***Packets*** and ***Nodes*** views in Capture windows or Packet File windows and **Packet Decode** windows. In the AiroPeek standard version of the program only, you can also use the ***Conversations*** view. In the AiroPeek NX version of the program only, you can also use the ***Expert*** and ***Peer Map*** views.

To add information from selected items to the Name Table:

1. Select an item in one of the appropriate views to be entered into the Name Table.

Note: Only those protocols not already identified by ProtoSpecs can be entered into the Name Table.

2. Click the **Insert Into Name Table** button, or right-click and use the **Insert Into Name Table…** command from the context menu.
3. This opens a dialog identical to the **Edit Name** dialog in form and function, but with a different dialog title. The title of the dialog that opens will depend on the nature of the item selected for insertion into the Name Table. Conversations, for example, include two addresses, each of which will be presented in turn. When you choose a packet from the ***Packets*** view for example, the first dialog that opens will be titled **Source Address**. The second will be titled **Destination Address**. In all cases, the dialog opens with the *Entry Type* and the *Entry* edit fields already filled in for the individual potential Name Table entry implied in your selection that is named in the dialog title. The *Name* field or other fields may also be filled in, depending on the information available in your selection.
4. Follow the instructions for making manual entries and edits to the Name Table given above.
5. You can only apply the **Insert Into Name Table** command to one entry at a time. If your selection presents an opportunity for adding or reviewing the settings of multiple Name Table entries, each one will be brought up in turn in a separate dialog. Click **Cancel** to close the dialog for any potential entry you do not wish to enter into the Name Table.

Trusted, known, and unknown nodes

In AiroPeek NX only, you can use the Name Table to set an attribute called *Trust* for any physical address in the Name Table. You can assign a value of *Trusted*, *Known*, or *Unknown* to any node. The default value, assigned to any node that is automatically added to the Name Table, and assumed for any node not listed there, is *Unknown*. You can assign a value of *Trusted* to the devices on your own network. The intermediate value of *Known* lets you identify familiar sources that are beyond your own control, such as an access point in a neighboring office.

You can set these values in the same way as any other Name Table attributes. Please see "Adding and editing name table entries manually" on page 132 for details.

Alternatively, you can use the context menu to edit the *Trust* value for any node in the ***802.11*** view of either the **Node Statistics** window or the ***Nodes*** view of a Capture window or Packet File window. To edit the Trust value for any node in the ***802.11*** view, right-click on the node and choose a value of **Trusted**, **Known**, or **Unknown** from the context menu. If the node is already in the Name Table, its *Trust* value will be updated. If the node is not yet in the Name Table, AiroPeek NX will silently add the node, using its physical address as the *Name* for the new entry. If the node is identified in the ***802.11*** view as an access point, the *Node type* of the new Name Table entry will also be set to *Access Point*. Otherwise, the *Node type* of new entries is set to *Unknown*.

AiroPeek NX uses the Trust information from the Name Table in the ***802.11*** view of **Node Statistics**, and in **Summary Statistics**. You can set alarms and send notifications based on Trust. The ***Expert*** can also use Trust information. Setting the Trust attributes for your network makes intrusion detection fast, accurate, and easy.

Resolving names and addresses

AiroPeek can actively resolve IP device or host names on your network if DNS is reachable. Once names are resolved, they can be added automatically to your Name Table, where the names will be available to replace logical address entries for devices in any AiroPeek displays. Remember that name substitutions will only appear in displays if you choose the **Name Table Entry** option in the **Display Format** submenu of the **View** menu. You can set rules governing how newly discovered names and addresses are written to the Name Table using the ***Name Resolution*** view of the **Options** dialog, described in the next section.

To resolve names manually:

1. Select the nodes or packets whose addresses you wish to resolve. You can do this directly in any window that shows the individual nodes, whether it is a ***Packets*** view, a Monitor statistics window, or one of the statistics views of a Capture window or Packet File window.
2. Click the **Resolve Names** button in the header of the window in which you've selected the items, or right-click and use the **Resolve Names…** command from the context menu.

   AiroPeek will use your network to find the names of the IP addresses of the selected packets. DNS must be reachable over the network, as AiroPeek uses this service to resolve names. Once names have been resolved, you will see name entries substituted for logical addresses in all AiroPeek displays.

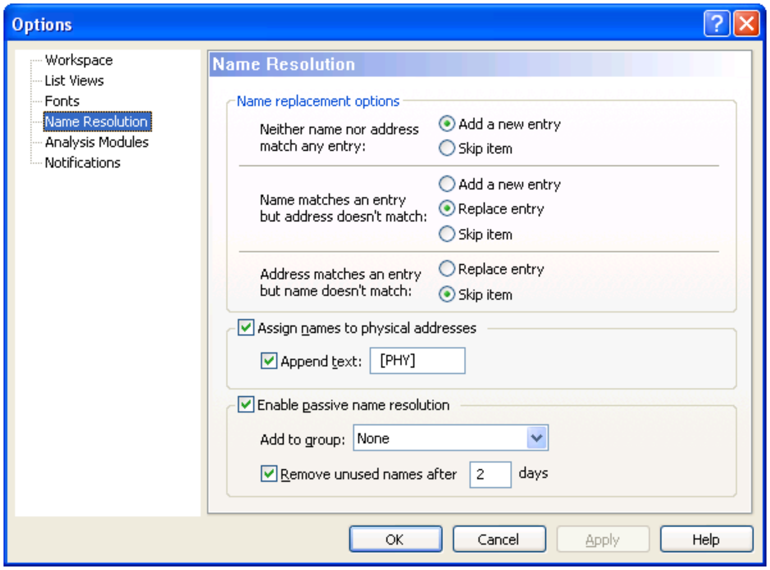
You may also look up the address of an IP name by clicking the **Resolve Name** button in the **Edit Name** dialog.

Important! Active name resolution and notifications using the email action require an active network connection. Because AiroPeek puts the NIC into a “listen only” mode when the network adapter is selected, network access while AiroPeek is running requires that a second network adapter must be installed for use by network services. Alternatively, selecting either *None* or *File* as the adapter can free the NIC for network services, if the card supports this functionality. Please see our website at http://www.wildpackets.com/support for details about specific cards.

Name resolution view of the options dialog

Name and address substitutions are controlled through the ***Name Resolution*** view of the **Options** dialog. Choose **Options…** from the **Tools** menu to open this dialog, and click the *Name Resolution* item in the navigation pane to open this view. Use the radio buttons in the *Name replacement options* section to determine how AiroPeek will use new information about names and addresses to automatically update the Name Table.

Note: AiroPeek uses a static set of rules for adding names to the Name Table when you use the **Insert Into Name Table** command. Using this command creates a new entry or edits any existing entry which matches the item you chose to insert.



Name Resolution

Name replacement options

Neither name nor address match any entry: ● Add a new entry ○ Skip item

Name matches an entry but address doesn't match: ○ Add a new entry ● Replace entry ○ Skip item

Address matches an entry but name doesn't match: ○ Replace entry ● Skip item

☑ Assign names to physical addresses

☑ Append text: [PHY]

☑ Enable passive name resolution

Add to group: None

☑ Remove unused names after 2 days

Figure 7.3 Name Resolution view of the Options dialog

Click the *Assign names to physical addresses* checkbox to automatically add names for the physical addresses found in the same packet as the logical addresses being resolved. Entries for these hardware addresses will be added to the Name Table following the same rules defined in *Name replacement options*. You may choose to add a short text string to the end of all names assigned by this function.

Note: Before resolving names and automatically assigning names to physical addresses, it is recommended that you manually add names for the physical address of intermediate link devices such as routers.

When *Enable passive name resolution* is checked, AiroPeek examines all incoming packets for symbolic names it can add to the Name Table. It adds these names according to the rules you set down in the *Name replacement options* section. Choose a Name Table group from the drop-down list if you want to put all discovered name and address pairs in a particular folder in the Name Table. This is particularly useful when much of the traffic from outside the local network uses symbolic names, as Web traffic does.

In some environments, very large numbers of new names may be discovered each day through passive name resolution. Web browsing, for example, generates packet traffic containing many more unique names than just the base URLs apparent to the casual user.

To keep the Name Table from becoming overgrown with unnecessary data, check the checkbox beside *Remove unused names after*, and enter a number of *days.* Names added by passive resolution will be removed from the Name Table when they go without being detected in network traffic for the specified time. If a name is encountered before its time is up, the clock for this item is restarted. In this way, you can ensure that all passively added names in the Name Table have been seen in network traffic at some time during, for example, the past two days.

Loading and saving name table data

You can load and save the contents of the Name Table, allowing you to keep descriptions of different segments, or to simply store and retrieve different ways of looking at the same segment.

Note: When you import items into the Name Table, a dialog asks if you want to *Delete all entries before importing?* the new names. If you click **Yes**, the imported names will be the only ones in the new Name Table, and all of the previous entries will be deleted. If you click **No**, the new names will be added to the Name Table alongside the existing entries. Only exact duplicates of existing entries will be ignored.

Importing vendor and protocol IDs

A variety of names files are included in the Names directory in the directory where you installed AiroPeek. You may wish to review these name files to determine if they would save you time in creating your own Name Table.

When there are no specific Name Table entries for devices on your network, vendor IDs provide vendor names in place of physical network addresses, giving you the information to identify the NIC vendor or type of device. With this information, you can then narrow down specific node activity on your network.

To add the vendor ID files to your Name Table:

1. Open the Name Table by choosing **View** > **Name Table** from the main menu.
2. Click the **Import** button in the **Name Table** window.
3. In the dialog which asks if you want to *Delete all entries before importing?*, click **No** to add the vendor IDs to the Name Table without deleting any of the existing entries.

4. Use the resulting **Open** dialog to navigate to the location of the VendorID.nam file, containing the vendor IDs. Its default location is in the Names directory within the directory where you installed AiroPeek.
5. Choose the VendorID.nam file and click **OK** to add the names to the Name Table.

Loading a previously saved name table

You can load the contents of previously built and saved Name Tables, including any Name Table files you may have created manually or exported using other WildPackets analyzers.

Note: In order for AiroPeek to recognize a file as a Name Table, the file must have a *.nam file extension.

To load the names from another Name Table into the current Name Table:

1. Open the Name Table by choosing **View** > **Name Table** from the main menu.
2. Click the **Import** button in the **Name Table** window.
3. In the dialog which asks if you want to *Delete all entries before importing?*, click **Yes** if you would like to replace the existing Name Table with the imported names. Alternatively, you could add the imported names to the current Name Table by clicking **No** in the warning dialog.
4. Use the resulting **Open** dialog to navigate to the location of the file you wish to load.
5. Choose this file and click **OK** to add the contents of this file to the current contents of the Name Table.

Saving the name table

You can save all or a selected subset of the Name Table to a new file. If your work involves managing several networks, it can often be useful to build and store Name Tables for each of the networks you support. Then, when you visit each network site, you can import into the Name Table the device and protocol names relevant to that environment.

To save the entire contents of the current Name Table under a new name:

1. Open the Name Table by choosing **View** > **Name Table** from the main menu.
2. Click the **Export** button in the **Name Table** window.

3. Use the resulting **Save** dialog to name the file and choose a location in which to save it.
4. Click **OK** to save the file.

   You can also save selected names from the Name Table. Group folder information is preserved when exporting either individual entries or the entire Name Table.

To save selected names from the current Name Table into a new Name Table file:

1. Open the Name Table by choosing **View** > **Name Table** from the main menu.
2. Select the entries you wish to export. You can use the standard Windows **Ctrl + click** and **SHIFT + click** to highlight multiple entries.
3. Right-click and choose **Export Selected…** from the context menu.
4. Use the resulting **Save** dialog to name the file and choose a location in which to save it.
5. Click **OK** to save the file.

Note: When a Name Table group folder is highlighted, the **Export Selected…** function will export the whole contents of the folder only if no individual entries within the folder are selected. If entries within the folder are highlighted, then only those highlighted entries will be exported, and not the whole contents of the folder.

Log File

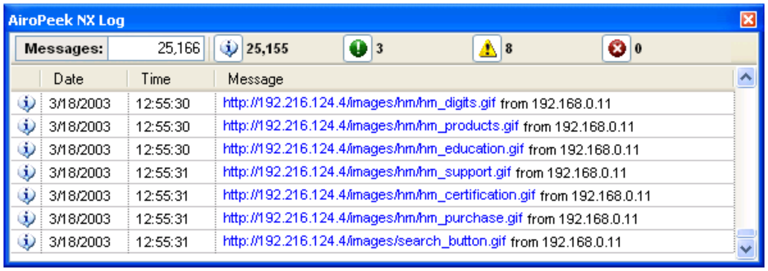
AiroPeek has a global log for the program as a whole, as well as individual log files for each Capture window and Packet File window. This chapter describes the functions of the log files.

In this Chapter:

When AiroPeek is launched, an AiroPeek Log file (called Peek.log) is created in the Application Data folder. This log is referred to in this manual as the global log file or the **AiroPeek Log** window. The title of the window itself will appear as **AiroPeek Log** in the AiroPeek standard version of the program and as **AiroPeek NX Log** in the AiroPeek NX version.

Three types of events can result in items being written to this AiroPeek Log. A few events, such as the starting or stopping of AiroPeek or the creation of a new Capture window, are hard-coded to send a message to the AiroPeek Log. Some events, such as the writing of statistics from the ***Statistics Output*** view function, will create an entry in the AiroPeek Log if the user specifies in the function's set-up dialog that it should do so. Other events are noted in the AiroPeek Log only when they send a notification which has as one of its actions the Log type action, as notifications of all levels of severity do by default. Analysis Modules, triggers and alarms are examples of this type. Alarms always send a notification, but the notification must have the Log type action in order for a message to be posted to the AiroPeek Log.

Individual Capture windows and Packet File windows also each have a view called ***Log*** which accepts the same classes of data from the same notifications as the global AiroPeek Log. The main difference is that the ***Log*** view of a Capture window or a Packet File window contains only the items that are relevant to that particular window. For example, the ***Log*** view of a Capture window will show results from any enabled Analysis Modules processing just those packets that are entered into the buffer of that window. The AiroPeek Log, in contrast, contains the results from any enabled Analysis Modules processing the packets used to calculate Monitor statistics. The ***Log*** view of a Capture window or a Packet File window has only 128K bytes of memory. Older entries are discarded to make room for new entries.


AiroPeek NX Log

Messages: 25,166 | 25,155 | 3 | 8 | 0

	Date	Time	Message
i	3/18/2003	12:55:30	http://192.216.124.4/images/hm/hm_digits.gif from 192.168.0.11
i	3/18/2003	12:55:30	http://192.216.124.4/images/hm/hm_products.gif from 192.168.0.11
i	3/18/2003	12:55:30	http://192.216.124.4/images/hm/hm_education.gif from 192.168.0.11
i	3/18/2003	12:55:31	http://192.216.124.4/images/hm/hm_support.gif from 192.168.0.11
i	3/18/2003	12:55:31	http://192.216.124.4/images/hm/hm_certification.gif from 192.168.0.11
i	3/18/2003	12:55:31	http://192.216.124.4/images/hm/hm_purchase.gif from 192.168.0.11
i	3/18/2003	12:55:31	http://192.216.124.4/images/search_button.gif from 192.168.0.11

Figure 8.1 AiroPeek NX Log window

The header area of the **AiroPeek Log** window shows the total number of messages in the log and their breakdown by level of severity of notification (represented by their icons). You can toggle between hiding and showing the notifications of any level of severity by clicking on their icon at the top of the window.

To view the contents of the AiroPeek Log, choose the **Log Window** command from the **View** menu or press **Ctrl + L**.

Tip The Web Analysis Module writes URLs it discovers in network traffic to the AiroPeek Log. You can access that Internet resource by double-clicking on the URL directly in the **AiroPeek Log** window. This launches your default Internet browser and opens the selected URL.

By default, the AiroPeek Log is limited to 4MB. When this limit is reached, the AiroPeek Log will delete older entries to make room for new ones. To change this upper limit, choose **Maximum Log File Size…** from the **AiroPeek Log** window context menu (right-click inside the **AiroPeek Log** window). This opens a dialog in which you can enter the new maximum size for the Log file, in kilobytes. Click **OK** to accept your changes or click **Cancel** to close the **Maximum Log File Size** dialog without making any changes.

To save the AiroPeek Log as a text file (tab-delimited or comma separated values), right-click in the **AiroPeek Log** window and choose **Save Log…** from the context menu. To copy individual lines from the AiroPeek Log to the clipboard as tab-delimited text, highlight the lines and choose **Copy** from the context menu. You can also choose to **Select All** lines by choosing that item in the context menu.

To clear or empty the AiroPeek Log, right-click in the **AiroPeek Log** window and choose **Clear Log** from the context menu.

To print the AiroPeek Log, right-click in the **AiroPeek Log** window and choose **Print Log…** from the context menu. To alter default print settings, choose **Print Setup…** from the **File** menu.

You can toggle the Auto Scroll feature of the **AiroPeek Log** window by choosing the **Auto Scroll** item from the context menu. A checkmark appears next to that item when it is enabled.

Statistics

For monitoring, baselining, or troubleshooting network problems of all kinds, statistics are a vital tool.

AiroPeek calculates a variety of key statistics in real time. It presents these statistics in intuitive graphical displays. You can save, copy, print, and/or automatically generate periodic reports on these statistics in a variety of formats.

Node Statistics and **Protocol Statistics** offer detailed views of any item in their main displays with a double-click of the mouse. You can also create a separate graph of items in these or the **Summary Statistics** display quickly and easily. You can create snapshots of your network in **Summary Statistics** and save them for later side-by-side comparison with current conditions.

You can control how statistics are presented in each window, allowing you to quickly isolate anomalies and potential problems.

You can also set sophisticated multi-step alarms based on most items in Monitor statistics displays. You can further key these alarms to notifications whose severity and type of response action you control. For more on Alarms, please see “Alarms” on page 242. For more on Notifications, please see “Notifications” on page 248.

This chapter describes Monitor statistics in general, then describes each type of statistic in detail. It notes differences between Monitor statistics and those found in Capture windows and Packet File windows. The chapter ends with a look at printing, saving, and other outputs of statistics.

In this Chapter:

General view of statistics windows

Under its default settings, AiroPeek begins calculating Monitor statistics as soon as the program is launched, and continuously updates its statistics as long as the program is running. More precisely, when the **Monitor Statistics** item under the **Monitor** menu is enabled (as it is by default), AiroPeek analyzes all network traffic continuously in the background from the moment the program loads and the adapter for Monitor statistics is chosen until you quit the program or disable the **Monitor Statistics** item.

All packets read from the network by the Monitor statistics functions are processed and then discarded. The Monitor statistics functions of AiroPeek keep only the aggregate information needed to provide an updated tally of all the tracked parameters. Monitor statistics are not altered by filters, triggers, or any other such function. Monitor statistics are simply on or off.

Because the packets used to calculate Monitor statistics are not saved, they do not function like packets in a Capture window or Packet File window. They cannot be examined individually or used for other purposes. To actually capture packets and make them available for individual decoding, you must use a Capture window. Packet File windows and Capture windows offer most of the statistical displays found in Monitor statistics, but base their calculations on the contents of their own buffers. For more on the distinction between Monitor statistics and the statistics in Capture windows and Packet File windows, please see “Statistics in capture windows” on page 180.

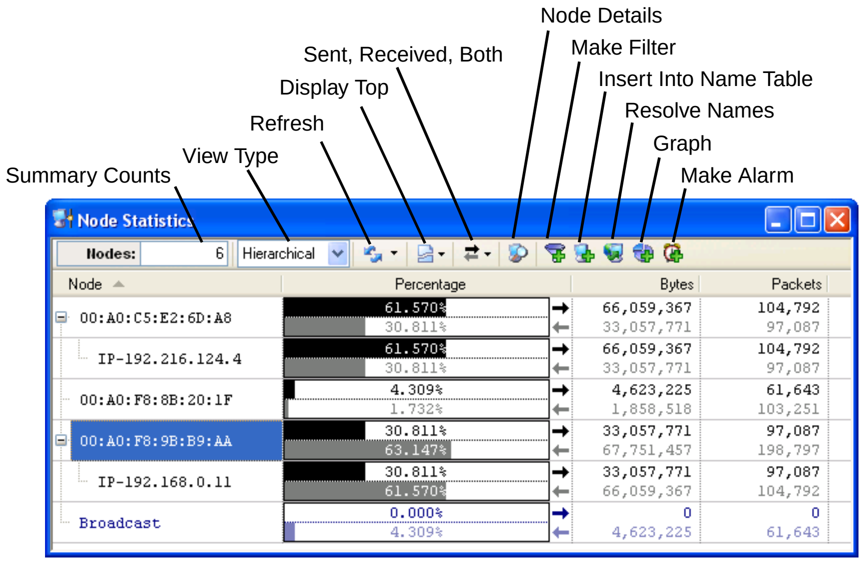
Start, stop and reset monitor statistics

By default, Monitor statistics begin calculation immediately and continue to accumulate data as long as AiroPeek is running. From the **Monitor** menu, you can change either of these defaults. Select the toggle choice labeled **Monitor Statistics** (enabled by default) to stop or start the collection of Monitor statistics. A ✓ checkmark indicates this item is enabled and Monitor statistics are being collected. Choose the item labeled **Reset Statistics** to discard all the Monitor statistics data accumulated to that moment and return all Monitor statistics displays to their zero or empty state.

Statistics window headers and display controls

This section describes the various elements of statistics windows and statistics views, both for Monitor statistics and for those in Capture windows and Packet File windows.

The following table (Table 9.1) describes the function of typical features of statistics windows. Please refer to Figure 9.1 for examples of most of these items.



Nodes: 6
Hierarchical

Node	Percentage		Bytes	Packets
00:A0:C5:E2:6D:A8	61.570% 30.811%	→ ←	66,059,367 33,057,771	104,792 97,087
IP-192.216.124.4	61.570% 30.811%	→ ←	66,059,367 33,057,771	104,792 97,087
00:A0:F8:8B:20:1F	4.309% 1.732%	→ ←	4,623,225 1,858,518	61,643 103,251
00:A0:F8:9B:B9:AA	30.811% 63.147%	→ ←	33,057,771 67,751,457	97,087 198,797
IP-192.168.0.11	30.811% 61.570%	→ ←	33,057,771 66,059,367	97,087 104,792
Broadcast	0.000% 4.309%	→ ←	0 4,623,225	0 61,643

Figure 9.1 Node Statistics window, showing window element labels

Table 9.1 Statistics window elements

Element	Usage
Summary counts	Several statistics windows, including **Node**, **Protocol** (and their **Detail Statistics** windows), and **Network Statistics**; show summary counts for a few key items. **Protocol Statistics**, for example, shows the total *Protocols seen* in the upper left of the window.

Table 9.1 Statistics window elements (continued)

Element	Usage
View Type	The **View Type** drop-down list in the **Node Statistics** window lets you choose between a ***Hierarchical*** view of network nodes, in which logical addresses and symbolic names are nested beneath their physical addresses, an ***802.11*** view of all wireless nodes in a nested SSID tree view, or any of a variety of flat (that is, un-hierarchical) tabular displays of nodes defined by a particular address type. The column headings also change with the **View Type** choice.
Refresh rate drop-down list and button	Several statistics windows, including **Node**, **Protocol**, and **History** statistics, allow the user to change the display refresh interval by selecting values from a drop-down list. If the interval is set to *Manual*, you must click the **Refresh** button to update the display.
Display top	For **Node** statistics, you can use the drop-down list to limit the display to the top *5*, *10, 20*, *50*, or *100* nodes seen, as measured by traffic volume. Alternatively, you can use the drop-down list to choose to display *All*.
Display Sent/Received/Both	Unique to the ***Hierarchical*** view of **Node** statistics, this drop-down list allows you to limit the display to packets *Sent*, or packets *Received*, or to show both by choosing *Sent and Received*.
Units	**History**, **Summary**, and **Channel** statistics each have a drop-down list used to select the units in which their statistics are displayed. **History** statistics can be displayed as a percent of network bandwidth *Utilization*, or as *Bytes/second* or *Packets/second*. **Summary** statistics can be displayed in either of these last two units, or in *Packets*, *Bytes*, or a percentage of either. The ***Channels*** view of the **Channel Statistics** window can display *Packets*, *Bytes*, or *All* (both). Other statistics windows present information in a variety of units within a single display.
Snapshot button	Unique to the **Summary Statistics** window, the **Snapshot** button saves the current statistics values for side by side comparison with future values.

Table 9.1 **Statistics window elements (continued)**

Element	Usage
Detail button	Opens **Detail Statistics** windows for all selected items. Available for **Node** and **Protocol Statistics** windows.
Pause button	Operates as a toggle to temporarily suspend scrolling or screen re-draw due to data update in the statistics list or graph. Available for **Size**, **Summary**, and **History Statistics** windows, and in the ***Signal*** view of the **Channel Statistics** window. This button is also used in all statistics **Graph** windows.
Make Filter button	Opens the **Edit Filter** dialog with parameters for a filter that will match the currently selected item. For details, please see “Make filter command” on page 211.
Insert Into Name Table button	Opens a dialog allowing you to enter the item into the Name Table. For details, see “Adding names from other windows” on page 134.
Resolve Names button	Attempts to resolve selected addresses using DNS, when that service is available. When names are found, they are inserted into the Name Table.
Graph button	Opens the **Graph Data Options** dialog to create a graphical representation of the selected item. Please see “Creating and controlling graph windows” on page 194 for more details.
Make Alarm button	Opens the **Make Alarm** dialog to define the parameters for establishing and resolving alarm conditions associated with the selected item. Available for **Node**, **Protocol**, **Summary**, and **Channel Statistics** windows. Please see “Alarms” on page 242 for more details.

Display options for statistics windows

You can change the sort order of statistics presented in a table (**Node** and **Protocol**), and collapse or expand those listed in a hierarchy (**Node**, **Protocol**, and **Summary**). In the ***List Views*** view of the **Options** dialog, you can customize background color and the style of vertical and horizontal lines in all list displays. To change this and other default aspects of window display, use the **Options** dialog, available by choosing **Options…**

under the **Tools** menu. The items, or individual elements of items, will take the colors assigned in the **Color** menu, accessible from the **View** menu.

Sorting, collapsing and expanding lists

To change the sort order of any list of statistics, click in the heading of the column by which you want to sort the display. Click in the column header again to toggle between ascending and descending order. The order is indicated by a small triangle pointing up or down, shown in the header of the column by which the display is sorted. In the ***Hierarchical*** view of the **Node Statistics** window, you can use the drop-down list to choose whether to display statistics about packets *Sent*, *Received*, or both.

Note: Hierarchical lists are sorted within their own level of the hierarchy.

To expand or collapse individual groups in hierarchical lists, click on the + plus or - minus sign in the left margin beside any group entry. Right-click to bring up a context menu with options to **Collapse All** or **Expand All** hierarchical items.

Controlling color in statistics lists

The **Color** sub-menu of the **View** menu determines how colors *already assigned in other dialogs* will be used in displaying data in the **Node Statistics** window. There are only two sources of color assignments for elements of network traffic in AiroPeek that have an effect on the **Node Statistics** display:

- The **Edit Name** dialog in the **Name Table** can set the color for packets associated with a particular address (node), port, or protocol.
- ProtoSpecs assign colors to all the protocols they know how to identify, and their color choices cannot be overridden.

The **Color** sub-menu of the **View** menu uses the color information from these other sources, and applies it to the display of nodes and protocols in statistics lists. For more about how colors are assigned to packet lists and statistics displays, please see “Color display options” on page 84.

Monitor statistics

You can open any or all Monitor statistics windows from the **Monitor** menu: **Node**, **Protocol**, **Network**, **Size**, **Summary**, **History,** and/or **Channel Statistics**. Each of these is described in detail in this section.

Tip All of the Monitor statistics windows can be displayed at the same time. However, if they are all displaying information in real-time during capture and the network is very busy, AiroPeek might not have enough time to process captured packets. This can cause statistics to lag behind actual network activity or cause packets to be dropped.

Node statistics

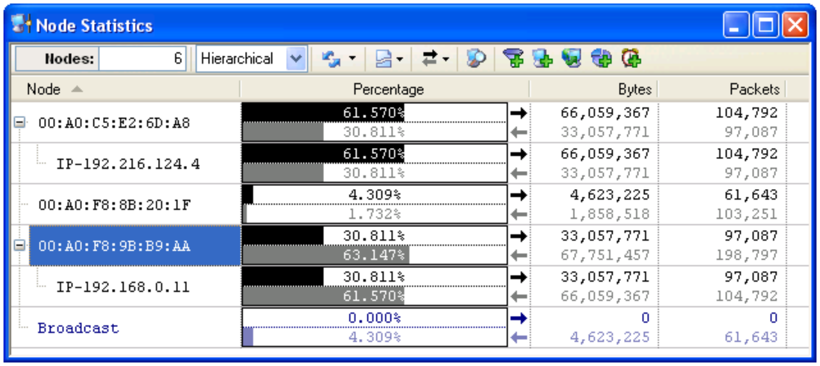
To open the **Node Statistics** window, choose **Nodes** from the **Monitor** menu or press **Ctrl + 1**. The **Node Statistics** window displays real-time data organized by network node.

The *View Type* drop-down list in the **Node Statistics** window lets you choose between a ***Hierarchical*** view of network nodes (in which logical addresses are nested beneath their physical addresses), an ***802.11*** view of all wireless nodes in a nested SSID tree view, or any of a variety of flat (that is, not hierarchical) tabular displays of nodes defined by a particular address type. The column headings also change with the *View Type* choice.

Hierarchical view of node statistics

The ***Hierarchical*** view shows network nodes or devices identified by their physical address, with any associated logical addresses nested underneath. The header of the window shows a count of the total network *Nodes* seen. For each node and unique address, the ***Hierarchical*** view can present information about traffic sent, received, or both, depending on you selection from the **Sent, Received, Both** drop down list in the window header. For each line, the ***Hierarchical*** view shows the total ***Bytes*** and ***Packets***, plus a ***Percentage*** column showing graphically and numerically the total bytes for this line, expressed as a percentage of total bytes for all lines in the ***Hierarchical*** view.

Use the drop-down lists at the top of the window to control the display. These items are labeled in Figure 9.1, and Table 9.1 describes how to use each of these elements to control the display of statistics and other functions.



Node	Percentage		Bytes	Packets
00:A0:C5:E2:6D:A8	61.570% 30.811%	→ ←	66,059,367 33,057,771	104,792 97,087
IP-192.216.124.4	61.570% 30.811%	→ ←	66,059,367 33,057,771	104,792 97,087
00:A0:F8:8B:20:1F	4.309% 1.732%	→ ←	4,623,225 1,858,518	61,643 103,251
00:A0:F8:9B:B9:AA	30.811% 63.147%	→ ←	33,057,771 67,751,457	97,087 198,797
IP-192.168.0.11	30.811% 61.570%	→ ←	33,057,771 66,059,367	97,087 104,792
Broadcast	0.000% 4.309%	→ ←	0 4,623,225	0 61,643

Figure 9.2 Node Statistics window

The ***Node*** column shows a hierarchical address list showing the physical address and any associated logical addresses (or their symbolic names) for each node being monitored. To set the window to show only the nodes generating or receiving the most traffic, select a value from the drop-down list at the top of the window labeled *Display top*. You can choose to display the top *5*, *10*, *20*, *50*, or *100* nodes; or you can choose to display *All*.

The ***Node*** address list can be set to look at the Name Table and replace physical or logical addresses with the symbolic names (and associated colors) stored there. To toggle the **Node Statistics** display's use of the Name Table, go to the **View** menu, pull down **Display Format** and choose **Name Table Entry**. A checkmark appears beside the choice when it is enabled.

The ***Percentage*** bar graph represents the bytes sent (top bar) and/or received (bottom bar) by each node. Use the drop-down list at the top of the window to display only *Sent*, only *Received*, or display both by choosing *Sent and Received*.

The ***Bytes*** column shows the total bytes, sent and/or received, for each node. The ***Packets*** column displays the number of packets, sent and/or received, for each node.

To change the sort order of any list of statistics, click in the heading of the column by which you want to sort the display. Click in the column header to toggle between ascending and descending order. The order is indicated by a small triangle pointing up or down, shown in the header of the column by which the display is sorted.

If you intend to keep the window open for some length of time, you may want to select a longer refresh interval, or set it to **Manual**. You can set the refresh interval for this window by using the drop-down list at the top of the display. This applies only to refresh of the display, as calculation goes on continuously in the background. Nevertheless, longer refresh intervals do save processing time for other tasks, such as processing packets. Click the **Refresh** button at any time to manually refresh the display.

802.11 view of node statistics

The ***802.11*** view of the **Node Statistics** window (Figure 9.3) shows an SSID (Service Set Identifier) tree view of wireless nodes. From top to bottom, the hierarchy is:

- ESSID - Extended Service Set Identifier - an optional shared identifier string
  - BSSID - Basic Service Set Identifier - hexadecimal identifier of a group
    - Station (STA) - station MAC address

The ESSID is a user-defined string which may optionally be used to identify a group of access points (APs) belonging to the same Extended Service Set (ESS). An ESS is two or more access points connected to the same wired network or DS (distribution system).

In theory, the ESSID was intended to help roaming nodes identify their network location. In practice many devices ship with the product name or other default values for ESSID. There is some concern that the ESSID, because it is always transmitted in the clear, could compromise security. Many installations leave this item blank or set APs to not transmit their ESSID. When the ESSID is not broadcast in Beacon packets, it is sometimes present in Probe Response packets, which AiroPeek can use to correctly identify the ESSID. When no ESSID can be established, the ***802.11*** view shows such nodes under the *ESSID Unknown* heading.

The BSSID (Basic Service Set ID) is a six digit hexadecimal identifier for the minimum configuration that represents a network. The 802.11 WLAN standards recognize two basic types of arrangements of wireless nodes: infrastructure mode, and ad hoc mode.

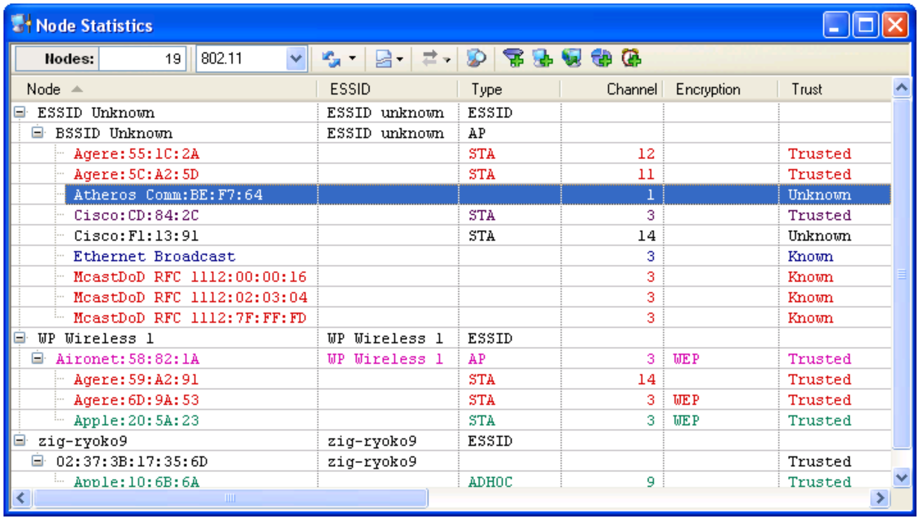
In infrastructure mode one or more stations are served by an access point that is connected to the wired network (the infrastructure). The access point or base station mediates communications among the nodes and provides a connection to resources on the wired network. The BSSID of such a group is typically the MAC address of the 802.11 WLAN card in the access point (AP) serving them. Access points advertise their presence by sending beacon packets. When a beacon packet is detected, the ***802.11*** view classifies the source node as an *AP*, shown in the ***Type*** column.

In ad hoc mode, two or more stations communicate directly, without reference to any wired network or its access points. The nodes simply “elect” one of their number to act as a base station and perform some of the mediating functions of the missing access point.

The BSSID of such a group (an IBSS, or Independent Basic Service Set) is derived from the MAC address of the node temporarily acting as a base station for the group. The station temporarily acting as the base station in such a group is identified as *ADHOC* in the ***Type*** column of the ***802.11*** view of **Node Statistics**.

Each individual station (*STA*) is ranged under the BSSID of the AP (or equivalent) to which it most recently sent a packet.

Stations which have never sent a packet cannot be assigned to an actual BSSID. Until they send a packet to an AP or to a member of an ad hoc group, these nodes are ranged under the placeholder heading *BSSID Unknown*. Two classes of addresses show up in the *BSSID Unknown* category: broadcast addresses, and nodes which are out of range of AiroPeek, but whose address is found in packets from nodes that are within range.



Node	ESSID	Type	Channel	Encryption	Trust
⊟ ESSID Unknown	ESSID unknown	ESSID			
⊟ BSSID Unknown	ESSID unknown	AP			
Agere:55:1C:2A		STA	12		Trusted
Agere:5C:A2:5D		STA	11		Trusted
Atheros Comm:BE:F7:64			1		Unknown
Cisco:CD:84:2C		STA	3		Trusted
Cisco:F1:13:91		STA	14		Unknown
Ethernet Broadcast			3		Known
McastDoD RFC 1112:00:00:16			3		Known
McastDoD RFC 1112:02:03:04			3		Known
McastDoD RFC 1112:7F:FF:FD			3		Known
⊟ WP Wireless 1	WP Wireless 1	ESSID			
⊟ Aironet:58:82:1A	WP Wireless 1	AP	3	WEP	Trusted
Agere:59:A2:91		STA	14		Trusted
Agere:6D:9A:53		STA	3	WEP	Trusted
Apple:20:5A:23		STA	3	WEP	Trusted
⊟ zig-ryoko9	zig-ryoko9	ESSID			
⊟ 02:37:3B:17:35:6D	zig-ryoko9				Trusted
Apple:10:6B:6A		ADHOC	9		Trusted

Figure 9.3 AiroPeek NX 802.11 view of Node Statistics , showing Type and Trust values

The ***802.11*** view of the **Node Statistics** window shows all the columns listed and described in Table 9.2. The table shows which of these columns are present by default in the ***802.11*** view. In addition, the ***802.11*** view also shows all the columns found in the flat views of **Node Statistics**, shown in Table 9.3. (Note that ***Broadcast Packets*** and ***Multicast Packets*** are present by default in all the flat node type views, but are off by default in the ***802.11*** view.)

Data rates are dependent on physical layer implementations, and different data rate columns are available, depending on the standards supported by the selected adapter. For more about data rates, please see “Transmission rates and channels” on page A-12.

Note: In 802.11 WLANs, every packet begins with a preamble and PLCP header sent at the lowest common data rate. The body of the packet can then be sent at any of the supported data rates. It is the data rate at which the body of the packet is sent that is reported in data rate columns.

Table 9.2 Columns in 802.11 view only

Default	Column	Description
X	***Node***	The ***Node*** column in the ***802.11*** view is unique in that it displays the nodes in a nested hierarchy of stations (*STA*) under *BSSID*s, under *ESSID*s.
X	***ESSID***	The ESSID for this node. ESSID (or SSID) is a short text string used to identify the members of an “Extended Service Set,” meaning a network with multiple access points, or an access point connecting to a wired LAN. When ESSIDs are in use, access points (or equivalents) will announce their ESSID in Beacon packets and/or Probe Response packets.
	Type	The type of node. This is either the identifying string of an extended service set (*ESSID*), an Access Point (*AP*), an ordinary station temporarily acting as the base station for an ad hoc group (*ADHOC*), or a Station (*STA*). Broadcast or Multicast addresses and unknown node types will show a blank in this field.
X	***Channel***	The channel on which AiroPeek was listening when the most recent packet for this node was captured. During a channel scan, this value may appear anomalous, as the same node may be detected on multiple channels but only the most recent will show in this column. IMPORTANT: The channel shown for Nodes identified as an Access Point (*AP*) will be the channel on which that AP is broadcasting, as identified in the AP’s Beacon packets and Probe Responses.

Table 9.2 Columns in 802.11 view only (continued)

Default	Column	Description
	Authentication	Shows the most recently seen form of authentication used by this node to connect with its BSSID. Example values include *EAPTLS*, *LEAP*, and *PEAP*. Note that AiroPeek does not monitor the authentication state of all nodes, but only registers the most recent authentication. Also, some authentication methods are encrypted in a way that prevents identification of the authentication method.
X	***Encryption***	Shows the most recently seen form of encryption used by this node to communicate with its BSSID. Example values include *CKIP*, *TKIP*, and *WEP*. Note that AiroPeek does not monitor the encryption state of all connections, but only registers the most recent method seen from each node.
X (AiroPeek NX only)	***Trust***	Unique to AiroPeek NX, this column shows the user-assigned trust setting from the Name Table for this BSSID or STA. Possible values are: *Unknown* (the default), *Known*, and *Trusted*. Right-click on any node in the ***802.11*** view to change this property for that node by selecting from the context menu.
	Signal Strength columns	A variety of columns showing statistics related to signal strength reported with each packet, expressed either as a percentage (***Min. Signal***, ***Cur. Signal***, and ***Max. Signal***) or in decibel milliWatts (dBm) (***Min. Signal dBm***, ***Cur. Signal dBm***, and ***Max. Signal dBm***). Min. = Minimum signal strength reported on this channel from the time the statistics count was created until the most recent update. Cur. = Most recently reported signal strength on the channel. Max. = Maximum signal strength reported on this channel from the time the statistics count was created until the most recent update.

Table 9.2 **Columns in 802.11 view only (continued)**

Default	Column	Description
	Noise columns	A variety of columns showing statistics related to noise reported with each packet, expressed either as a percentage (***Min. Noise***, ***Cur. Noise***, and ***Max. Noise***) or in decibel milliWatts (dBm) (***Min. Noise dBm***, ***Cur. Noise dBm***, and ***Max. Noise dBm***). Min. = Minimum noise reading reported on this channel from the time the statistics count was created until the most recent update. Cur. = Most recently reported noise reading on the channel. Max. = Maximum noise reading reported on this channel from the time the statistics count was created until the most recent update.
	Total Bytes	Total bytes for all traffic seen to and from this node.
X	***Retry Packets***	The number of Retry packets sent by this node.
X	***WEP Packets***	The number of packets sent by this node with their WEP bit set to 1, indicating the packet contents were encrypted.
X	***WEP ICV Errors***	The number of packets sent by this node that showed a failed ICV check. The ICV is a checksum performed over the data portion of a WEP-encrypted packet. On an otherwise properly formed packet, this often means the WEP keys used to decrypt the packet are not the right ones. Packets with CRC errors will commonly show as also having WEP ICV errors.
X	***WEP Key***	The WEP Key ID used by this node. This value (in the simplest configurations, *0*, *1*, *2*, or *3*) indicates which of multiple shared keys was used for encryption.
	Total Packets	Count of total packets seen to and from this node.
	Beacon Packets	The number of Beacon packets sent by this node.

Table 9.2 Columns in 802.11 view only (continued)

Default	Column	Description
	Broadcast ESSID	Shows whether or not beacon packets from this node contained an ESSID string.
	Data Rate columns	Columns can show the number of packets sent at the data rate or the number of bytes sent at the data rate, shown in the column header. You can show either or both types for any and all data rates supported by the current adapter. [data rate] ***Mbits/s Packets*** Shows the number of packets sent from this node in which the body of the packet (not the preamble) was sent at the data rate shown in the column header. [data rate] ***Mbits/s Bytes*** Shows the number of bytes sent from this node in which the body of the packet (not the preamble) was sent at the data rate shown in the column header.

Flat views of node statistics

In addition to the ***Hierarchical*** view and the ***802.11*** view, the **Node Statistics** window can present data in a variety of flat tables which list nodes of a particular type in the left-most column and data about the traffic of those nodes in a series of columns to the right. These flat views each correspond to one particular protocol or address type. The columns shown in the **Node Statistics** window change to match the view type. The available flat view types for **Node Statistics** are: ***Physical***, ***IP***, ***IPv6***, ***AppleTalk***, ***DECnet***, and ***IPX***.

Table 9.3 lists and describes the columns common to all of the flat view types and notes for each whether it is present by default. (The ***802.11*** view also shows all the columns in Table 9.3, although ***Broadcast Packets*** and ***Multicast Packets*** are not present by default in the ***802.11*** view. The ***802.11*** view also has an additional set of columns, listed and described in Table 9.2.)

To change which columns are visible in any particular flat table view of the **Node Statistics** window, right click in any column header to bring up a list of all available columns. Visible columns show a check mark beside them. Click on any column name to toggle its state between shown or not shown.

Table 9.3 **Columns in 802.11 view and flat views**

Default	Column	Description
X	***Node***	The address or name of the node, in the format appropriate to the view type.
X	***Bytes Sent***	Total bytes sent by this node.
X	***Packets Sent***	Total packets sent by this node.
X	***Bytes Received***	Total bytes received by (or addressed to) this node.
X	***Packets Received***	Total packets received by (or addressed to) this node.
X	***Broadcast Packets***	Total broadcast packets sent by this node.
	Broadcast Bytes	Total broadcast bytes sent by this node.
X	***Multicast Packets***	Total multicast packets sent by this node.
	Multicast Bytes	Total multicast packets sent by this node.
	Min. Size Sent	The size of the smallest packet sent by this node.
	Max. Size Sent	The size of the largest packet sent by this node.
	Avg. Size Sent	The average size of the packets sent by this node.
	Min. Size Received	The size of the smallest packet received by this node.
	Max. Size Received	The size of the largest packet received by this node.
	Avg. Size Received	The average size of the packets received by this node.
	First Time Sent	Time stamp of the first packet sent by this node.
	Last Time Sent	Time stamp of the most recent packet sent by this node.
	First Time Received	Time stamp of the first packet received by this node.

Table 9.3 Columns in 802.11 view and flat views (continued)

Default	Column	Description
	Last Time Received	Time stamp of the most recent packet received by this node.
	Duration	The difference between the time stamp of the earliest sent or received packet and that of the most recent sent or received packet.

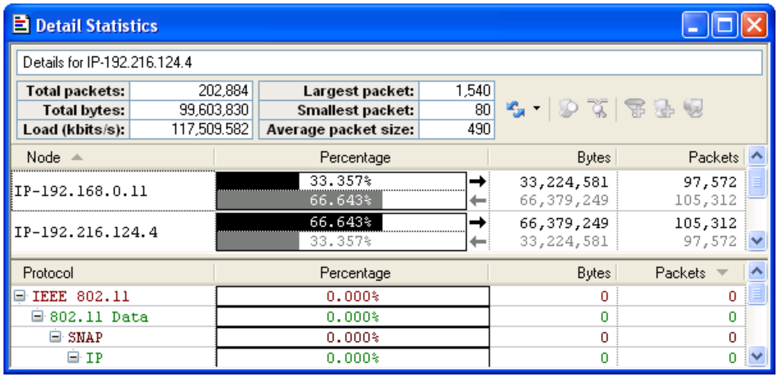
Viewing details for a network node

Double-click the entry to see more detail about the activity for the selected node or protocol. A window similar to that shown in Figure 9.4 opens.

The additional detail includes:

- Details of communications partners for this node.
- A hierarchical list of protocols used by this node and its communications partners. For details on display conventions, see “Protocol utilization statistics” on page 165.
- The *Total packets* and *Total bytes* for this node.
- Network *Load (kbits/s)* attributed to this node.
- *Largest packet*, *Smallest packet* and *Average packet* size for the specific node or protocol.

Click the **Refresh** button to update the display. Alternatively, you can use the **Refresh** drop-down list to set a refresh interval for the **Detail Statistics** window.



Detail Statistics

Details for IP-192.216.124.4

Total packets:	202,884	Largest packet:	1,540
Total bytes:	99,603,830	Smallest packet:	80
Load (kbits/s):	117,509.582	Average packet size:	490

Node	Percentage		Bytes	Packets
IP-192.168.0.11	33.357% 66.643%	→ ←	33,224,581 66,379,249	97,572 105,312
IP-192.216.124.4	66.643% 33.357%	→ ←	66,379,249 33,224,581	105,312 97,572

Protocol	Percentage	Bytes	Packets
⊟ IEEE 802.11	0.000%	0	0
⊟ 802.11 Data	0.000%	0	0
⊟ SNAP	0.000%	0	0
⊟ IP	0.000%	0	0

Figure 9.4 Node Detail Statistics window.

Note: Node **Detail Statistics** windows show both sent and received traffic, regardless of the settings in the main **Node Statistics** window.

Protocol statistics

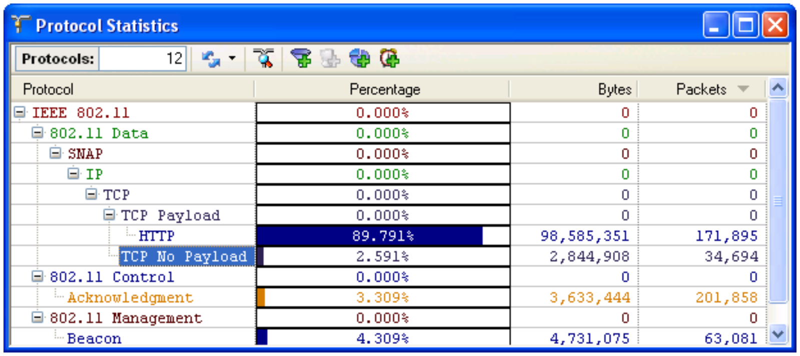
To open the **Protocol Statistics** window, choose **Protocols** from the **Monitor** menu or press **Ctrl + 2**.

The **Protocol Statistics** window shows network traffic volume, in packets and in bytes, broken down by protocol and sub-protocol.

This window is useful in determining which protocols or sub-protocols are generating a high percentage of the overall network traffic.

The ***Percentage*** bar graph represents the percentage of bytes for each protocol and sub-protocol type.

The ***Bytes*** column shows the total bytes used by that protocol. The ***Packets*** column displays the number of packets transmitted and received by all nodes combined for that protocol.



Protocols: 12

Protocol	Percentage	Bytes	Packets
IEEE 802.11	0.000%	0	0
802.11 Data	0.000%	0	0
SNAP	0.000%	0	0
IP	0.000%	0	0
TCP	0.000%	0	0
TCP Payload	0.000%	0	0
HTTP	89.791%	98,585,351	171,895
TCP No Payload	2.591%	2,844,908	34,694
802.11 Control	0.000%	0	0
Acknowledgment	3.309%	3,633,444	201,858
802.11 Management	0.000%	0	0
Beacon	4.309%	4,731,075	63,081

Figure 9.5 Protocol Statistics window

The *Protocols* item at the top of the display shows the total number of different protocols encountered.

To change the sort order, click in the heading of the column by which you want to sort the display to toggle between ascending and descending order. The order is indicated by a small triangle pointing up or down, shown in the header of the column by which the display is sorted.

If you intend to keep the window open for some length of time, you may want to select a longer refresh interval. You can set the refresh interval for this window by using the drop-down list at the top of the display. This applies only to refresh of the display, as calculation goes on continuously in the background. Nevertheless, longer refresh intervals do save processing time for other tasks, such as processing packets. You can click the **Refresh** button in the window header at any time to immediately refresh the display.

ProtoSpecs™

ProtoSpecs™ is an exclusive feature that quickly and accurately identifies the protocols nested within 802.11 WLAN packets.

ProtoSpecs use multiple identifiers within a packet to create a tree-structure that specifies a top-level or parent protocol (such as IP) and sub-protocols that it contains (such as FTP or SNMP). The protocol list in the **Protocol Statistics** window uses a hierarchical structure. Click the + plus sign preceding a name to see additional levels of protocol detail, or right-click to access the context menu, presenting choices which allow you to expand or collapse the entire protocol list.

ProtoSpecs recognize hundreds of different protocols and sub-protocols. Nevertheless, there are still some protocols that are not identified by name in the program. AiroPeek will list unidentified LSAP (one-byte) and SNAP (five-byte) protocol types by their numeric value in hexadecimal. You may add these to the Name Table to assign them a symbolic name.

When AiroPeek cannot identify a sub-protocol, it lists the protocol with other unidentified types at the highest known protocol level. For example, UDP port 1378, which is reserved for the Elan License Manager, is not uniquely identified by AiroPeek. Instead, the packet statistics associated with this protocol are collected under the identified name of UDP protocol statistics.

For a more detailed look at protocols: what they are, how they work, and how they are handled in AiroPeek, see Appendix A, “Packets and Protocols” on page A-3.

You can add new protocol discrimination definitions to the ProtoSpecs hierarchy by editing the associated PSpecs.xml file in accordance with its schema, PSpecs.xsd. Both of these files are located in the same directory as the AiroPeek program file. Additional instructions for adding new protocol discriminators to the ProtoSpecs hierarchy can be found in a file called ProtoSpecsXML.pdf, located in the Documents directory under the directory in which you installed AiroPeek.

Note: ProtoSpecs protocol discriminators test for particular values at specified locations (offset, or offset and mask) within packets. They also rely on the hierarchical relationship between protocols (encapsulation) for proper functioning. Writing protocol discriminators requires a good understanding of protocol characteristics and packet structure, as well as some knowledge of XML syntax.

Protocol information

For a quick refresher on the meaning and usage of a particular protocol or sub-protocol, highlight the protocol in any window where it is shown, right click and choose **Protocol Info…** from the context menu. Brief descriptions of hundreds of protocols and sub-protocols are stored here for ready reference.

Protocol utilization statistics

When the hierarchical view is collapsed (with a plus sign + in front of the protocol name), the utilization statistics show the sum of all sub-protocols within that protocol. When the hierarchical view is expanded (with a minus sign - in front of the protocol name), utilization statistics are broken out by individual sub-protocol. The top-level protocol (such as IP) then shows statistics only for itself and for any sub-protocols that seem to be a part of the top-level protocol, but that are not uniquely defined by ProtoSpecs. Statistics that do not belong to any of the recognized sub-protocols are added to the totals for the parent protocol. This allows statistics for unrecognized sub-protocols to be included in the totals with as much precision as possible.

Viewing details for a protocol

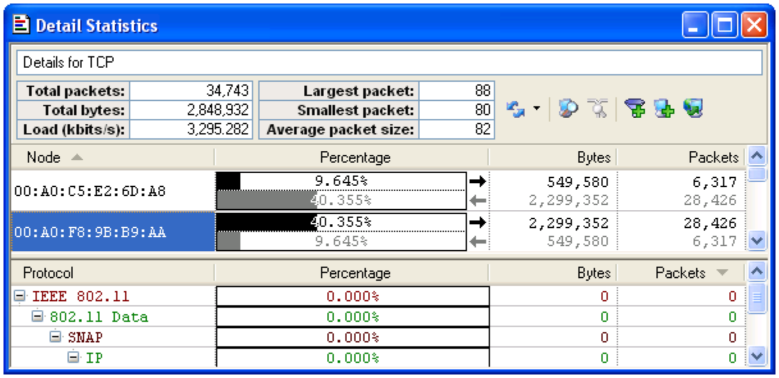
To view more detail about the traffic in a particular protocol or sub-protocol, double-click the protocol or sub-protocol name. This opens a **Detail Statistics** window.

This window displays more detail about nodes generating the selected protocol. The additional detail includes:

- Details for nodes communicating in this protocol (and its sub-protocols, if any).
- The relative percentage of traffic represented by any sub-protocols.
- The *Total packets* and *Total bytes* of traffic for this protocol.
- Network *Load (kbits/s)* used by the protocol (and its sub-protocols, if any).
- *Largest packet*, *Smallest packet* and *Average packet size* for the protocol.

The bar graph in this detail window lists all nodes receiving or sending packets of the selected protocol type, their respective percentage share of the protocol traffic, and the number of packets that percentage represents.

Click the **Refresh** button to update the display. Alternatively, you can use the **Refresh** drop-down list to set a refresh interval for the **Detail Statistics** window.



Details for TCP

Total packets:	34,743	Largest packet:	88
Total bytes:	2,848,932	Smallest packet:	80
Load (kbits/s):	3,295.282	Average packet size:	82

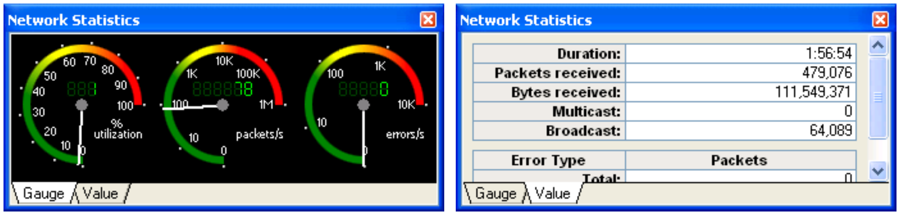
Node	Percentage	Bytes	Packets
00:A0:C5:E2:6D:A8	9.645% 40.355%	549,580 2,299,352	6,317 28,426
00:A0:F8:9B:B9:AA	40.355% 9.645%	2,299,352 549,580	28,426 6,317

Protocol	Percentage	Bytes	Packets
⊟ IEEE 802.11	0.000%	0	0
⊟ 802.11 Data	0.000%	0	0
⊟ SNAP	0.000%	0	0
⊟ IP	0.000%	0	0

Figure 9.6 Protocol Detail Statistics window

Network statistics

To open the **Network Statistics** window, choose **Network** from the **Monitor** menu or press **Ctrl + 3**.



Duration:	1:56:54
Packets received:	479,076
Bytes received:	111,549,371
Multicast:	0
Broadcast:	64,089

Error Type	Packets
Total:	0

Figure 9.7 Network Statistics window, Gauge and Value views

The default ***Gauge*** view of the **Network Statistics** window shows network utilization (as a percent of capacity), traffic volume (in packets per second), and error rate (total errors per second) as analog dials with corresponding digital displays at their centers.

The ***Value*** tab at the bottom of the window opens an alternate view showing two tables. The first shows duration, traffic volumes and utilization. The lower table shows counts of CRC error packets. The upper table lists five parameters that show total counts from the time AiroPeek began collecting Monitor statistics to the current second. They are:

Duration — This parameter shows elapsed time in “days: hours: minutes: seconds:” format since you started collecting Monitor statistics.

Packets received — This parameter shows packets received since you started collecting Monitor statistics.

Bytes received — This parameter shows bytes received since you started collecting Monitor statistics.

Multicast — This parameter shows packets addressed to multicast addresses since you started collecting Monitor statistics.

Broadcast — This parameter shows packets addressed to broadcast addresses since you started collecting Monitor statistics.

The lower table in the ***Value*** view of the **Network Statistics** window shows error counts for *Total Errors* since you began collecting Monitor statistics.

Error types and error packets

AiroPeek recognizes only the CRC error type, shown in the table below:

Table 9.4 Error Types

Error Type	Description
CRC Error	At the end of the packet, four bytes are transmitted which force the checksum to a known constant. If the receiving end does not compute the same constant after receiving the four bytes, the packet must have been corrupted. A CRC error occurs when the CRC (Cyclic-Redundancy Check) fails. These bytes are referred to as a Frame Check Sequence or FCS.

Size statistics

To open the **Size Statistics** window, choose **Size** from the **Monitor** menu or press **Ctrl + 4**.

The *Packet Size Distribution* graph sets up size classes for packets (their length in bytes) and shows what percentage of the packets on the network are in each size class.

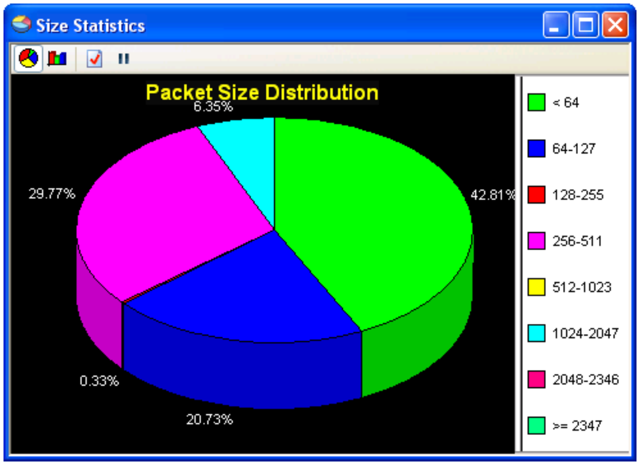


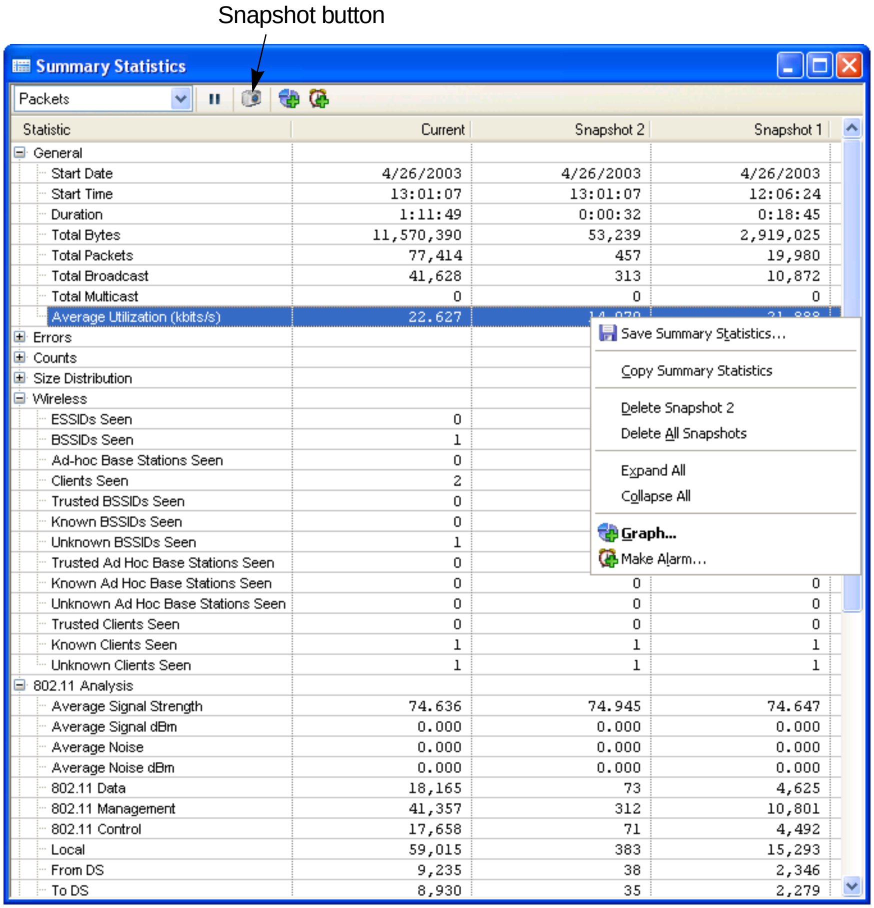
Figure 9.8 Size Statistics window

You can choose a bar chart or a pie chart display format by clicking the **Pie** chart or the **Bar** chart button in the upper left hand corner of the **Size Statistics** window. Click the **Options** button to choose additional options for color, borders, and three-dimensional or two-dimensional display. Click the **Pause** button to temporarily suspend chart updates.

Summary statistics

To open the **Summary Statistics** window, choose **Summary** from the **Monitor** menu or press **Ctrl + 5**.

The **Summary Statistics** window allows you to monitor key network statistics in real-time and save those statistics for later comparison. To create a new Summary Statistics Snapshot, click the **Snapshot** button at the top of the window. The new column labeled *Snapshot 1* will appear immediately to the right of the column labeled *Current*. Any previous snapshots will be pushed further to the right, so that the most recent (highest numbered) is next to the current statistics. If you had three snapshots, for example, the columns, reading from left to right, would be named *Snapshot 3*, *Snapshot 2*, *Snapshot 1*. To delete a particular snapshot, right-click in the column you wish to delete and choose **Delete Snapshot #** (where # is the number of the particular snapshot). Alternatively, you can choose **Delete All Snapshots** to clear all.



Statistic	Current	Snapshot 2	Snapshot 1
⊟ General			
Start Date	4/26/2003	4/26/2003	4/26/2003
Start Time	13:01:07	13:01:07	12:06:24
Duration	1:11:49	0:00:32	0:18:45
Total Bytes	11,570,390	53,239	2,919,025
Total Packets	77,414	457	19,980
Total Broadcast	41,628	313	10,872
Total Multicast	0	0	0
Average Utilization (kbits/s)	22.627	14,070	21,888
⊞ Errors			
⊞ Counts			
⊞ Size Distribution			
⊟ Wireless			
ESSIDs Seen	0		
BSSIDs Seen	1		
Ad-hoc Base Stations Seen	0		
Clients Seen	2		
Trusted BSSIDs Seen	0		
Known BSSIDs Seen	0		
Unknown BSSIDs Seen	1		
Trusted Ad Hoc Base Stations Seen	0		
Known Ad Hoc Base Stations Seen	0	0	0
Unknown Ad Hoc Base Stations Seen	0	0	0
Trusted Clients Seen	0	0	0
Known Clients Seen	1	1	1
Unknown Clients Seen	1	1	1
⊟ 802.11 Analysis			
Average Signal Strength	74.636	74.945	74.647
Average Signal dBm	0.000	0.000	0.000
Average Noise	0.000	0.000	0.000
Average Noise dBm	0.000	0.000	0.000
802.11 Data	18,165	73	4,625
802.11 Management	41,357	312	10,801
802.11 Control	17,658	71	4,492
Local	59,015	383	15,293
From DS	9,235	38	2,346
To DS	8,930	35	2,279

Figure 9.9 Summary Statistics window, showing context menu for Snapshot 2

Use the snapshot feature to baseline normal network activity, save the data as a snapshot, and then compare these saved statistics with those observed during periods of erratic network behavior to help pinpoint the cause of the problem.

Summary statistics are also extremely valuable in comparing the performance of two different BSSs or two different networks. For example, a field support engineer could compare the real-time statistics on a client’s network with a saved healthy snapshot and easily diagnose or eliminate the source of inconsistent or poor performance.

Click on the plus sign + or minus sign - in the margins beside the major headings to expand or collapse the view of that section of the hierarchy. Details are hidden when the hierarchy is collapsed and no summary of those hidden details is provided at higher levels. Right-click to bring up a context menu with options to **Expand All** or **Collapse All** hierarchical items.

To set the display units for the **Summary Statistics** window, choose from the drop-down list in the upper left. Your choices are: *Packets*, *Bytes*, *Percent of Packets*, *Percent of Bytes*, *Packets per second*, or *Bytes per second*.

Tip When you have a supported adapter selected, the **Summary Statistics** window also displays *Driver* statistics detailing performance of the adapter itself. This is only available for Monitor statistics, and is not shown in the ***Summary*** view of Capture windows or Packet File windows.

History statistics

To open the **History Statistics** window, choose **History** from the **Monitor** menu or press **Ctrl + 6**.

The **History Statistics** window shows a graph of network performance at selected intervals over time. You can choose to measure that performance as *Utilization* (percent of capacity as set in the **Network Speed** dialog), or as *Packets/second* or *Bytes/second* by choosing from the drop-down list in the upper left of the **History Statistics** window, as shown in Figure 9.10. The scale at the left can be fixed, or it can be dynamically adjusted to cover only the range of values encountered so far.

You can choose how the historical data is displayed by selecting a sampling interval from the drop-down list. The drop-down list sets the displayed sampling interval for the **History Statistics**. The choices are described in Table 9.5.

Table 9.5 **History statistics sampling intervals**

Sampling Interval	Description
1 sec. / 30 min.	Takes the average over every one second to produce a graph that covers a total of 30 minutes.
5 sec. / 2 hr.	Takes the average over every five seconds to produce a graph that covers a total of two hours.

Table 9.5 History statistics sampling intervals (continued)

Sampling Interval	Description
15 sec. / 6 hr.	Takes the average over every 15 seconds to produce a graph that covers a total of six hours.
30 sec. / 12 hr.	Takes the average over every 30 seconds to produce a graph that covers a total of 12 hours.
60 sec. / 24 hr.	Takes the average over every one minute to produce a graph that covers a total of 24 hours.

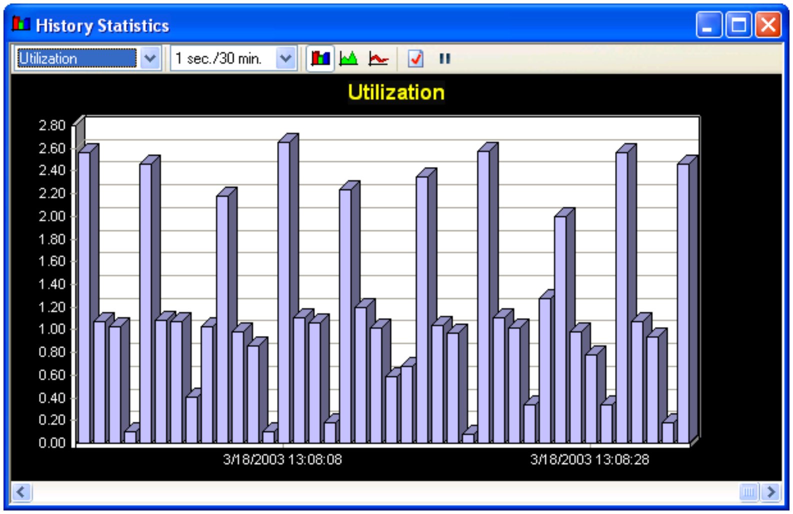
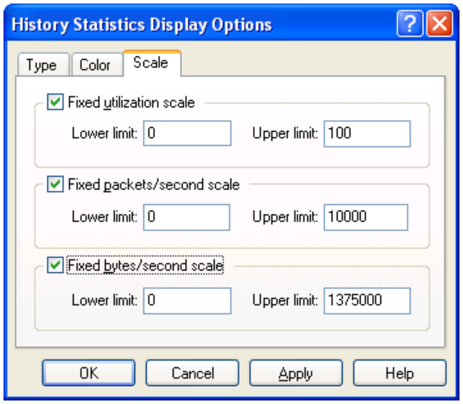


Figure 9.10 History Statistics

The first three buttons to the right of the interval drop-down list show: a bar graph, a filled line graph, and an ordinary line graph. You can quickly change the display format of the **History Statistics** to any one of these formats by clicking on its button.



☑ Fixed utilization scale
Lower limit: 0 Upper limit: 100

☑ Fixed packets/second scale
Lower limit: 0 Upper limit: 10000

☑ Fixed bytes/second scale
Lower limit: 0 Upper limit: 1375000

Figure 9.11 Scale view of the History Statistics Display Options dialog

The last two buttons at the far right of the **History Statistics** window are the **Options** button and the **Pause** button. The **Pause** button, at the far right, temporarily stops the otherwise continuous scrolling of the display. Click the **Pause** button when you want to go back and review an earlier time segment and temporarily suspend screen updates and the scrolling they entail. Calculations will go on uninterrupted in the background. Scrolling will resume when you unclick the **Pause** button or when you close and re-open the **History Statistics** window.

The **Options** button is the second button in from the right of the row of buttons, immediately to the left of the **Pause** button. This button opens the **History Statistics Display Options** dialog, where you can set the appearance of the History Statistics graph. The **History Statistics Display Options** dialog has three views, ***Type***, ***Color***, and ***Scale***, accessible by clicking their respective tabs. The first two views are common to other statistics display options and are described elsewhere. For details on the ***Type*** and ***Color*** views, please see “Controlling the graph display” on page 196.

The ***Scale*** view, shown in Figure 9.11, allows you to use a fixed scale (checked) or a dynamically adjusted scale based on the largest values seen so far (unchecked), for each of three parameters: *Utilization*, *Packets/second*, and/or *Bytes/second*. Use the text entry boxes to set a *Lower limit* and an *Upper limit* for any enabled fixed scale. Click **Apply** to see the effect of your changes. Click **OK** to accept the changes, or click **Cancel** to close the dialog without making any changes.

Channel statistics

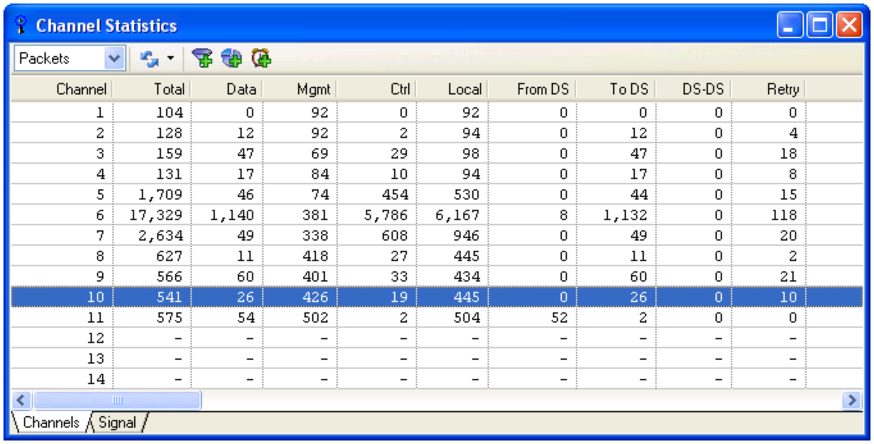
To open the **Channel Statistics** window, choose **Channel** from the **Monitor** menu or type **Ctrl + 7**. The **Channel Statistics** window has two views: ***Channels*** and ***Signal***, available by clicking the labeled view tabs at the bottom of the window.

Note: In North American implementations of the 802.11g and 802.11b WLAN protocols, channels 12 through 14 are not used.

Channels view of channel statistics

The ***Channels*** view of the **Channel Statistics** window (Figure 9.12) shows a variety of statistics and counts for each channel, laid out in a tabular form. Use the units drop-down list to display information by *Packets*, *Bytes* or *Both*. If you choose *Both*, the display will show two columns, one for bytes and one for packets, where that is appropriate.

You can add or remove columns from the ***Channels*** view or rearrange their order. To add or remove columns from the view, right click anywhere in the column headers and select from the context menu. Columns shown in the ***Channels*** view have a checkmark beside their entry in the context menu. Click on the name of any column in this context menu to toggle its display on or off. To change the order of columns, use drag and drop in the ***Channels*** view. A complete list of the available columns and a brief description of their contents is shown in Table 9.6.



Channel	Total	Data	Mgmt	Ctrl	Local	From DS	To DS	DS-DS	Retry
1	104	0	92	0	92	0	0	0	0
2	128	12	92	2	94	0	12	0	4
3	159	47	69	29	98	0	47	0	18
4	131	17	84	10	94	0	17	0	8
5	1,709	46	74	454	530	0	44	0	15
6	17,329	1,140	381	5,786	6,167	8	1,132	0	118
7	2,634	49	338	608	946	0	49	0	20
8	627	11	418	27	445	0	11	0	2
9	566	60	401	33	434	0	60	0	21
10	541	26	426	19	445	0	26	0	10
11	575	54	502	2	504	52	2	0	0
12	-	-	-	-	-	-	-	-	-
13	-	-	-	-	-	-	-	-	-
14	-	-	-	-	-	-	-	-	-

View Tabs

Figure 9.12 Channel Statistics window, Channels view

You can sort the display by any column by clicking in the column header. Click again to reverse the sort order. Sort order is indicated by a triangle in the header of the column by which you are sorting. The triangle points in the direction of the sort.

Table 9.6 **Channels view available columns**

Column	Description
Channel	The number of the channel, indicating its center frequency. Note that channels are dependent on physical layer implementation, and are distinct for 802.11a WLANs and 802.11b WLANs. Channel use is also regulated by appropriate authorities in different regulatory jurisdictions, such as the FCC in the United States.
Total	Total of all traffic on the channel.
Data	Data packets.
Mgmt	Management packets.
Ctrl	Control packets.
Local	Local traffic, not associated with any Distribution System (DS). Includes Station to Station plus management and control packets. The TO DS and FROM DS bits are both set to 0.
From DS	Traffic from an access point (AP) being forwarded from the Distribution System (DS). The TO DS bit is set to 0 and the FROM DS bit is set to 1.
To DS	Traffic to an access point (AP), bound for the Distribution System (DS). The TO DS bit is set to 1 and the FROM DS bit is set to 0.
DS-DS	Traffic which has been handled by two access points, indicating that the packet was relayed through the Distribution System (DS). The TO DS and FROM DS bits are both set to 1.
Retry	Packets in which the Retry bit is set to 1, indicating the packet is a retransmission.
WEP	Packets in which the WEP bit is set to 1, indicating the packet payload is WEP encrypted.

Table 9.6 Channels view available columns (continued)

Column	Description
Order	Packets in which the Order bit is set to 1, requesting the contents be handled in strict order. Examples might include Voice over IP (VoIP).
Data Rate columns	Columns show the number of packets sent at the data rate named in the column header. You can show columns for any and all data rates supported by the current adapter. For additional information on data rates in 802.11 WLANs, please see “802.11 view of node statistics” on page 155.
[Data Rate] *Mbits/s*	Packets in which the data portion of the packet was transmitted at the specified data rate.
CRC Error	Packets with CRC errors. The CRC is a checksum performed over the whole packet. CRC errors indicate the packet was truncated or garbled in transmission. This is common in cases of channel overlap and interference.
WEP ICV	Packets containing WEP ICV Errors. The ICV is a checksum performed over the data portion of a WEP-encrypted packet. On an otherwise properly formed packet, a WEP ICV failure often means the WEP keys used to decrypt the packet are not the right ones. Packets with CRC errors will commonly show as also having WEP ICV errors.

Table 9.6 **Channels view available columns (continued)**

Column	Description
Signal Strength columns	A variety of columns showing statistics related to signal strength reported with each packet, expressed either as a percentage (***Min. Signal***, ***Max. Signal***, ***Cur. Signal***, and ***Avg. Signal***) or in decibel milliWatts (dBm) (***Min. Signal dBm***, ***Max. Signal dBm***, ***Cur. Signal dBm***, and ***Avg. Signal dBm***). Min. = Minimum signal strength reported on this channel from the time the statistics count was created until the most recent update. Max. = Maximum signal strength reported on this channel from the time the statistics count was created until the most recent update. Cur. = Most recently reported signal strength on the channel. Avg. = Average signal strength over the period of statistics collection on this channel. Calculated as the simple average of all reported signal strengths seen, regardless of duration.
Noise columns	A variety of columns showing statistics related to noise reported with each packet, expressed either as a percentage (***Min. Noise***, ***Max. Noise***, ***Cur. Noise***, and ***Avg. Noise***) or in decibel milliWatts (dBm) (***Min. Noise dBm***, ***Max. Noise dBm***, ***Cur. Noise dBm***, and ***Avg. Noise dBm***). Min. = Minimum noise reading reported on this channel from the time the statistics count was created until the most recent update. Max. = Maximum noise reading reported on this channel from the time the statistics count was created until the most recent update. Cur. = Most recently reported noise reading on the channel. Avg. = Average noise reading over the period of statistics collection on this channel. Calculated as the simple average of all reported noise readings seen, regardless of duration.
Created	Date and time at which this channel was first scanned for a signal, in the current session.
Updated	Date and time of the most recent scan of this channel, in the current session.

When the ***Channels*** view is active, you can save the channels statistics table to a tab-delimited text file by choosing **Save Channels Statistics…** from either the **File** menu or the context menu (right click).

Signal view of channel statistics

The ***Signal*** view of the **Channel Statistics** window (Figure 9.13) shows a continuously updated bar graph of the most recently reported signal strength, noise, or signal to noise comparison on every channel on which traffic is detected. You can temporarily suspend the update of the display by clicking the **Pause** button at the upper left of the ***Signal*** view. You can customize the color and appearance of the graph and change the value of the high and low thresholds using the **Signal Statistics Options** dialog, available by clicking the **Options** button at the top left of the ***Signal*** view.

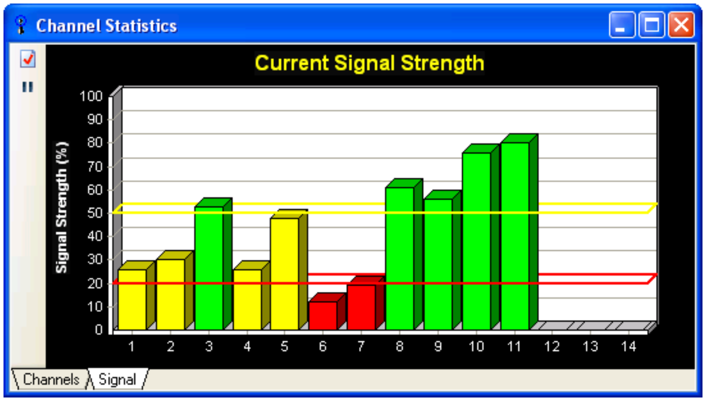


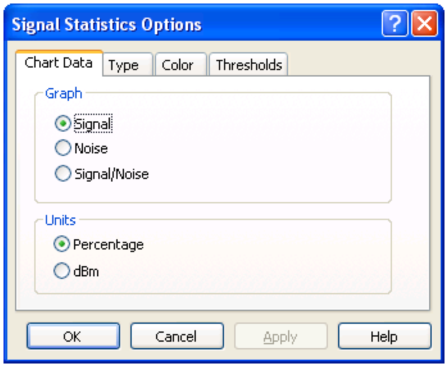
Figure 9.13 Channel Statistics window, Signal view

The graph in the ***Signal*** view shows two horizontal reference lines: an upper threshold and a lower threshold. You can change the location of these reference lines by changing the values they mark. The upper threshold must always be above the lower. That is, the upper threshold must always mark a higher signal strength. The color of a threshold reference line matches the color you assign to signal strengths falling immediately below that threshold.

Each bar in the ***Signal*** view represents the most recently reported signal strength on a particular channel. The color of the bar changes to show whether the reported signal strength is below the low threshold, between the high and low thresholds, or above the high threshold. By default, the colors associated with these values are set to red, yellow, and green, respectively. You can change the colors of the bars and set the value for the *Low* and *High* thresholds in the ***Thresholds*** view of the **Signal Statistics Options** dialog.

To open the **Signal Statistics Options** dialog, click the **Options** button at the top left of the ***Signal*** view. The **Signal Statistics Options** dialog has four views: ***Chart Data***, ***Type***, ***Color***, and ***Thresholds***. Click the labeled tabs to open any of these views.

The ***Chart Data*** view (Figure 9.14) lets you control the type of data presented in the ***Signal*** view, and the units used to express it. Use the radio buttons in the *Graph* section to choose the type of data to be displayed. You can choose *Signal*, *Noise*, or *Signal/Noise*. In the *Units* section, use the radio buttons to choose the units in which to display the data. Choose *Percentage* or *dBm*. The *Percentage* units show the RSSI (Receive Signal Strength Indicator), normalized to a percentage. The *dBm* units are decibel milliWatts. For more about signal strength measurements, please see “Signal and noise measurement” on page A-11.



Graph

● Signal
○ Noise
○ Signal/Noise

Units

● Percentage
○ dBm

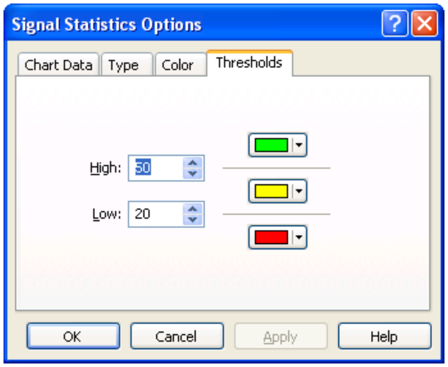
Figure 9.14 Signal Statistics Options dialog, the Chart Data view

Note: Reporting RSSI, the basis of the *Percentage* units of signal strength, is mandated by the 802.11 WLAN standards. Reporting signal and noise as dBm is not mandated, and is not supported by all cards. If the current adapter does not support dBm reporting, the ***Signal*** view will show readings of zero when *dBm* is selected for the *Units*. Change the *Units* to *Percentage* for these adapters.

The ***Type*** view lets you set whether the ***Signal*** view will use a *Three dimensional chart* for the bars and whether it will *Show borders* for them. Check the checkbox to enable these features.

The ***Color*** view lets you set the color of *items other than the bars and thresholds*. Click in the color boxes to open a palette of available colors for such items as background and text.

The ***Threshold*** view (Figure 9.15), lets you set the value of the *High* threshold and the *Low* threshold, and to set the colors for bars showing signal strengths which fall below the *Low* value, between the two, or above the *High* threshold value. Click the arrows beside the color swatches to open a palette of available colors.



High: 50

Low: 20

Figure 9.15 Signal Statistics Options dialog, Thresholds view

When you have made your changes to the **Signal Statistics Options** dialog, click **Apply** to see them immediately take effect, click **OK** to accept your changes and close the dialog, or click **Cancel** to close the dialog without making any changes.

When the ***Signal*** view of the **Channel Statistics** window is active, you can save the values shown for each channel to a text file by choosing **Save Signal Statistics…** from the **File** menu. The **Save Signal Statistics…** item also lets you save an image of the graph as a bitmapped image (*.bmp) or in Portable Network Graphic (*.png) format. You can also copy an image of the graph to the clipboard by typing **Ctrl + C** or by choosing **Copy** from the **Edit** menu. From the clipboard, you can paste the image into a document or an image editing program.

Statistics in capture windows

While Monitor statistics offer a continuous view of all network traffic on their selected adapter, Capture windows can be used to collect statistics on a more narrowly defined aspect of network traffic. Capture windows allow you to filter traffic before statistics are calculated, and they allow you to select groups of packets and save them for later analysis. Unlike Monitor statistics, Capture windows allow you to save and analyze individual packets. This can be crucial in understanding what certain nodes are attempting to do on the network, for example.

Please see Chapter 15, “Post-capture Analysis” on page 305, for a more detailed view of the analytical tools available for looking at traffic that has been captured and saved. This section just gives the basic distinctions between the statistics available in Monitor statistics and those available in Capture windows and Packet File windows.

Monitor vs. capture or packet file window statistics

The primary difference between Monitor statistics and those calculated in Capture windows or Packet File windows is that statistics in these windows are based on a subset of network traffic. If the capture options for a window are set to *Continuous capture* and the buffer has wrapped (that is, been emptied and begun to re-fill, or begun to overwrite older entries), statistics are still based on all packets seen since capture began, even though much of the traffic may no longer be visible in the ***Packets*** view. If packets are hidden using any of the Hide functions from the **Edit** menu, however, statistics are re-calculated based on the remaining, visible packets. Unhiding the packets will cause the statistics to once again be re-calculated.

Hide and Unhide have no effect on Monitor statistics.

Statistics in the views of a Capture window or a Packet File window are calculated based on the packets that are visible and in the buffer at the time the statistics are calculated. Filters can control what packets are placed in the buffer of a Capture window, and packet slicing can affect the contents of packets in either type of buffer. Please see “Using packet slicing” on page 61 for more information about packet slicing.

While you can create a new alarm from within any Capture window or Packet File window, the alarm itself will always watch Monitor statistics only. If **Monitor Statistics** is turned off, a message appears in the **Alarms** window warning you that alarms cannot function properly without Monitor statistics.

For creating reports of statistics from Capture windows or Packet File windows, please see “Saving reports from capture windows” on page 187. You can also periodically output statistics from any open Capture window using the ***Statistics Output*** view of the **Capture Options** dialog. Please see “Statistics output views” on page 188 for details.

Nodes

The ***Nodes*** view in a Capture window or in a Packet File window presents essentially the same view and provides the same customization features, detailed views, and calculations for the subset of traffic in its window that the Monitor statistics' **Node Statistics** window does for all traffic seen on the Monitor statistics adapter. Please see "Node statistics" on page 153 for details.

Protocols

The ***Protocols*** view in a Capture window or in a Packet File window presents essentially the same view and provides the same customization features, detailed views, and calculations for the subset of traffic in its window that the Monitor statistics' **Protocol Statistics** window does for all traffic seen on the Monitor statistics adapter. Please see "Protocol statistics" on page 163 for details.

Network statistics equivalents

There is no Network Statistics view for Capture windows or Packet File windows. The instantaneous measure of network performance makes no sense in a Packet File window, as no packets are being received. For Capture windows, however, the ***Graphs*** view lets you create one or more graphs that would show much the same information.

Error counts equivalents

There is no Error counter as such in Capture windows or Packet File windows. Error counts do appear in the ***Summary*** view, and advanced filters allow you to capture packets with CRC errors (see "Error filter nodes" on page 231). In addition, the ***Graphs*** view lets you graph any combination of statistics from the ***Summary*** view in a variety of formats.

Alternatively, after capture you could use the **Select Related Packets**, or the **Select…** function from the **Edit** menu to select only the types of error packets from a more heterogeneous group of captured traffic.

Size and history equivalents

The ***Graphs*** view of a Capture window or Packet File window provides a number of default graphs which present the same information for the subset of traffic in their window that the Monitor statistics' **Size Statistics** and **History Statistics** windows do for all traffic seen on the Monitor statistics adapter.

The default *Size* graph is equivalent to the **Size Statistics** display in Monitor statistics. Please see “Size statistics” on page 168 for details.

Most of the various functions of the **History Statistics** window in Monitor statistics are covered in two default graphs in the ***Graphs*** view: *Bytes/Second*, and *Packets/Second*. Please see “History statistics” on page 171 for more details.

For more information about the ***Graphs*** view, please see “Graphs view of capture windows and packet file windows” on page 201.

Summary

The ***Summary*** view in a Capture window or in a Packet File window presents essentially the same view and provides the same customization features, detailed views, and calculations for the subset of traffic in its window that the Monitor statistics’ **Summary Statistics** window does for all traffic seen on the Monitor statistics adapter. The ***Summary*** view does not show the *Driver* statistics item, however. Please see “Summary statistics” on page 169 for details.

Channel

The ***Channels*** view in a Capture window or in a Packet File window presents essentially the same view and provides the same customization and other features for the subset of traffic in its window that the ***Channels*** view of the Monitor statistics’ **Channel Statistics** window does for all traffic seen on the Monitor statistics adapter. Note that the ***Signal*** view for Capture windows and Packet File windows is a separate view. Please see “Channels view of channel statistics” on page 174 for details.

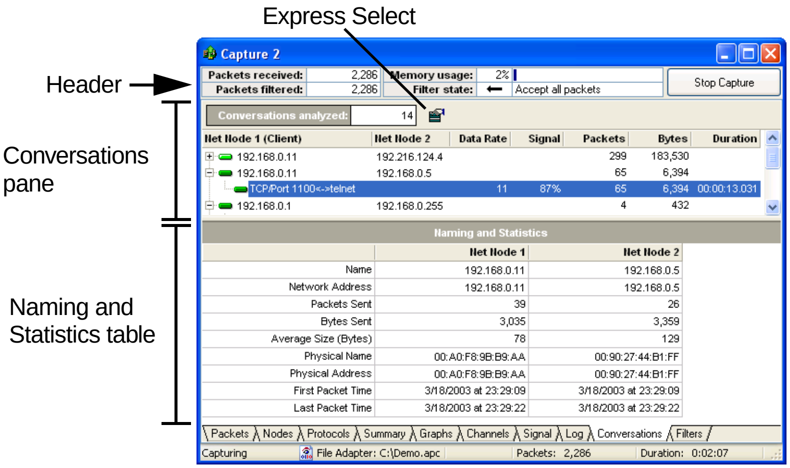
Signal

The ***Signal*** view in a Capture window or in a Packet File window presents essentially the same view and provides the same customization and other features for the subset of traffic in its window that the ***Signal*** view of the Monitor statistics’ **Channel Statistics** window does for all traffic seen on the Monitor statistics adapter. Please see “Signal view of channel statistics” on page 178 for details.

Conversations

The ***Conversations*** view in a Capture window or in a Packet File window has no equivalent in Monitor statistics, and is unique to AiroPeek standard.

The ***Conversations*** view (Figure 9.16) groups traffic in a Capture window or Packet File window into conversations between pairs of network nodes. The ***Conversations*** view presents information about each conversation in tabular form in the upper Conversations pane, and additional information about each peer in the selected conversation in the *Naming and Statistics* table in the lower pane.



Packets received:	2,286	Memory usage:	2%	
Packets filtered:	2,286	Filter state:	⟵	Accept all packets

Conversations analyzed: 14

Net Node 1 (Client)	Net Node 2	Data Rate	Signal	Packets	Bytes	Duration
192.168.0.11	192.216.124.4			299	183,530	
192.168.0.11	192.168.0.5			65	6,394	
TCP/Port 1100<->telnet		11	87%	65	6,394	00:00:13.031
192.168.0.1	192.168.0.255			4	432	

Naming and Statistics

	Net Node 1	Net Node 2
Name	192.168.0.11	192.168.0.5
Network Address	192.168.0.11	192.168.0.5
Packets Sent	39	26
Bytes Sent	3,035	3,359
Average Size (Bytes)	78	129
Physical Name	00:A0:F8:9B:B9:AA	00:90:27:44:B1:FF
Physical Address	00:A0:F8:9B:B9:AA	00:90:27:44:B1:FF
First Packet Time	3/18/2003 at 23:29:09	3/18/2003 at 23:29:09
Last Packet Time	3/18/2003 at 23:29:22	3/18/2003 at 23:29:22

Capturing | File Adapter: C:\Demo.apc | Packets: 2,286 | Duration: 0:02:07

Figure 9.16 Conversations view of a Capture window in AiroPeek standard

The header section of the ***Conversations*** view shows the number of *Conversations*. To the right of this information is the **Express Select** button. Click the **Express Select** button to use the currently selected conversation as the basis for a **Select Related Packets** selection in the ***Packets*** view.

The Conversations pane of the ***Conversations*** view shows the current conversations, with information about each conversation displayed in a user-definable set of columns. Right-click in the Conversations pane to open the context menu and choose **Visible columns…** to select the columns you wish to display. Use drag and drop to change column order. To use drag and drop, click on a column heading, then drag the ghost image of the column heading to a new location and release the mouse button. The columns available in the Conversations pane of the ***Conversations*** view are shown in Table 9.7. Columns present in the default Conversations pane layout show an **X** in the **Default** column of Table 9.7.

Table 9.7 **Conversations view, conversations pane columns**

Default	Column	Description
X	***Net Node 1 (Client)***	The client or first peer in the selected conversation.
X	***Net Node 2***	The server or second peer in the selected conversation.
	Protocol	The protocol under which the packets in this conversation were exchanged.
	Channel	The channel on which AiroPeek standard was listening when the current conversation was added.
X	***Data Rate***	The data rate at which the current conversation took place.
X	***Signal***	The signal strength at which the current conversation took place.
X	***Packets***	The number of packets in the selected exchange. Note that packet totals are rolled up when the view is collapsed, such that higher levels of aggregations show totals for all sub-elements.
X	***Bytes***	The total bytes represented by the packets which were a part of the selected conversation.
X	***Duration***	The elapsed time, from the first to the last packet of the selected exchange, represented in the form Hours:Minutes:Seconds:Milliseconds.

The Conversations pane of the ***Conversations*** view of a Capture window or Packet File window provides a hierarchical view of all conversations contained in the visible packets in the buffer of the window. Each highest-level item in the display represents a single node acting as the Client or first peer in a particular conversation. When a group of conversations differ only in port number, they are ranged below the Client node in order by port number.

Note: “Conversation” has a precise meaning in the ***Conversations*** view. For IP, the end-to-end IP address, and UDP or TCP ports form a unique conversation for a given application. For IPX, the end-to-end IPX address, socket number, and connection IDs form a unique conversation for a given application.

Items in the Conversations pane are color coded for easy scanning. When a conversation is still active, the color block beside that item is bright green. When the conversation is completed, the color block is dull green.

Click on the + (plus) or - (minus) signs at the left margin to expand or collapse individual elements of the display. Alternatively, you can right-click anywhere in the Conversations pane to open the context menu and choose either **Expand All** or **Collapse All**.

When one or more conversations are highlighted, you can use the context menu to **Select Related Packets** either **By Source and Destination**, which chooses packets with matching source and destination addresses, or **By Conversation**, choosing packets sent between two nodes in either direction, with the matching protocol and port.

The *Naming and Statistics* table shows additional details for the participants in the selected conversation, identified as ***Net Node 1*** and ***Net Node 2***. The *Naming and Statistics* table shows the characteristics described in Table 9.8 for both Net Node 1 and Net Node 2.

Table 9.8 Naming and Statistics table parameters

Parameter	Description
Name	The name (or address) of each node. The node is identified by its logical address or by the symbolic name for that address if one exists in the Name Table.
Network Address	The logical or physical address, as appropriate to the conversation.
Packets Sent	The total number of packets sent by this node as a part of this conversation.
Bytes Sent	The total number of bytes sent by this node as a part of this conversation.
Average Size (Bytes)	The average size of the packets sent by this node as a part of this conversation, in bytes.
Physical Name	The name (if any) associated with the physical address of this node. An example might be a WINS or NetBIOS name. If no such name is discovered in the traffic itself or found in the Name Table, the MAC address of the node will appear here.

Table 9.8 **Naming and Statistics table parameters (continued)**

Parameter	Description
Physical Address	The physical address of the node. Its MAC address.
First Packet Time	The date and time of capture (to the nearest second) of the first packet for this node in the current conversation.
Last Packet Time	The date and time of capture (to the nearest second) of the last packet for this node in the current conversation.

Output from statistics

You can save statistics to text files, print them out, or save them automatically to HTML or XML files using customized templates. Many graphical displays such as **Size Statistics** and the contents of the ***Graphs*** view of Capture windows can also be saved as images. This section describes the most important methods of saving statistics from Monitor statistics and from statistics functions in Capture windows and Packet File windows.

Saving statistics

When a statistics view other than **Network Statistics** is displayed in the front-most or active window, the **File** menu changes to **Save ___ Statistics…**, such as **Save Node Statistics…** or **Save Size Statistics…**, for example. You can choose to save the file as either a tab-delimited (*.txt) or a comma-delimited (*.csv) text file which can be read by most database, spreadsheet and charting programs. Statistics presented in graphical form, such as **Size** and **History** statistics, the ***Signals*** view of **Channel Statistics**, and any separately created **Graph** windows, can also be saved as an image of the current display in either a bitmapped (*.bmp) or Portable Network Graphic (*.png) format.

Saving reports from capture windows

When a Capture window or Packet File window is the active or front-most window, you can choose **Save Report…** from the **File** menu to create an integrated collection of documents in XML, HTML, or text formats, reporting statistics from that window. Note that statistics calculations in Capture windows and Packet File windows follow slightly different rules than those in Monitor statistics. Please see “Monitor vs. capture or packet file window statistics” on page 181 for details.

The *CSV Row Report* outputs the current **Summary** statistics in a single row. The statistics included in all other report formats are: **Node**, **Protocol**, and **Summary Statistics** (both current snapshot and all snapshots), and the statistics associated with any graphs in the ***Graphs*** view. See the sections at the end of this chapter for more details on the structure of each of these report output formats.

Use the drop-down list to choose a *Report type* and choose a *Report folder* in which to save the report. Click **Save** to create the specified report. The resulting XML or HTML reports are viewable in Internet Explorer 5.5 or compatible browsers.

Printing statistics

To print a statistics window or view, make it the front-most or active window and choose **Print…** from the **File** menu. You can access all standard printer functions from the **Print Setup…** command under the **File** menu. You can print any statistics window or details window except the **Network Statistics** window.

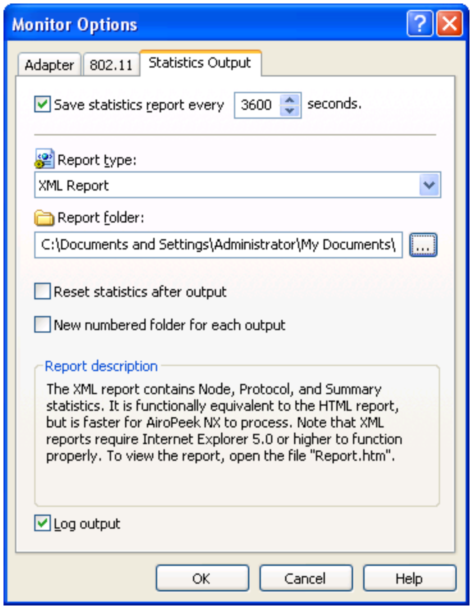
Statistics output views

Statistics from open Capture windows or open Monitor statistics windows can be periodically saved as XML, HTML or in a variety of text formats.

To periodically save a particular set of statistics to text, HTML, or XML files:

1. Open the source for the statistics: either the Monitor statistics windows or the Capture window whose statistics you want to save.
2. If your source is Monitor statistics, choose **Statistics Output…** under the **Monitor** menu to open the ***Statistics Output*** view of the **Monitor Options** window (Figure 9.17). If your source is a Capture window, open its **Capture Options** window and choose the *Statistics Output* tab to open the ***Statistics Output*** view. These views have the same name and offer identical choices. Only the source of statistics is different.
3. Click the checkbox in the upper left to enable saving statistics.
4. Set the frequency with which you want to update the statistics files, setting the interval in *seconds*.

5. Choose the report *Type* from the drop-down list. The *XML Report*, *HTML Report*, *Text Report (tab-delimited)* and *CSV Report (comma-delimited)* include all data from the **Node**, **Protocol**, and **Summary Statistics** windows or views. In addition, the tab-delimited (*.txt) and *.csv reports also include data from the **Size** and **History** statistics windows of Monitor statistics, or the statistics used by the graphs of the ***Graphs*** view of a Capture window. The *CSV Row Report* outputs the current **Summary** statistics in a single row, appending to the same file each time statistics are written. See the following sections for more details on the structure of each of these report output formats.



☑ Save statistics report every 3600 seconds.

Report type:
XML Report

Report folder:
C:\Documents and Settings\Administrator\My Documents\

□ Reset statistics after output

□ New numbered folder for each output

Report description
The XML report contains Node, Protocol, and Summary statistics. It is functionally equivalent to the HTML report, but is faster for AiroPeek NX to process. Note that XML reports require Internet Explorer 5.0 or higher to function properly. To view the report, open the file "Report.htm".

☑ Log output

Figure 9.17 Statistics Output view of the Monitor Options dialog

6. Choose an *Output folder* location for the statistics output.

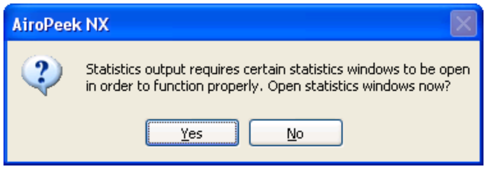
7. You can *Reset statistics after output* by checking the checkbox beside this item. Resetting statistics returns the counts to zero in the source of statistics (Monitor statistics or Capture window) and begins a fresh count. This is useful for creating a series of snapshots of network conditions.

8. You can create a *New numbered folder for each output* by checking the checkbox beside this item. When you choose this option, each time statistics are output, the resulting files are placed in a new folder within the directory you specified. The folders are numbered

sequentially, beginning with 001. If statistics are output more than 999 times, folder numbers will continue to increment with number 1000, 1001, 1002, and so forth. This option allows you to use any of the standard report types to create a complete data set. When this option is not enabled (unchecked), all reports other than the *CSV Row Report* will overwrite older entries each time statistics are output.

9. If you want a message placed in the global log file each time statistics are output, check the *Log output* checkbox at the bottom left of the dialog. Log entries include the path name of the output folder.

Note: Although you can enable the periodic output of Monitor statistics at any time, the output will only contain data if **Monitor Statistics** is enabled under the **Monitor** menu. The required statistics windows must also be open, although they may be reduced to icons. Similarly, periodic output from a Capture window can take place only when the window is open and capturing.



AiroPeek NX

Statistics output requires certain statistics windows to be open in order to function properly. Open statistics windows now?

Figure 9.18 Statistics output requires source windows to be open

10. When you have set the parameters for statistics output, click the **OK** button to accept your changes, or click **Cancel** to close the dialog without making any changes. When **Statistics Output…** is enabled, a ✔ checkmark appears beside that entry in the **Monitor** menu.

XML output

Choose *XML Report* from the *Type* drop-down list to output statistics as XML. The *XML Report* includes **Node**, **Protocol** and **Summary Statistics** information. When this report type is generated for a Capture window or Packet File window, it also includes statistics for all graphs in the ***Graphs*** view. The report is written to a file called StatsReport.xml in the directory you specified in *Output folder.* Supporting files are also written to this directory, including an HTML presentation of the data called Report.htm, the XSL style sheets used to present the report, and a copy of the XML Schema. You can view the formatted output in Report.htm in Internet Explorer, version 5.5 and above.

XML Report provides the same detail as the HTML output formats (except **History Statistics**), but with less processing demand on the program. In addition, XML provides a structured output for data interchange. For more detail about the structure of XML output, please see the Readme file located in the Reports directory where you installed AiroPeek and StatsReportSchema.xml, located in the Reports\Auxiliary subdirectory.

HTML output

The *HTML Report* includes **Node**, **Protocol**, **Summary** and **History Statistics** information. When this report type is generated for a Capture window or Packet File window, there are no **History Statistics** as such, but the report does include statistics for all graphs in the ***Graphs*** view.

AiroPeek outputs Monitor statistics to HTML files, one file for each statistics window or view. All of the output files are linked through a page called Stats.htm, and all are written to the directory you specified in *Output folder.* AiroPeek creates HTML files using templates. The HTML template contains keywords for the various parameters of each statistical display. These keywords are then replaced by the values returned by the statistics function each time it saves. The result is written to a standard HTML file and placed in the *Output folder* or directory of your choosing. You can use the templates supplied or create your own templates. Detailed instructions are included in the Readme file located in the Reports directory within the directory where you installed AiroPeek.

Text output

Choose *Text Report (tab-delimited)* from the *Type* drop-down list to output statistics as tab-delimited text (*.txt) or choose *CSV Report (comma-delimited)* to output text with comma separated values (*.csv). Either function creates files of the specified type, one for each statistics window or view, and places them in the directory you specified in *Output folder.* These text formats output **Node**, **Protocol**, **Summary**, **Size**, **History**, and **Channel** statistics for Monitor statistics. For output from Capture windows, periodic output in these formats includes statistics from the ***Nodes***, ***Protocols***, ***Summary***, and ***Channels*** views (one file per view) and from the ***Graphs*** view (one file per graph).

Row report

Choose *CSV Row Report (comma delimited)* to periodically append the current **Summary Statistics** data to a single named file. Unlike the other reports, the Row Report does not overwrite the target file when statistics are output. Instead it adds a new row to the end of the target *.csv file each time statistics are output. Each such row contains the whole contents of the ***Current*** column of the **Summary Statistics** window (or view) as comma-separated values. You can import CSV format files to spreadsheet and database programs for trending and other analysis.

Graphs of Monitor and Capture Statistics

In addition to the standard statistical displays of Monitor statistics and of Capture windows and Packet File windows, AiroPeek offers multiple methods for displaying individual statistical items or groups of items in user-defined graphs.

From creating instant graphs to defining complex suites of graphical displays, AiroPeek offers speed, power, and flexibility in the display of statistics. This chapter explains the tools for graphing statistics from Monitor statistics and from Capture windows and Packet File windows.

In this Chapter:

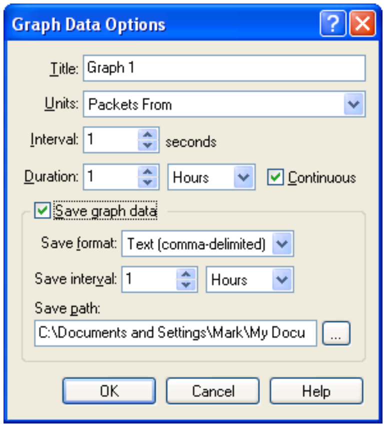
Creating and controlling graph windows

Individual items from the **Node**, **Protocol** and **Summary Statistics** windows and the ***Channels*** view of the **Channel Statistics** window (or from the analogous views of a Capture window) can be displayed graphically in real time. The data from these graphs can also be saved as tab-delimited or comma-delimited text, or as XML. This section describes how to create and modify the appearance of statistics graphs. The **Size** and **History Statistics** windows and the ***Signal*** view of the **Channel Statistics** window are displayed graphically by default. With the noted exceptions, what is said below about graph display options also applies to these windows.

Creating a new graph window

You can create a graphic view, updated in real time, of any item in the **Node**, **Protocol** or **Summary Statistics** windows (or from the analogous views of a Capture window) by selecting the item and clicking the **Graph** button at the top of the display.

Note: The **Graph Data Options** dialog will appear with added options in the lower half of the display when you create a new **Graph** window from items in a Capture window or Packet File window. These additional options relate to adding statistics items to the ***Graphs*** view of Capture windows or Packet File windows and are covered in their own section. Please see “Graphing statistics from capture and packet file windows” on page 199 for details.



Graph Data Options

Title: Graph 1

Units: Packets From

Interval: 1 seconds

Duration: 1 Hours ☑ Continuous

☑ Save graph data

Save format: Text (comma-delimited)

Save interval: 1 Hours

Save path: C:\Documents and Settings\Mark\My Docu

Figure 10.1 Graph Data Options dialog for Monitor statistics

To create a real-time graph of an item in a statistics display:

1. Open an appropriate statistics window or statistics view of a Capture window. You can create graphs of items in the **Node**, **Protocol** or **Summary Statistics** windows or from items in the analogous views of a Capture window.
2. Select the item you wish to graph and click the **Graph** button at the top of the statistics window (or view), or right click and choose **Graph…** from the context menu.
3. This opens the **Graph Data Options** dialog, shown in Figure 10.1. (The version of the **Graph Data Options** dialog presented when graphing a statistic from a Capture window offers additional options, but can be used as described here.)
4. Fill in the **Graph Data Options** dialog. The table below (Table 10.1) describes each of the parameters used to set up a statistics graph and to save data from it.
5. When you have chosen the parameters, click **OK** to create the new graph and begin displaying data, or click **Cancel** to close the dialog and return to the statistics display.

Table 10.1 Graph Data Options dialog parameters

Parameter	Usage
Title	The title of the graph.
Units	The units to be graphed. The dialog is aware of the statistic to be graphed, and will only present those units which make sense in context.
Interval	Enter a number to set the refresh and sampling interval, in *seconds*.
Duration	The total length of time to be covered by the graph. Choose units of *Minutes*, *Hours,* or *Days* from the drop-down list.
Continuous	If this checkbox is checked, the graph will represent a moving window of the size specified in *Duration* above. If the checkbox is unchecked, graphing will stop when the *Duration* time is reached.

Table 10.1 Graph Data Options dialog parameters (continued)

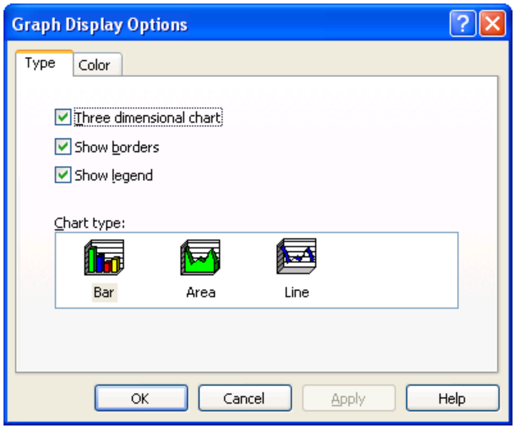
Parameter	Usage
Save graph data	Check this checkbox to enable the remainder of this dialog, specifying the format, interval and path with which to save graph data. Uncheck this checkbox to disable saving graph data.
Save format	Choose from the drop-down list one of the three supported formats: comma-delimited text (*.csv), tab-delimited text (*.txt), or XML (*.xml).
Save interval	Specify the frequency with which graph data is written to the specified file. Enter a number and use the drop-down list to choose units of *Minutes*, *Hours* or *Days*.
Save path	Choose the directory in which the graph data files should be saved. To browse, choose the button marked with the **…** ellipses.

Controlling the graph display

Statistics graphs, including the **History Statistics** graph, scroll each time data is refreshed so the most recent data appears at the far right of the screen. To temporarily suspend scrolling and make it possible to view data which has scrolled off-screen to the left, click the **Pause** button, located at the top of the **Graph** window.

Note: The scroll bar represents the position within a window of the size you set in the *Duration* parameter. For example, if you set a duration of one hour and have been graphing statistics for only ten minutes, only the right-most portion of the scroll bar will show any graphed data.

You can quickly change from one display type to another by clicking the icons representing **Bar**, **Area**, and **Line** display types, located at the top of the **Graph** window. For a finer control of the appearance of the graph, click the **Options** button at the top of the Graph window to open the **Graph Display Options** dialog, described below.



Graph Display Options

Type | Color

☑ Three dimensional chart

☑ Show borders

☑ Show legend

Chart type:

Figure 10.2 Graph Display Options dialog, Type view

Note: The ***Type*** and ***Color*** views of the **History Statistics Display Options**, **Signal Statistics Display Options** and **Size Statistics Display Options** dialogs are nearly identical to the **Graph Display Options** dialog, differing primarily in the choices of chart types available in each.

The **Graph Display Options** dialog presented for free-standing **Graph** windows has two tabs. From left to right, they are:

Type: Set the display format to *Bar* graph, *Area* graph or *Line* graph by choosing the appropriate labeled icon. The choice of graph types is context sensitive, and only those choices applicable to the graph being modified are available. You can also turn borders on or off by checking or unchecking the *Show borders* checkbox. Borders are on by default. Change the graph display from two dimensional to three-dimensional by checking the *Three dimensional chart* checkbox. Toggle the display of the key or legend by checking or unchecking the *Show legend* checkbox.

Color: Click in the color swatches to change the color of any of the listed display elements. Clicking in the swatch opens a small palette as a new window. Choose from this palette or click the **Other…** button at the bottom of the new window to open the **Color** dialog where you can create custom colors.

Click **Apply** to see the effect of your changes on the graph, click **OK** to accept changes, or click **Cancel** to return to the graph without making any changes.

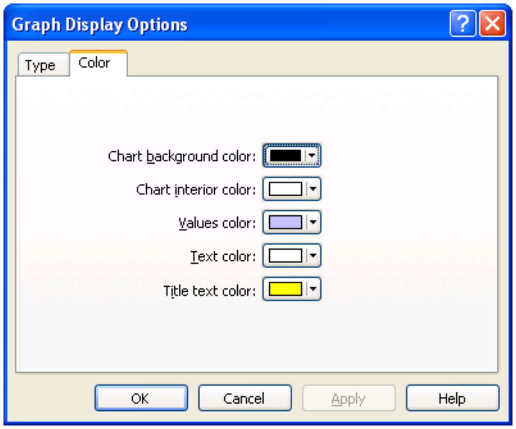


Chart background color: ■
Chart interior color: □
Values color: ▨
Text color: □
Title text color: ▨

Figure 10.3 Graph Display Options dialog, Color view

Saving graph windows

When a **Graph** window is the active or frontmost window, you can choose **Save Graph…** from the **File** menu to open a standard **Save As** dialog, from which you can save either the graph data or the current image of the **Graph** window itself. To save the graph data give the file a name, and choose a *Save file format* of *Text (tab delimited)(*.txt)*, *CSV (comma delimited)(*.csv)*, or *XML (*.xml)* from the drop-down list. To save the current image of the **Graph** window itself, give the file a name and choose either *Bitmap image (*.bmp)* or *PNG image (*.png)* from the *Save file format* drop-down list.

These options are separate from any settings you may have made in the **Graph Data Options** dialog to periodically *Save graph data*.

Monitor statistics graphs and alarms

Click the **Alarm** icon in the header of any statistics **Graph** based on Monitor statistics to create an alarm based on that statistic. Clicking on the **Alarm** icon opens the **Make Alarm** dialog where you can specify all characteristics of the alarm. Please see “Alarms” on page 242 for details.

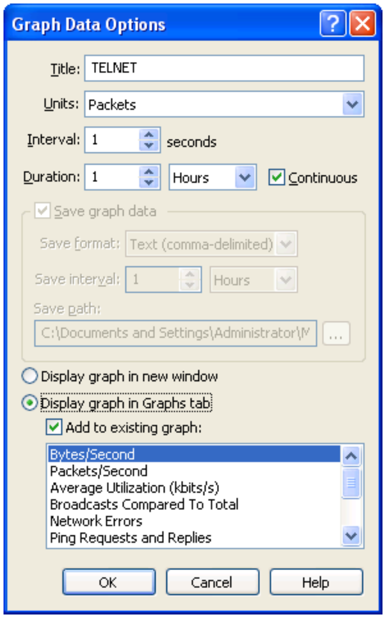
Important! Alarms only watch Monitor statistics. They never watch the statistics from a Capture window or Packet File window.

Graphing statistics from capture and packet file windows

You can graph any statistics item calculated in a particular Capture window or Packet File window in either of two basic ways:

- Create a new statistics **Graph** window showing just the selected statistic
- Create or add to a graph displayed in the ***Graphs*** view

In either case, the graph displays the statistics calculated in the Capture window or Packet File window from which it was created. The main distinction between the two types of graphs is in their formatting options and the ability to save and retrieve these formats.



Graph Data Options

Title: TELNET

Units: Packets

Interval: 1 seconds

Duration: 1 Hours ☑ Continuous

☑ Save graph data

Save format: Text (comma-delimited)

Save interval: 1 Hours

Save path: C:\Documents and Settings\Administrator\M

○ Display graph in new window

● Display graph in Graphs tab

☑ Add to existing graph:

Bytes/Second
Packets/Second
Average Utilization (kbits/s)
Broadcasts Compared To Total
Network Errors
Ping Requests and Replies

Options unique to Capture window or Packet File window statistics graphs

Figure 10.4 Graph Data Options dialog for Capture window or Packet File window statistics

To create a graph of a statistics item in the ***Nodes***, ***Protocols***, or ***Summary*** views of a Capture window or Packet File window, highlight the item and click the **Graph** button at the top of the display, or right-click and choose **Graph…** from the context menu. This opens the **Graph Data Options** dialog (Figure 10.4). Note that the top half of this dialog is identical to the dialog of the same name used to control graphs made from Monitor statistics. The bottom half presents options for adding the statistic to the ***Graphs*** view.

These options are unique to graphs created from Capture windows or Packet File windows.

Use the radio buttons to choose whether to *Display graph in new window* or *Display graph in Graphs tab.*

Display graph in new window

If you choose to *Display graph in new window*, your options are identical to those available in creating a similar new **Graph** window for a Monitor statistics item. Only the source of statistics is different. A new window is created, showing a single statistic. When you close the source of statistics (in this case, the Capture window or Packet File window), the **Graph** window disappears. A new **Graph** window created from a Capture window or Packet File window offers the same formatting and data saving options as a **Graph** window created for a Monitor statistics item. Please see “Creating and controlling graph windows” on page 194 for details.

Important! Alarms only watch Monitor statistics. They never watch the statistics from a Capture window or Packet File window. You cannot create an alarm based on a graph from a Capture window or Packet File window.

Adding a statistic to the graphs view

If you chose to *Display graph in Graphs tab*, you have two options. If you make no further selection, the new graph will be created and added to those listed in the ***Graphs*** view. Its name will be added to the list of graphs already displayed there. To see the graph, select its name from the list at the left side of the ***Graphs*** view. The graph will be displayed on the right.

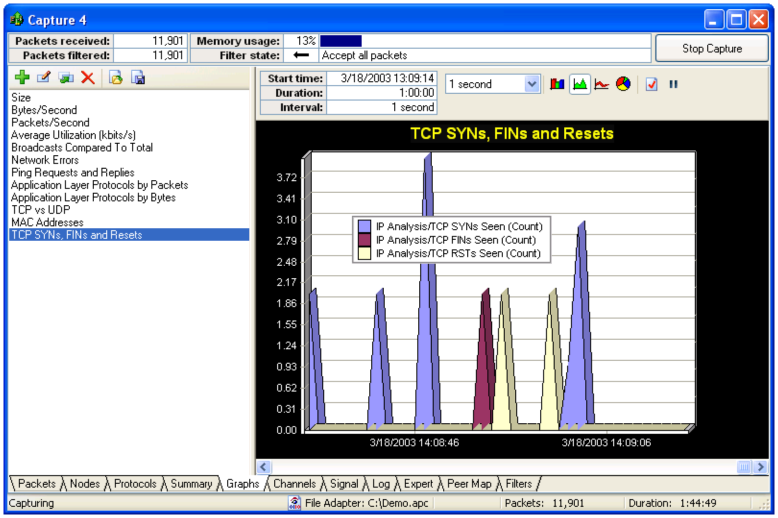
Alternatively, you can add the selected statistics item to one of the graphs that already exists in the ***Graphs*** view. Click the *Display graph in Graphs tab* radio button. Check the checkbox labeled *Add to existing graph*, and choose the target graph by highlighting its title in the list shown below. When you click the **OK** button, the statistics item you selected will be displayed under its default parameter name as a new item in the graph you selected. To view this item, select the title of the graph to which you added the statistic, using the list at the left of the ***Graphs*** view. The graph with the new statistics item will appear at the right. You can add up to 20 statistics items to a single graph in the ***Graphs*** view, although for ease of reading you may want to keep to a smaller number.

When you choose to *Display graph in Graphs tab*, the *Save graph data* section of the **Graph Data Options** dialog becomes grayed out. This is because, unlike separate **Graph** windows, the graphs in the ***Graphs*** view are treated as a part of the Capture window or Packet File window, and their data is saved using the same methods as other items in those windows. Briefly, you can use the **File** > **Save Report…** menu option for either Capture windows or Packet File windows. For Capture windows only, you can also use the ***Statistics Output*** view of the **Capture Options** dialog to set parameters for periodic output of statistics, including all statistics from graphs in the ***Graphs*** view. For details on these methods, please see “Output from statistics” on page 187.

Graphs view of capture windows and packet file windows

Click the *Graphs* tab to open the ***Graphs*** view (Figure 10.5) of any Capture window or Packet File window. The ***Graphs*** view contains four default graphs: *Size*, *Bytes/Second*, *Packets/Second*, and *Average Utilization (kbits/s)*.

The ***Graphs*** view allows great flexibility in the display of statistics. You can add to, delete, rearrange, create, edit, export, and import graphs of a wide range of formats, each based on single or multiple statistics from the current Capture window. This section explains how to manage graphs in the ***Graphs*** view.


Packets received: 11,901
Packets filtered: 11,901
Memory usage: 13%
Filter state: Accept all packets
Start time: 3/18/2003 13:09:14
Duration: 1:00:00
Interval: 1 second
1 second
Capturing
File Adapter: C:\Demo.apc
Packets: 11,901
Duration: 1:44:49

Capture 4
Stop Capture
Size
Bytes/Second
Packets/Second
Average Utilization (kbits/s)
Broadcasts Compared To Total
Network Errors
Ping Requests and Replies
Application Layer Protocols by Packets
Application Layer Protocols by Bytes
TCP vs UDP
MAC Addresses
TCP SYNs, FINs and Resets
TCP SYNs, FINs and Resets
3.72
3.41
3.10
2.79
2.48
2.17
1.86
1.55
1.24
0.93
0.62
0.31
0.00
IP Analysis/TCP SYNs Seen (Count)
IP Analysis/TCP FINs Seen (Count)
IP Analysis/TCP RSTs Seen (Count)
3/18/2003 14:08:46
3/18/2003 14:09:06
Packets
Nodes
Protocols
Summary
Graphs
Channels
Signal
Log
Expert
Peer Map
Filters

Figure 10.5 Graphs view of a Capture window showing TCP SYNs, FINs and Resets graph

The ***Graphs*** view is divided into a list pane on the left and a display pane on the right. The list pane presents the list of available graphs. The title of the currently visible graph is shown by a highlight in this list. The graph itself appears on the right. Select any title from the list to display that graph. Right-click on any title to open a context menu which mirrors the buttons at the top of the list pane. The buttons (or context menu items) and their functions are described in Table 10.2 below.

Table 10.2 Buttons in list pane of Graphs view

Button	Usage
Insert	Opens the **New Graph: Pick a Statistic** dialog, presenting above, a scrollable hierarchical list of all statistics in the ***Summary*** view, and below, a drop-down list for choosing the *Units* of display for the high-lighted statistics item. Choose any statistics item. If alternative units are possible for the selected item, you can choose them from the drop-down list. Click **OK** to add the new graph to the ***Graphs*** view.
Edit	Opens the **Graph Display Options** dialog for the selected graph.
Duplicate	Creates a copy of the selected graph and adds it to the list pane, with the word *Copy* added to its name.
Delete	Deletes the selected graph.
Import	When you click **Import**, the program first asks if you would like to *Delete all graphs before importing?* If you choose **Yes**, all the graphs currently shown in the ***Graphs*** view will be deleted and replaced by the contents of the imported *.gph file. If you choose **No**, the graphs you import will be added to the current list. Use the file **Open** dialog to navigate to the location of the *.gph file you wish to import, and click **OK**.
Export	You can export the entire contents of the ***Graphs*** view to a *.gph file, which is a set of parameters for defining all the graphs currently in the ***Graphs*** view. This allows you to create and maintain groups of graphs for particular troubleshooting tasks, or for particular environments.

Tip You can restore the default ***Graphs*** view by importing the Default Graph.gph file, located in the Graphs directory in the directory where you installed AiroPeek.

Controlling display of graphs in the graphs view

Graphs in the ***Graphs*** view have a standard basic layout.

A header section at the top of the display contains a drop-down list for setting the display interval, buttons for choosing a graph style, a **Pause** button to temporarily halt the scrolling of the display, and an **Options** button to open the **Graph Display Options** dialog for the graph. Some graphs may also show tabular data at the left of this header area, as appropriate to the statistics being displayed.

Tip You may need to increase the width of the Capture window or Packet File window in order to see all the items in the graph display pane header area.

Below this header area is the graph itself. You can choose whether the graph key or legend is displayed within the graph area or at the right side. Double-click in the legend to toggle its placement.

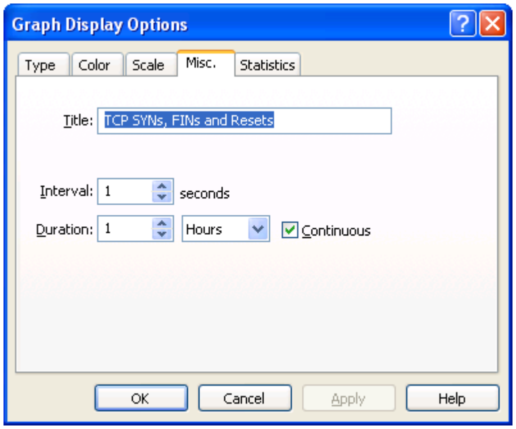
There are three basic sets of tools for controlling graph display. The first is the tools in the header section. The second is the **Graph Display Options** window, available by clicking the **Options** button in the graph display pane, or by clicking the **Edit** button in the list pane. The third is the **Chart FX Properties** dialog, available by double-clicking within any graph display.

The header options and the first two panes of the **Graph Display Options** dialog (the graph ***Type*** and ***Color*** views) are essentially identical to the analogous options for graphs created for Monitor statistics. Please see “Controlling the graph display” on page 196 for details. The remaining tools, the last three views of the **Graph Display Options** dialog and the **Chart FX** dialog, are unique to graphs created in the ***Graphs*** view of Capture windows and Packet File windows. These additional tools are described below.

Graph display options for the graphs view

The appearance of graphs is controlled by the **Graph Display Options** dialog. When graphs are displayed as a separate **Graph** window, this dialog only shows the first two tabs and views: ***Type*** and ***Color***. When graphs are displayed in the ***Graphs*** view, three more tabs or views are added to this dialog: ***Scale***, ***Misc.***, and ***Statistics***. These are described below.

The ***Scale*** view controls the scale used for the Y-axis (vertical scale) of the graph. Check the *Logarithmic* checkbox to plot the data against a logarithmic Y-axis. Check the *Fixed scale* checkbox and enter a *Minimum* and a *Maximum* value to force the Y-axis to this scale. If the *Fixed scale* checkbox is unchecked (the default), AiroPeek attempts to dynamically adjust the scale to match the data.



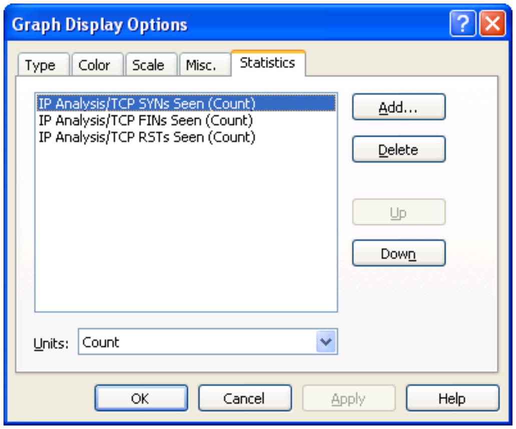
Title: TCP SYNs, FINs and Resets

Interval: 1 seconds

Duration: 1 Hours ☑ Continuous

Figure 10.6 Misc. view of the Graph Display Options dialog

Use the ***Misc.*** view to edit the *Title* of the graph, or set the sampling *Interval* by entering a number of *seconds*. You can set the *Duration* of the graph by entering a value in the text entry box and specifying the units (*Minutes*, *Hours*, or *Days*) by using the drop-down list. Check *Continuous* to restart collection when the *Duration* is reached, or leave *Continuous* unchecked to stop graphing when the *Duration* value is first reached. Note that the *Duration* sets the nominal width of the graph window.



IP Analysis/TCP SYNs Seen (Count)
IP Analysis/TCP FINs Seen (Count)
IP Analysis/TCP RSTs Seen (Count)

Units: Count

Figure 10.7 Statistics view of the Graph Display Options dialog

The ***Statistics*** view of the **Graph Display Options** dialog (Figure 10.7) presents a list of each statistics item displayed in the current graph. The drop-down list at the bottom of the display presents alternative choices for the *Units* used to measure the selected statistics item. If alternate units are available, you can choose them from this list.

Use the buttons at the right of the ***Statistics*** view to **Add…** a new statistics item to the list, to **Delete** an item, or to move the selected item **Up** or **Down** in the display. When you click the **Add…** button, it opens the **Add Statistic** dialog (Figure 10.8). This dialog presents a scrollable hierarchical list of all statistics in the ***Summary*** view, and below, a drop-down list for choosing the *Units* of display for the highlighted statistics item. Choose any item. If alternative units are possible, you can choose them from the drop-down list. Click **OK** to add the new statistics item to the list of those shown in the ***Statistics*** view.

Tip You can also add statistics items from the ***Nodes*** or ***Protocols*** views to any graph in the ***Graphs*** view. Please see “Adding a statistic to the graphs view” on page 200 for details.

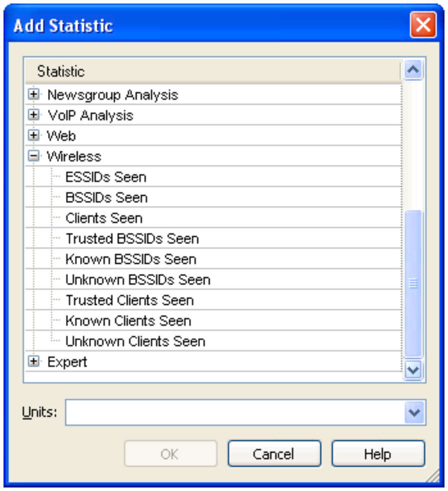


Figure 10.8 Add Statistic dialog

Chart FX display options in the graphs view

Double-click on the graph display area of any graph in the ***Graphs*** view to open the **Chart FX Properties** dialog for that graph. The **Chart FX Properties** dialog offers a wide range of tools for fine tuning and customizing the appearance of graphs and charts. The ***General*** view of the **Chart FX Properties** dialog lets you set styles for axes, grid lines and general appearance qualities such as color schemes and fill patterns. The ***Series*** view offers control over color and style for individual statistics items within a graph. The ***Axes*** view offers a range of options for controlling the appearance of tick marks, value labels, and so forth. The ***3D*** view can set angle, shading, and perspective for three-dimensional graph views.

Filters

This chapter describes how to create, edit, and use filters in AiroPeek. Filters work by testing packets against the criteria specified in the filter. Packets whose contents or other attributes meet these criteria are said to “match” the filter.

When you use a filter to limit the flow of packets into a Capture window, or to select packets already captured, you can specify whether you want to see all the packets that match the filter, or only those packets which do not match. You can also use a filter match as the test condition for a trigger that will start or stop capture in a Capture window.

Filters are so easy to create in AiroPeek that you can often create a custom filter on-the-fly while analyzing suspect traffic on your network and use that filter to narrow your search in real time.

Filters are discrete individual tools that can be saved, imported, exported, edited, and used in combination with one another. You can build filters to test for just about anything found in a packet: addresses, protocols, sub-protocols, ports, error conditions, and more. This chapter explains how.

In this Chapter:

Using filters

Filters are used to isolate particular types of traffic on the network for troubleshooting, analysis, and diagnostics. Filters can be used singly or in groups. If multiple filters are used together, AiroPeek treats them as being OR'ed together. That is, a packet matching any *one* of the enabled filters is treated the same as a packet that matched all.

Note: Filters never apply to Monitor statistics, which are always calculated on the basis of *all* network traffic. Filters can only be used either to restrict the flow of packets into a Capture window or to select packets already captured to a buffer, either in a Capture window or from a saved packet file in a Packet File window.

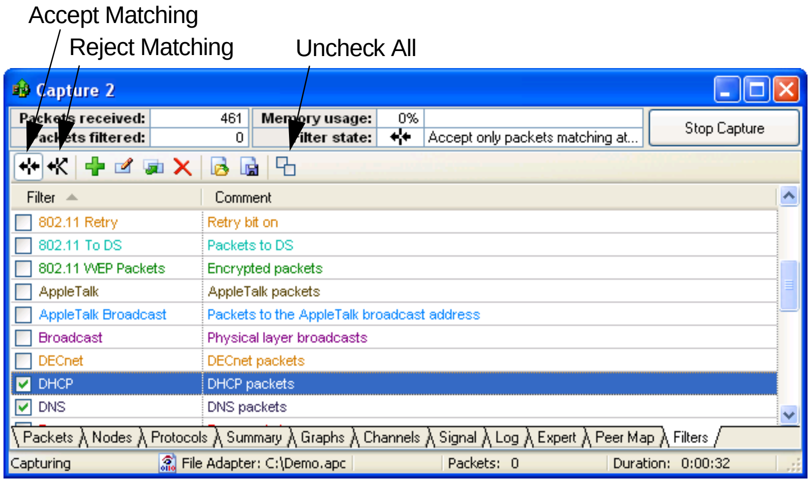
Enabling filters in a capture window

To set one or more filters to control capture into a particular Capture window

1. Click the *Filters* tab to open that window's ***Filters*** view (Figure 11.1).
2. Check to enable, or uncheck to disable, any listed filter(s).
3. Use the buttons at the top of the view to choose how the Capture window should apply the filters. Choose either to **Accept Matching** or to **Reject Matching** packets.

   When you enable multiple filters, they are logically OR'ed together. If you choose **Accept Matching**, only those packets matching any one of the selected filters are captured into the buffer. If you choose **Reject Matching**, packets matching any one of the enabled filters will be rejected, and only those packets not matching any of the enabled filters will be captured into the buffer.

   You can also set filters in the similar ***Filters*** view of the **Capture Options** dialog. All available filters are shown in all filter lists. Changes made in the ***Filters*** view of the Capture window take effect immediately. If you use the **Capture Options** dialog to manually change the filter settings for a Capture window, the changes take place only when you click **OK** to accept the dialog's settings. The ***Filters*** view of the **Capture Options** dialog allows you to include filter settings in capture templates and AutoCapture files.



Packets received: 461
Packets filtered: 0
Memory usage: 0%
Filter state: Accept only packets matching at...

	Filter	Comment
□	802.11 Retry	Retry bit on
□	802.11 To DS	Packets to DS
□	802.11 WEP Packets	Encrypted packets
□	AppleTalk	AppleTalk packets
□	AppleTalk Broadcast	Packets to the AppleTalk broadcast address
□	Broadcast	Physical layer broadcasts
□	DECnet	DECnet packets
☑	DHCP	DHCP packets
☑	DNS	DNS packets

Capturing | File Adapter: C:\Demo.apc | Packets: 0 | Duration: 0:00:32

Figure 11.1 Enabling filtering in a Capture window: the Filters view

To view the details of any particular filter, double-click on the filter to open it in its appropriate **Edit Filter** dialog. This displays that filter’s attributes, ready for editing. Click **Cancel** to close the filter without making any changes. For more details, see “Editing and duplicating filters” on page 213.

Tip You can create a filter testing for nearly any attribute of network traffic, including packet details, in a matter of two clicks using the **Make Filter** command. Please see “Make filter command” on page 211 for details.

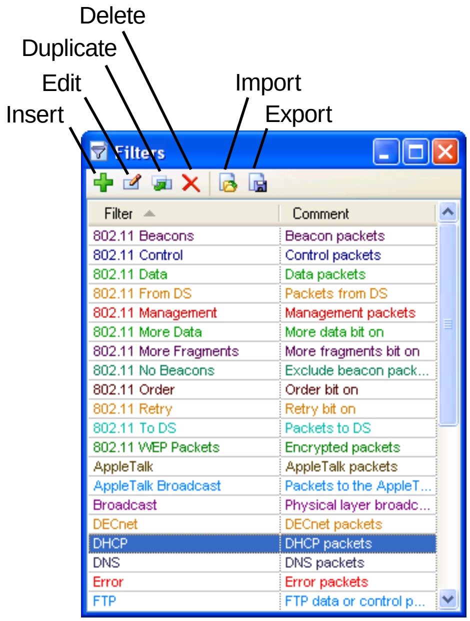
Using filters in a packet file window

Filters you create or import can be used as selection criteria in the **Select** dialog, available by choosing **Select…** from the **Edit** menu. For more on using the **Select** dialog, see “Select dialog: filters, analysis modules and more” on page 313.

Filter resources in AiroPeek

AiroPeek includes a number of resources for filtering packets. The central resource is the **Filters** window. To open the **Filters** window, choose **Filters** from the **View** menu or press **Ctrl + M**.

The **Filters** window lists all currently loaded filters. From the **Filters** window, you can create a new filter by clicking the **Insert** button. When one of the existing filters in the window is selected, you can use the buttons to **Edit**, **Delete**, or **Duplicate** that filter. You can **Export** to save existing filters to a file, or use the **Import** button to add the contents of any *.flt file to the existing filters. For a detailed discussion of each of these functions, please see “Creating and editing filters” on page 213.



Filter	Comment
802.11 Beacons	Beacon packets
802.11 Control	Control packets
802.11 Data	Data packets
802.11 From DS	Packets from DS
802.11 Management	Management packets
802.11 More Data	More data bit on
802.11 More Fragments	More fragments bit on
802.11 No Beacons	Exclude beacon pack...
802.11 Order	Order bit on
802.11 Retry	Retry bit on
802.11 To DS	Packets to DS
802.11 WEP Packets	Encrypted packets
AppleTalk	AppleTalk packets
AppleTalk Broadcast	Packets to the AppleT...
Broadcast	Physical layer broadc...
DECnet	DECnet packets
DHCP	DHCP packets
DNS	DNS packets
Error	Error packets
FTP	FTP data or control p...

Figure 11.2 Filters window

Ready-made filters

AiroPeek ships with a number of filters already made and loaded, by default, into the **Filters** window. These may be used as they are, or they can provide a start for creating your own more precise filters. The **Filters** window in Figure 11.2 shows the list of ready-made filters. These ready-made filters are in the file Default.flt in the Filters directory in the directory where you installed AiroPeek, and can be loaded into the **Filters** window using the **Import** button. Please see “Saving and loading filters” on page 232.

Simple filter

The ***Simple*** view (the default view) of the **Edit Filter** dialog allows you to create filters based on address, protocol, and/or port. Double-click on an existing simple filter or click the **Insert** button in the **Filters** window to open the ***Simple*** view of the **Edit Filter** dialog.

Advanced filter

Double-clicking on an existing advanced filter or choosing *Advanced* from the drop-down list in the upper right of the **Edit Filter** dialog opens the ***Advanced*** view of the **Edit Filter** dialog. Here you can create more complex filters with a wider range of filter parameters (including specific offsets and string values). In addition, the ***Advanced*** view allows you to construct a single filter based on a chain of filter properties connected by logical AND, logical OR, and logical NOT statements.

Make filter command

An easy way to create a new filter is to use the **Make Filter** command, available as the **Make Filter** button in many windows, or from the context menu (right-click) where applicable. The **Make Filter** command creates a filter based on the selected packet or statistics item. **Make Filter** can also be used in the Name Table to create a filter based on the selected named node, protocol, or port. It can also be used in the **Packet Decode** window (or the decode panes of the ***Packets*** view of a Capture window or Packet File window) to create a filter based on the selected data item.

When you use the **Make Filter** command, an unnamed filter is created matching the parameters of the selected packet, node, protocol, conversation, or packet decode item. An **Edit Filter** dialog will open with the parameters for your selection already loaded. Use this dialog to make any additional changes, and save the filter under a new name.

If multiple items are selected, the **Make Filter** command will attempt to create a filter for each one.

Using multiple filters simultaneously

When multiple filters are enabled simultaneously, AiroPeek considers them to be connected by logical OR statements. That is, packets matching any one of the enabled filters will pass or be rejected, depending on whether you chose to accept or reject matching packets.

Filter parameters

Filters can operate on the properties of packets shown in Table 11.1 below. As the table shows, filters created in either view of the **Edit Filter** dialog can test for address, protocol and/or port. The additional parameters are available only for filters constructed in the ***Advanced*** view of the **Edit Filter** dialog.

Table 11.1 Filter parameters

Filter Parameter	Simple	Advanced	Description
802.11		**yes**	Tests for channel, data rate, encryption state and more, based on information provided in the headers of 802.11 WLAN packets.
Address	**yes**	**yes**	Tests the identity of the network node, either receiving or sending, for that packet. This can be a physical address, or a logical address under a particular protocol.
Protocol	**yes**	**yes**	AiroPeek can filter for protocols and for many of the individual types of traffic within a given protocol, which we call sub-protocols. For example, FTP is a sub-protocol of TCP, which is itself a sub-protocol of IP.
Port	**yes**	**yes**	Tests for a port (or socket) within a particular protocol. IP, AppleTalk, and NetWare provide services at different ports or sockets on the server. The default port for Web traffic under TCP, for example, is port 80. ProtoSpecs assume that subprotocols are using the standard default ports (well known ports in TCP and UDP, for example), but you can also set filters to test explicitly for traffic to and/or from particular ports.
Value		**yes**	Tests the numerical value of a particular part of each packet (at a particular offset with a particular mask) for its relation (greater than, less than, equal to, and so forth) to the value you specify.

Table 11.1 Filter parameters (continued)

Filter Parameter	Simple	Advanced	Description
Pattern		**yes**	Tests for the presence of a particular character string (hexadecimal or ASCII) in each packet. Can be constrained to search within a specified location for greater efficiency.
Length		**yes**	Tests the length of the packet and matches those within the range you set, specified in bytes.
Error		**yes**	Tests for CRC errors.
Analysis Module		**yes**	Packets handled by the specified Analysis Module will match the filter.

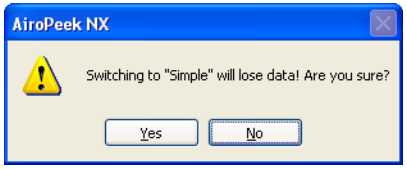
Creating and editing filters

This section describes the details of how to build filters, from the simple to the advanced. It also describes how to export, duplicate, import and edit filters.

Editing and duplicating filters

Editing an existing filter uses all the same tools as creating a new filter. Select the filter you wish to edit and click the **Edit** button, or simply double-click on any named filter to open the **Edit Filter** dialog. The dialog will open in the ***Simple*** view or the ***Advanced*** view automatically, depending on the filter you chose to edit. The filter's parameters will be displayed, ready to edit. You can make changes to the filter and click **OK** to save it.

If you want to make a new filter based on an existing filter, you must first duplicate the existing filter, then edit the duplicate. To duplicate a filter, highlight the filter and click the **Duplicate** button. A copy will appear with the words "*Copy of*" prepended to the filter name. Edit the copy and save it under a new name.



Switching to "Simple" will lose data! Are you sure?

Figure 11.3 Some filter types can only be created in the Advanced view

Note: You can switch back and forth between the ***Simple*** and ***Advanced*** views of the **Edit Filter** dialog while editing a filter. If, on moving from the ***Advanced*** to the ***Simple*** view, you are in danger of losing the ability to specify parameters you have already entered, a warning will be displayed and you will be given the opportunity to abort switching to the ***Simple*** view of the dialog.

Simple filters

Simple filters can test for address, protocol and port in a single filter. When multiple parameters are chosen they are connected by logical AND statements. That is, packets must match all of the conditions in order to match the filter.

To open the edit filter dialog simple filter view

To create a new simple filter, choose **Filters** from the **View** menu (or press **Ctrl + M**) to view the **Filters** window. Click the **Insert** button to bring up the **Edit Filter** dialog in its default ***Simple*** view.

The default name "*Untitled Filter*" shows in the *Filter* text entry box where you can enter a new name. The color assigned to this filter (black is the default for a new filter) is shown in the color swatch at the top of the **Edit Filter** dialog, to the right of the *Filter* box. Click the arrow to the right of this color swatch to open the drop-down list of color choices.

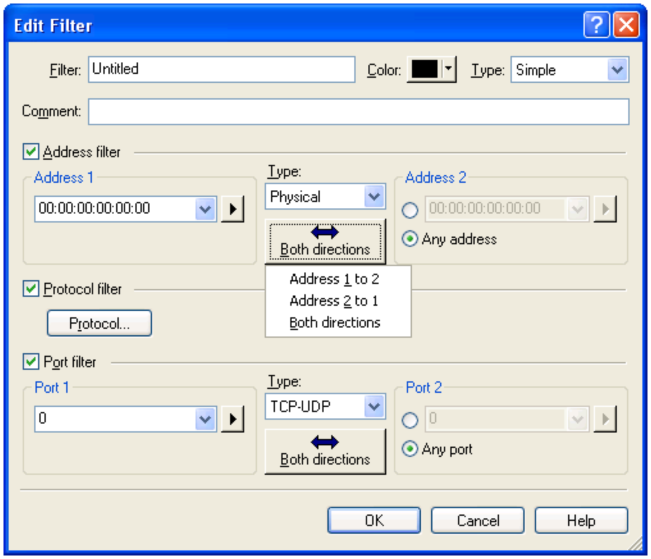
In addition to its name, you can enter a *Comment* for the filter. This comment appears in the **Filters** window and in all filter lists, and allows you, for example, to create a more complete description of the filter's properties. You can sort any list of filters by either the ***Filter*** name or the ***Comments*** column.

Specify the parameters for *Address Filter*, *Protocol Filter*, and/or *Port Filter* according to the directions given below and click **OK** to create the new filter. The new filter will appear in the **Filters** window and all other filter lists and can be enabled by checking the box beside the filter's name (see "Using filters" on page 208). To edit an existing filter, double-click on its name in any filter list to open the **Edit Filter** dialog with that particular filter's parameters displayed.

Specifying address filter parameters

To specify an address filter, click the checkbox to the left of the *Address Filter* section of the **Edit Filter** dialog. Notice that there is room for two addresses. Between these two address text entry boxes are two drop-down lists.

The topmost specifies the *Type* of addresses you want to enter. Both addresses must be of the same type and must be entered in the correct format for the address type you have selected in this drop-down list. For more on addresses and their notation formats, see Appendix B, "Addresses and Names" on page A-33.



Filter: Untitled

Color: ■

Type: Simple

Comment:

☑ Address filter

Address 1: 00:00:00:00:00:00

Type: Physical

Both directions

Address 2: ○ 00:00:00:00:00:00 ● Any address

☑ Protocol filter

☑ Port filter

Port 1: 0

Type: TCP-UDP

Both directions

Port 2: ○ 0 ● Any port

Figure 11.4 Edit Filter dialog in the Simple view

The second drop-down list specifies the send/receive relationship between the two addresses. The default value is to match all packets going in either direction between *Address 1* and *Address 2*. You could instead match only traffic going from *Address 1* to *Address 2*, or match only traffic going the other direction.

You must enter a valid address in *Address 1*, but you can choose either a particular address for *Address 2* or simply choose *Any Address* by clicking the radio button beside that choice. This allows you to filter for all traffic addressed to a particular node regardless of its source, or to filter all traffic from a particular address regardless of its destination.

The drop-down list immediately to the right of each address text entry box contains the most recently used addresses. The drop-down list arrows further to the right of each *Address* box allow you to specify an address by reference to either the Name Table or any reachable name resolution servers. Selecting *Name Table* from this drop-down list takes you to the Name Table, where you can select an address by simply clicking on its entry there. If you choose *Resolve*, AiroPeek will query the appropriate name service to attempt to find a name for the address, or an address for the name entered in the edit box.

Important! Active name resolution and notifications using the email action require an active network connection. Because AiroPeek puts the NIC into a “listen only” mode when the network adapter is selected, network access while AiroPeek is running requires that a second network adapter must be installed for use by network services. Alternatively, selecting either *None* or *File* as the adapter can free the NIC for network services, if the card supports this functionality. Please see our website at http://www.wildpackets.com/support for details about specific cards.

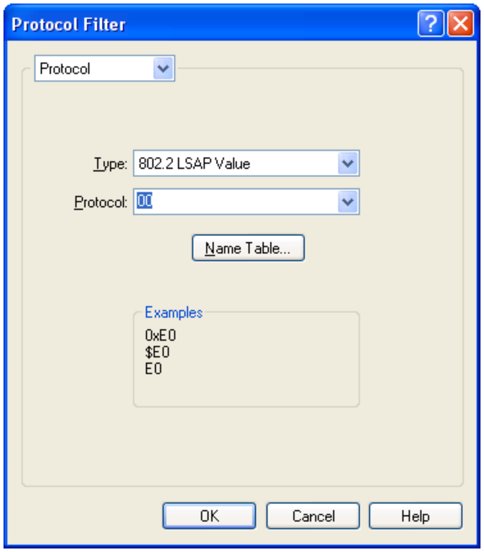
You can use the asterisk * character as a wildcard when specifying addresses. The program will replace the asterisk with its most inclusive equivalent. For example, if you specified an IP address of 192.216.124.* the program would interpret the wildcard to mean “all possible values for this element.” If you save and reopen a filter with this example, you will see that the program has interpreted the address as 192.216.124.0/24, which is standard dotted decimal/subnet notation for all addresses within the specified Class C network.

Note: Address filters support CIDR for the IP address space.

Specifying protocol filter parameters

To specify a protocol filter, click the checkbox to the left of the *Protocol Filter* section of the **Edit Filter** dialog. Click the **Protocol…** button to bring up the **Protocol Filter** dialog. At the top of the **Protocol Filter** dialog is a drop-down list whose default value is *ProtoSpec*. This allows you to choose the method AiroPeek will use to define and test for the protocol you select.

Note: In general, ProtoSpecs provide the easiest path to nearly every protocol and sub-protocol type. The secondary edit capability is provided for new or unusual protocol situations and also for backward compatibility.



Protocol

Type: 802.2 LSAP Value

Protocol: 00

Examples
0xE0
$E0
E0

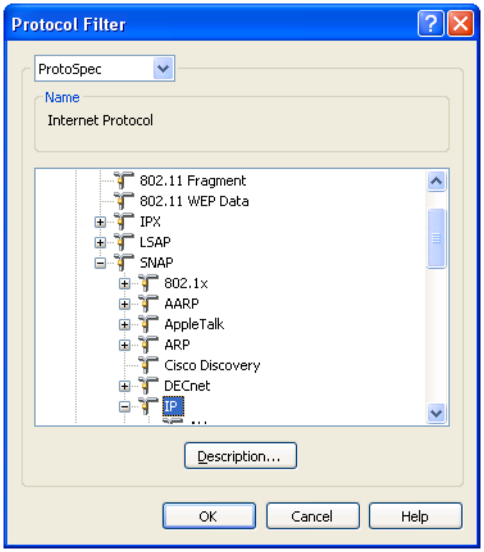
Figure 11.5 Specifying a protocol using the encoding in the 802.2 LLC header

If you choose *Protocol* rather than *ProtoSpec* as your protocol definition method, the dialog switches to its ***Protocol*** view. From this view, you can choose *802.2 LSAP Value* or *802.2 SNAP ID* from the *Type* drop-down list.

Each of these choices represents a distinct method for denoting the protocol of the network data framed by the packet. Each has its own format for representing these protocols. Choose the type of protocol and enter a value in the appropriate format. You can use a wildcard in these entries. The asterisk character (*) is a wildcard and stands for zero or more alphanumeric characters.

You may also select a protocol from the Name Table by clicking the **Name Table…** button and choosing from the protocols listed there. In this case, the name of the protocol selected rather than the discrimination values will appear in the *Protocol* text entry box. For more information about 802.11 WLAN frames and protocols, see Appendix A, “Packets and Protocols” on page A-3.

If you choose *ProtoSpec* as your protocol definition method, your protocol choices are listed in the default ***ProtoSpec*** view of the **Protocol Filter** dialog.



Name: Internet Protocol

Figure 11.6 Specifying a protocol from the ProtoSpecs list as the object of a filter

The list of protocols is in a hierarchical format. That is, when there is a + plus sign at the left margin, it indicates that other entries are nested below and hidden. When there is a - minus sign, it indicates that entries nested under this one in the hierarchy are visible. Click on the + plus or - minus signs to show or hide items nested below.

To specify a protocol, simply highlight one from the list. The active choice will appear above the list box in the space between the list box and the *ProtoSpec/Protocol* drop-down list. If the protocol you highlight has other sub-protocols listed under it, your filter will match any of these sub-protocols as well.

To finish choosing the protocol, click **OK** at the bottom of the **Protocol Filter** dialog to return to the **Edit Filter** dialog. Your protocol choice will be shown in the *Protocol Filter* section of the **Edit Filter** dialog.

Protocol descriptions

To find more information about a particular protocol, simply select it in the list and click the **Description…** button at the bottom of the **Protocol Filter** dialog. Brief descriptions of many of the most commonly used protocols are included with AiroPeek and will appear in a new dialog when you click the **Description…** button. For more on how

AiroPeek and ProtoSpecs deal with protocols, see Appendix A, “Packets and Protocols” on page A-3.

Specifying port filter parameters

To specify a port filter, click the checkbox to the left of the *Port Filter* section of the **Edit Filter** dialog. Notice that there is room for two ports. Between these text entry fields are two drop-down lists. The topmost, whose default value is *TCP-UDP*, specifies the protocol which uses the ports you want to enter. Both ports must be of the same type and must be entered in the correct format for the type you have selected in this drop-down list. For more on ports, sockets, and their notation formats, see “Ports and sockets” on page A-38.

The second drop-down list specifies the source/destination relationship between the two ports. The default value is to match all packets going in either direction between *Port 1* and *Port 2*. You could instead match only traffic going from *Port 1* to *Port 2*, or match only packets going the other direction.

You must enter a valid port designation in *Port 1*, but you can choose either a particular port for *Port 2* or simply choose *Any Port* by clicking the radio button beside that choice. This allows you to filter for all traffic to a specific port regardless of the source port, or to filter all traffic from a specific port regardless of the destination port.

Advanced filters

The ***Advanced*** view of the **Edit Filter** dialog allows you to create filters that match any of the filter parameters supported by AiroPeek (see “Filter parameters” on page 212). In addition, it allows multiple parameters to be joined with logical AND, logical OR, and logical NOT statements to create very precise tests in a single named filter.

To open the edit filter dialog advanced filter view

To create a new advanced filter, choose **Filters** from the **View** menu (or press **Ctrl + M**) to view the **Filters** window. Click the **Insert** button to bring up the **Edit Filter** dialog in its default ***Simple*** view. Choose *Advanced* from the *Type* drop-down list in the upper right to switch to the ***Advanced*** view of the **Edit Filter** dialog.

The default name “*Untitled Filter*” shows in the *Filter* text entry box where you can enter a new name. The color assigned to this filter (black is the default for a new filter) is shown in the color swatch at the top of the **Edit Filter** dialog, to the right of the *Filter* box. Click the arrow to the right of this color swatch to bring up the drop-down list of color choices.

In addition to its name, you can enter a *Comment* for the filter. This comment appears in the **Filters** window and in all filter lists, and allows you, for example, to create a more complete description of the filter's properties. You can sort any list of filters by either the ***Filter*** name or the ***Comments*** column.

Specify the parameters for the new filter according to the directions given below and click **OK** to create the new filter. The new filter will appear in all the filter lists.

To edit any existing filter, select the filter and click the **Edit** button, or simply double-click on its name in any filter list to open the **Edit Filter** dialog with that particular filter's parameters displayed and ready to edit.

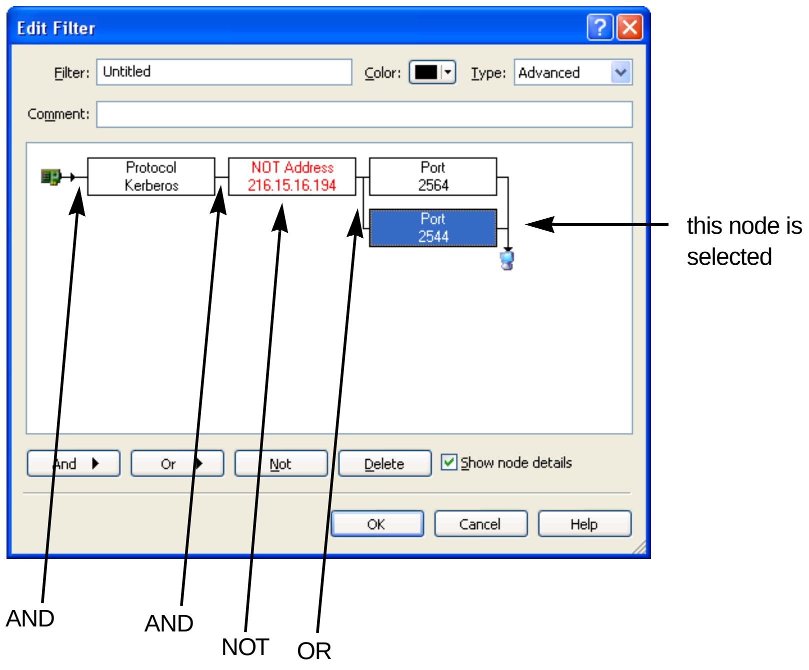
Logical AND, OR, and NOT operators in advanced filters

When you open the ***Advanced*** view of the **Edit Filter** dialog, you will see a screen with an icon in the upper left corner representing a network adapter. When you add the first node to the filter, a new icon will appear representing the computer or its capture buffer, and an arrow will appear connecting the card to the computer. The arrow points from the network adapter icon to the icon for the computer on which AiroPeek is installed. As you add sets of filter parameters, called *filter nodes*, the relationship between and among these filter nodes is displayed on this screen in a logical tree or flow diagram, starting from the network side and building toward the computer icon. Each filter node you define is treated as a building block and displayed as a labeled rectangle. The internal logic of an advanced filter is that of a pass filter. That is, any packet which could pass through the criteria established in the flow diagram is said to match the advanced filter.

The *Show node details* checkbox causes the rectangles representing filter nodes to display an approximation of the logical content of each filter node. If this checkbox is unchecked, nodes will display only their parameter type.

To view the details of any node, double-click on the rectangle that represents it. This will open the appropriate edit dialog, displaying all the specifications for that node. You can click **Cancel** if you do not wish to make any changes.

The graphic display helps to make clear the logical relationship of the various filter nodes you create in the ***Advanced*** view. The relationships are limited to three simple choices represented in the buttons at the bottom of the **Edit Filter** dialog:



Edit Filter

Filter: Untitled

Color:

Type: Advanced

Comment:

☑ Show node details

this node is selected

AND

AND

NOT

OR

Figure 11.7 Advanced view shows nodes joined by logical AND, OR, and NOT

Table 11.2 Advanced view of the Edit Filter dialog, buttons and functions

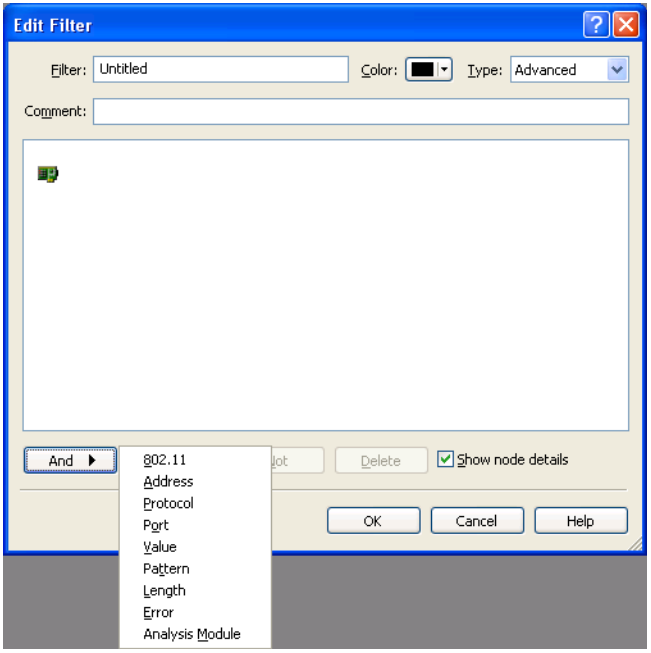
Button	Description
And	Use this button to create the first node of a new advanced filter. Clicking **And** creates a new node just after (to the right of) the currently selected node and establishes an **And** relationship with the argument of that node. That is, a packet must meet both the previous node's criteria and the newly added node's criteria in order to match the filter.

Table 11.2 Advanced view of the Edit Filter dialog, buttons and functions

Button	Description
Or	Clicking the **Or** button creates a new filter node in parallel with the node that was selected when you pressed the **Or** button. That is, the new filter node will get the same inputs as the filter node that was selected when you pressed the **Or** button, and packets meeting the criteria of either filter node will pass through, or match this stage. Please note that when you have created a set of filter nodes that is several stages deep, choosing an early node (one far to the left) and pressing the **Or** button will create a parallel path that bypasses any nodes further to the right. In other words, the new OR statement will create a node on a path that is parallel to the whole of the remaining structure, not just to the single node selected when you pressed **Or**.
Not	Negates or inverts the filter node selected when you pressed the **Not** button, changing it from a pass node to a blocking node. All packets *except* those matching the criteria inside the negated node will now be passed to the next stage.
Delete	Deletes the selected filter node.

Adding a filter node

Click on the **And** or the **Or** button in the ***Advanced*** view of the **Edit Filter** dialog and choose a filter type from the drop-down list to begin specifying the parameters of the new filter node.



Edit Filter

Filter: Untitled

Color:

Type: Advanced

Comment:

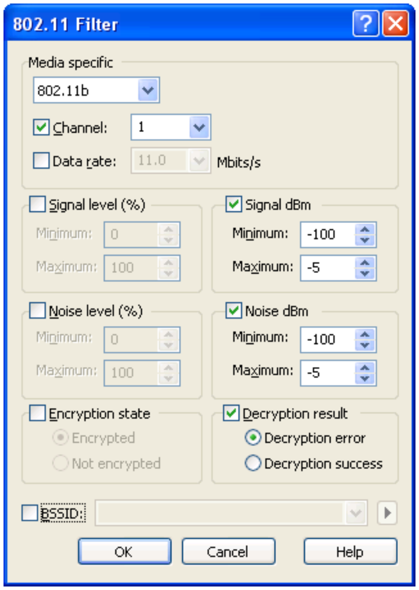
☑ Show node details

Figure 11.8 Choosing the filter node type for a new advanced filter

802.11 filter nodes

To specify a filter based on data contained in 802.11 WLAN management, control, or data packet headers, choose *802.11* from the drop-down list to open the **802.11 Filter** dialog (Figure 11.9). You can specify one or more aspects of 802.11 WLAN traffic in the filter. Multiple parameters will be treated as logically AND’ed together. That is, packets must match all of the specified parameters in order to match the 802.11 filter node you create in this dialog. Check the checkbox beside one or more parameters and specify the details of each as appropriate (see Table 11.3).

When you have finished specifying the filter node, click **OK** to return to the ***Advanced*** view of the **Edit Filter** dialog. The filter node you have just created will be selected and show the 802.11 parameters for which this node is testing, or, if *Show node details* is unchecked, it will simply be labeled *802.11*.



802.11 Filter

Media specific

802.11b

☑ Channel: 1

□ Data rate: 11.0 Mbits/s

□ Signal level (%)

Minimum: 0

Maximum: 100

☑ Signal dBm

Minimum: -100

Maximum: -5

□ Noise level (%)

Minimum: 0

Maximum: 100

☑ Noise dBm

Minimum: -100

Maximum: -5

□ Encryption state

● Encrypted

○ Not encrypted

☑ Decryption result

● Decryption error

○ Decryption success

□ BSSID:

Figure 11.9 802.11 Filter node dialog

Table 11.3 802.11 filter node parameters

Parameter	Options
Media Specific	These items (indented below) change depending on the physical layer specifications of the WLAN standard chosen.
WLAN Standard	Choose the 802.11 WLAN standard to use in defining channels and data rates. Choose *802.11a* or *802.11b* from the drop-down list.
Channel	Choose a channel from the drop-down list. Note that channels *12-14* are not used in North American implementations of 802.11b WLANs.
Data rate	Choose one of the supported data rates from the drop-down list.
Signal level (%)	Use the *Minimum* and *Maximum* data entry boxes to establish the low and high end of the range that will match this filter.

Table 11.3 **802.11 filter node parameters (continued)**

Parameter	Options
Encryption state	Use the radio buttons to have the filter match packets which are *Encrypted* or *Not Encrypted*.
Decryption result	Use the radio buttons to have the filter match packets which show a *Decryption error* or *Decryption success*.
BSSID	Enter the BSSID of the packets which will match the filter. You can choose recently used BSSIDs from the drop-down list or click the arrow to the right in order to choose a BSSID from the Name Table.

Address filter nodes

To specify an address filter node, choose *Address* from the drop-down list to open the **Address Filter** dialog. This dialog offers exactly the same choices as the *Address Filter* section of the ***Simple*** view of the **Edit Filter** dialog, but laid out in a slightly different order, as shown in Figure 11.10.

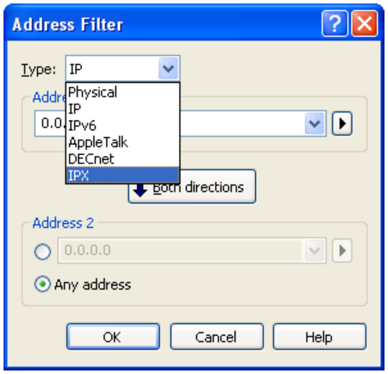


Figure 11.10 Advanced filters: the Address Filter dialog

Set the parameters for the address filter node. For detailed instructions, see “Specifying address filter parameters” on page 215.

When you have finished specifying the filter node, click **OK** to return to the ***Advanced*** view of the **Edit Filter** dialog. The filter node you have just created will be selected, with the first address in the filter displayed, or, if *Show node details* is unchecked, with the simple label: *Address*.

Protocol filter nodes

To specify a protocol filter node, choose *Protocol* from the drop-down list to open the **Protocol Filter** dialog. At the top of the **Protocol Filter** dialog is a drop-down list offering the choice of *Protocol* or *ProtoSpec*. This allows you to choose the method AiroPeek will use to define and test for the protocol you select.

For a detailed description of the **Protocol Filter** dialog and how to use it, please see “Specifying protocol filter parameters” on page 216.

When you have selected the protocol, click **OK** at the bottom of the **Protocol Filter** dialog to return to the ***Advanced*** view of the **Edit Filter** dialog. The node you have just created will be selected and show the name of the protocol that describes the parameter of the newly constructed node, or, if *Show node details* is unchecked, it will simply be labeled *Protocol*.

Port filter nodes

To specify a port filter node, choose *Port* from the drop-down list to open the **Port Filter** dialog. Specify the protocol which uses the ports for which you want to filter, using the drop-down list at the top of the dialog. Both ports must be of the same type and must be entered in the correct format for the type you have selected in this drop-down list. For more on ports, sockets, and their notation formats, see “Ports and sockets” on page A-38.

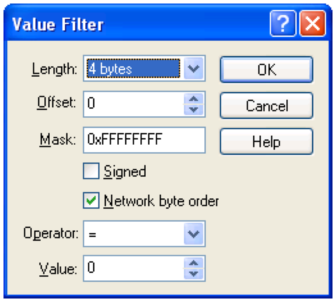
A second drop-down list located between the port text entry boxes specifies the source/destination relationship between the two ports. The default value is to match all packets going in either direction between *Port 1* and *Port 2*. You could instead match only traffic going from *Port 1* to *Port 2*, or match only packets going the other direction.

You must enter a valid port designation in *Port 1*, but you can choose either a specific port for *Port 2* or simply choose *Any Port* by clicking the radio button beside that choice. This allows you to match all traffic addressed to a specific port regardless of its source, or to match all traffic from a specific port regardless of its destination.

When you have finished specifying the filter node, click **OK** to return to the ***Advanced*** view of the **Edit Filter** dialog. The filter node you have just created will be selected and show the value you entered for *Port 1*, or, if *Show node details* is unchecked, it will simply be labeled *Port.*

Value filter nodes

To specify a value filter node, choose *Value* from the drop-down list to open the **Value Filter** dialog.



Length: 4 bytes
Offset: 0
Mask: 0xFFFFFFFF
□ Signed
☑ Network byte order
Operator: =
Value: 0

Figure 11.11 Editing a Value Filter in the Advanced view of the Edit Filter dialog

A value filter is used to test whether the specified bits at a specified location in a packet have the specified relationship to a numerical value you set. If the particular part of a tested packet has a numerical value with the relationship you specified to the numerical value you set, the packet matches the filter.

Tip You can quickly create a value filter node matching any item in the ***Decode*** view of a **Packet Decode** window or the Decode Pane of any ***Packets*** view, by highlighting the item and clicking the **Make Filter** button, or by choosing **Make Filter…** from the context menu (right-click).

The **Value Filter** dialog can be understood as an IF:THEN statement of the following form:

Default values:

If the number of *Length* "*4 bytes*"
at *Offset* "*0*"
with a *Mask* of "*0xFFFFFFFF*",
where the packet value [unchecked means "is not"] *Signed*
and it [✓ means "is in"] *Network byte order*,
has the relationship defined by the *Operator* "="
to the *Value* of "*0*"
then the packet matches the filter.

Parameters:

If the number of length (*Length*)
at offset (*Offset*)
with a mask of (*Mask*)
where the packet value [is/is not] *Signed*
and it [is in/is not in] *Network byte order*,
has the relationship (*Operator*)
to the value (*Value*)
then the packet matches the filter.

Taking each of these parameters in turn, you need to specify:

Length

What is the size of the number you wish to test? The choices are: *4 bytes*, *2 bytes*, or *1 byte*. Remember that the mask specified below must be of the correct format to properly mask a number of this length.

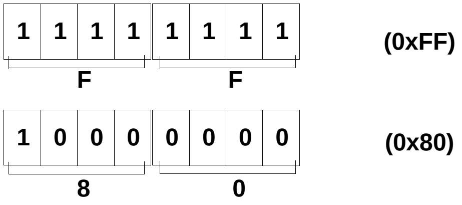
Offset

What is the location in the packet of the beginning of the first byte of the number you want to test? The location is specified as the distance (in bytes) from the beginning of the packet to the beginning of the first byte of the number you wish to test, or its *offset* from the first byte of the packet. If you want to test the first byte, it begins 0 bytes away from the beginning of the packet, so enter an offset of "*0*." The second byte of the packet begins 1 byte away, so it is at offset 1, and so on. Enter a decimal number or a hex number with the "*0x*" prefix for the offset.

To see the offset and mask for any element in a packet ***Decode*** view, click the **Show Offsets** button.

Mask

The number in this field is used to isolate particular bits inside of the byte or bytes you specified in the Length and Offset parameters. The value of the Mask is logically AND'ed with the value present in the byte or bytes you choose to test, and the result is examined. If you choose to test a one-byte number and enter a mask of "0xFF", AiroPeek will examine all of the bits in the byte. With a mask of "0x80" AiroPeek would examine only the most significant bit of that byte, as shown below:



You can enter a mask value in hex or in decimal format, but it will display in hex format when the filter is re-opened for editing.

Signed

Click the checkbox labeled *Signed* if the number at the offset you chose to test is signed. If it is not signed, leave the box unchecked.

Network byte order

AiroPeek must be told in what order to evaluate the bytes at the offset you specified. Make sure the checkbox beside *Network byte order* is checked (the default) if the bytes are in network byte order, as they usually are for most network packets. Uncheck this checkbox if the bytes at the specified offset are *not* in network byte order.

Operator

What is the relationship of the number you are testing to the value you have chosen? Remember that the mask will be applied to the bytes you specified before their value is calculated. Your choices are: equal to, greater than, less than, greater than or equal to, less than or equal to, or not equal to. Choose a relationship from the drop-down list.

Value

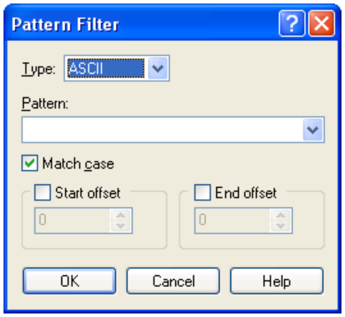
The number in this field is the constant that AiroPeek compares to the value it obtains by applying the *Mask* to the byte or bytes specified in *Length* and beginning at the location in the packet specified in *Offset*. If that calculated value has the specified relationship to the value you enter here, then the packet matches. You can enter a number in hex (with the 0x prefix) or in decimal format.

Note: Network byte order, also known as Big Endian (most significant byte first), is the form in which most protocols write their data. Little Endian (least significant byte first), or not network byte order, is the native form for Intel machines. When they communicate, however, they typically write the data in network byte order to insure compatibility with others. A few protocols such as SMB (a part of NetBIOS) may encode data in Little Endian, or not network byte order. SMB data can ride inside an IP packet. In such cases the 802.11 WLAN header and the IP header would be in network byte order, but the SMB portion of the packet would be in Little Endian, or not network byte order.

When you have finished specifying the filter node, click **OK** to return to the ***Advanced*** view of the **Edit Filter** dialog. The filter node you have just created will be selected and show the value and relationship for which this node is testing, or, if *Show node details* is unchecked, it will simply be labeled *Value*.

Pattern filter nodes

To specify a pattern filter node, choose *Pattern* from the drop-down list to open the **Pattern Filter** dialog.



Pattern Filter

Type: ASCII

Pattern:

☑ Match case

□ Start offset 0

□ End offset 0

Figure 11.12 Advanced filters: the Pattern Filter dialog

Pattern filter nodes test packets for the presence of a specific character string within the bounds of a packet. Enter a character string up to 255 characters long in the *Pattern* box. Use the *Match case* checkbox to match case as well as character form of the string. Specify where in the packet you want AiroPeek to start or end the search by specifying either a *Start offset*, an *End offset*, or both. If you select neither of these offset options, AiroPeek will search the whole packet. Limiting the area of search can speed performance.

Note: Offset is a measure of the distance in bytes from the beginning of the packet. The first byte of the packet begins 0 bytes away from the first byte of the packet, and is therefore at offset 0. The second byte of the packet begins one byte away at offset 1, the third byte begins at offset 2, and so on. To see the offset and mask for any element in a packet ***Decode*** view, click the **Show Offsets** button.

Any packet containing the pattern you specified (and in the exact case, if you specified *Match case*) will match the filter if it can be found within the offsets you specified.

When you have finished specifying the filter node, click **OK** to return to the ***Advanced*** view of the **Edit Filter** dialog. The filter node you have just created will be selected and labeled with as much of the search pattern as will fit, or, if the *Show node details* checkbox is unchecked, with the simple label: *Pattern*.

Length filter nodes

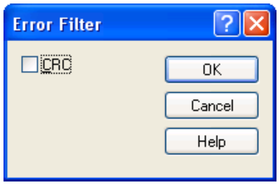
To specify a length filter node, choose *Length* from the drop-down list to open the **Length Filter** dialog.

Specify the length range (in bytes) of the packets you wish to match this filter by checking *Maximum length* and/or *Minimum length* and entering a value in bytes in the respective text entry boxes.

When you have finished specifying the filter node, click **OK** to return to the ***Advanced*** view of the **Edit Filter** dialog. The filter node you have just created will be selected and show a representation of the length range you have chosen, or, if *Show node details* is unchecked, it will simply be labeled *Length*.

Error filter nodes

To specify an error filter node, choose *Error* from the drop-down list to open the **Error Filter** dialog.


Error Filter

□ CRC

Figure 11.13 Adding an error filter node to an advanced filter

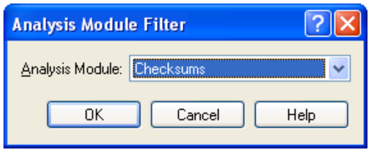
Choose to capture *CRC* errors by clicking the checkboxes beside it.

CRC	Cyclic Redundancy Check is a type of error that indicates data was corrupted in transmission.

When you have finished specifying the filter node, click **OK** to return to the ***Advanced*** view of the **Edit Filter** dialog. The filter node you have just created will be selected and show the initial of each error type you chose, or, if *Show node details* is unchecked, the node will have the simple label: *Error.*

Analysis Module filter nodes

You can use Analysis Modules to filter packets. Packets which are handled by the Analysis Module named in the filter will match the filter. To specify an Analysis Module filter node, choose *Analysis Module* from the drop-down list to open the **Analysis Module Filter** dialog. For details on the behavior of individual Analysis Modules and the kinds of packets each one is designed to handle, see Chapter 13, “Analysis Modules” on page 257.



Analysis Module Filter

Analysis Module: Checksums

Figure 11.14 Adding an Analysis Module filter node to an advanced filter

Saving and loading filters

You can save and load filters. This allows you to create multiple sets of filters for different requirements. Clicking the **Export** button in the **Filters** window lets you save the whole set of filters under a new name. Alternatively, you can save a selection of filters by highlighting them and using the **Export Selected…** command from the context menu (right click).

To save the existing set of filters under a new name:

1. Open the **Filters** window by choosing **View** > **Filters** or typing **Ctrl + M**.
2. Click the **Export** button to open the **Save** dialog.
3. Give the file a name and save it by clicking the **Save** button.

When you import a previously saved group of filters into the **Filters** window, it adds them to the filters already there.

To import filters from another *.flt file into the existing **Filters** window:

1. Click the **Import** button at the left of the **Filters** window.
2. Use the dialog to navigate to the saved filters file of your choice.
3. Click **Open** to load the selected file.

Note: Imported filters are added to the existing filters list. Duplicates of existing filters will be ignored if they have identical parameters as well as identical names. Filters with the same name but different parameters will be added with “*copy*” added to their names.

Triggers, Alarms and Notifications

The evidence of network problems is often fleeting. AiroPeek provides a variety of real-time monitoring tools to help you automate the search for anomalies and problem conditions.

AiroPeek can be programmed to take a variety of actions based on network traffic or statistical events. There are four classes of actions that can be automated:

- Actions you assign directly to a trigger using one of the **Trigger** dialogs
- Actions you assign directly to an Analysis Module using the ***Analysis Modules*** view of the **Options** dialog
- Actions you associate with notifications using the ***Notifications*** view of the **Options** dialog
- Notifications sent when user-defined **Alarm** conditions are detected in statistics outputs

Triggers, alarms and Analysis Modules can be configured to make notifications. When they do, these notifications will execute any action(s) you have assigned to that particular level of severity of notification: write to the Log file, send an email message, play a sound file, or run a program.

Triggers and Analysis Modules scan all incoming packets for matching conditions. Alarms periodically query statistics functions to find their specified conditions. This chapter describes the creation and function of triggers, alarms, and Notifications. For more on Analysis Modules, see Chapter 13, “Analysis Modules” on page 257.

In this Chapter:

Triggers

Triggers are used to start or stop capture in a Capture window at a specified time or network event. They are very useful for pinpointing the origins of intermittent network problems. For example, you can set a Start Trigger so that capture begins when a problem occurs. Conversely, you can stop capturing when the problem occurs so that you can see exactly what happened just prior to the observed symptom. Alternatively, if you know that problems occur at a particular time, you can set a time event to begin capturing packets during that time. Start and Stop Triggers can help you uncover many hard-to-find network problems.

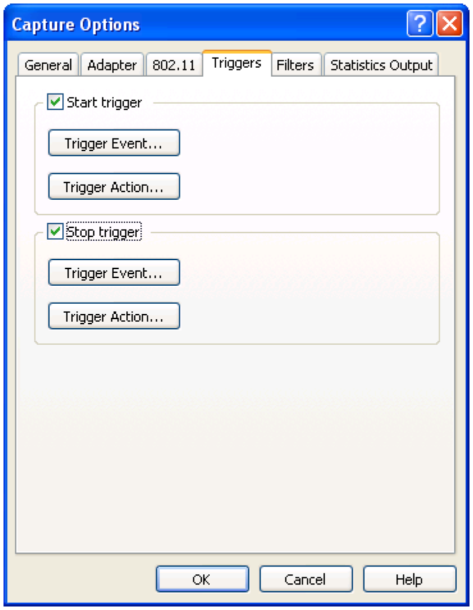
Trigger events

A trigger event can be one of the following:

- A user-specified time occurs.
- A packet matches one of any number of user-specified filters.
- A stop trigger may be set to trip when a specified number of bytes are captured.

Note: Although the same list of filters is used for capture filtering, triggering, and post-capture selection in the **Select** dialog, enabling the use of a filter in one area does not enable that filter in any other area. For example, specifying a filter in a trigger does not mean that the filter will be applied during capture activity.

To create a trigger, you must make the Capture window for which you want to create the trigger the active window. If it is an existing Capture window, you must also stop capture before creating a new Start Trigger. With the target Capture window active, choose **Capture Options…** from the **Capture** menu, or double-click the current adapter listing in the status bar of the Capture window to open the **Capture Options** dialog. Click the *Triggers* tab to display the ***Triggers*** view.



☑ Start trigger

☑ Stop trigger

Figure 12.1 Triggers view of the Capture Options dialog

From the ***Triggers*** view of the **Capture Options** dialog you can set a Start Trigger, a Stop Trigger, or both; define the triggering event(s), and specify what action(s) the trigger(s) will take. Details for each of these are discussed below.

About start triggers

A Start Trigger instructs a Capture window to remain idle, reviewing but not capturing packets, until a specified event occurs. When the trigger event occurs, you can specify that the Capture window:

- begins capture (according to the set-up of the Capture window it triggers).
- uses a defined notification option to alert you to the trigger event.
- performs a combination of these actions.

While idle, all packets on the network are reviewed but not captured. The Start Trigger tests all network traffic against any filters you have set as Trigger Events, but ignores any filters enabled for the Capture window itself. Once the Start Trigger event occurs, the configuration you set for the Capture window itself takes over; including any enabled filters, packet slicing options, use of buffer memory, columns to be displayed, and so forth.

When you have finished specifying the Start Trigger and you click **OK** in the ***Triggers*** view of the **Capture Options** dialog, the **Start Capture** button in the active Capture window changes to **Start Trigger**. The trigger will not begin reviewing incoming packets or checking to see if its assigned time has arrived until you click this button.

When you click on the **Start Trigger** button it changes to **Abort Trigger** and the Start Trigger begins searching the incoming packets and/or the system clock for the event(s) you specified. When any one of the specified events occurs, the actions you specified are performed and the button changes back to **Stop Capture**. Clicking on the **Abort Trigger** button at any time will stop the process and return the Capture window to its normal state.

Tip If you have already captured traffic in the current window and wish to add the new capture to the old, hold down the **Shift** key when you click the **Start Trigger** button. This will bypass the warning dialog asking if you wish to save the existing contents of the Capture window. When the Start Trigger is tripped, capture will resume just as it does when you use **Shift + Click** to restart capture manually.

When you first open the Capture window, the status bar at the bottom will show *Idle*. When you press the **Start Trigger** button, the status bar will show *Waiting for Start Trigger*. When the trigger event occurs, the status bar will show *Capturing*. If, instead, you press the **Abort Trigger** button before the Start Trigger is tripped, the status bar message will return to *Idle*.

Creating a start trigger

To specify a Start Trigger:

1. Open a new Capture window, or make a new Capture window the active window.
2. Choose **Capture Options…** from the **Capture** menu to open of the **Capture Options** dialog, and click the *Triggers* tab to open the ***Triggers*** view.
3. Check the *Start trigger* checkbox in the ***Triggers*** view to enable the **Trigger Event…** and the **Trigger Action…** buttons.
4. Click the **Trigger Event…** button to specify the event which will trip the trigger. You can specify a time event, a filter event, or both. If you specify both, the first one to occur will trip the trigger. Please see “Setting a time trigger event” below and “Setting a filter trigger event” on page 240 for details.

5. Click the **Trigger Action…** button to define what will take place when the trigger is tripped. You can choose to begin capture in the selected Capture window, to send a notification of a specified severity, or both. Please see “Specifying trigger actions” on page 240 for details.

6. When you have specified both the event(s) and the action(s) for the trigger, click the **OK** button in the **Capture Options** dialog to create the trigger for the active Capture window.

Setting a time trigger event

To create a trigger that will trip at a specified time, or date and time:

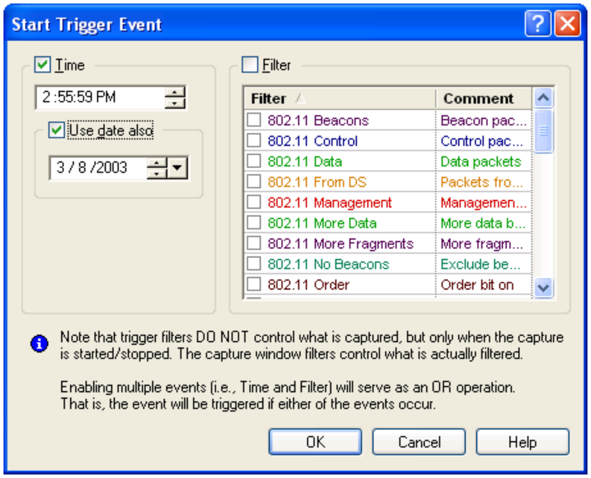
1. From the ***Triggers*** view of the **Capture Options** dialog, click the **Trigger Event…** button to open the **Trigger Event** dialog.

2. Click in the *Time* checkbox in the **Trigger Event** dialog.

3. Edit the time directly or use the arrows at the right of the time box to set the time for the trigger event. When this time is reached, the trigger will trip.

4. Click the *Use date also* checkbox and enter the date in a similar fashion if you want to include this parameter. At the far right of the date text entry box is a drop-down list that allows you to choose the date by reference to monthly calendars.

5. Click **OK** to return to the ***Triggers*** view.



☑ Time

2:55:59 PM

☑ Use date also

3 / 8 /2003

□ Filter

Filter	Comment
□ 802.11 Beacons	Beacon pac...
□ 802.11 Control	Control pac...
□ 802.11 Data	Data packets
□ 802.11 From DS	Packets fro...
□ 802.11 Management	Managemen...
□ 802.11 More Data	More data b...
□ 802.11 More Fragments	More fragm...
□ 802.11 No Beacons	Exclude be...
□ 802.11 Order	Order bit on

Note that trigger filters DO NOT control what is captured, but only when the capture is started/stopped. The capture window filters control what is actually filtered.

Enabling multiple events (i.e., Time and Filter) will serve as an OR operation. That is, the event will be triggered if either of the events occur.

Figure 12.2 Start Trigger Event dialog

Setting a filter trigger event

The **Trigger Event** dialog includes the same list of filters that appears in the **Filters** window. To view the details of filters or to make edits or duplicates of any filter, choose **Filters** from the **View** menu or press **Ctrl + M** to open the **Filters** window. You can also open any filter in its appropriate view of the **Edit Filter** dialog by double-clicking on its listing in this or any other list of filters.

To set a trigger based on a filter:

1. Check the checkbox beside any filter or filters you wish to enable. The checkbox labeled *Filter* will be checked (or unchecked) automatically, to show that this option is enabled.
2. You can set one or more filters, or you can enable both filter and time events in a single trigger. Each enabled trigger event is independent of the others that have been enabled; that is, the Trigger Action is started if any one of the enabled trigger events occurs.
3. When you have selected the trigger event(s), click **OK** to return to the ***Triggers*** view of the **Capture Options** dialog.

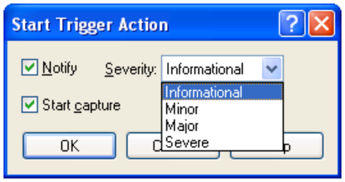
Specifying trigger actions

In a Start Trigger, you can perform one or more of the following actions when the trigger event occurs:

- Start capturing packets in this Capture window, with all its enabled filters, packet slicing options, or any other options you have enabled for it.
- Send a notification of the *Severity* you specify using the drop-down list. The default value is *Informational*, the lowest level.

Note: If you have already assigned actions to these severity levels in the ***Notifications*** view of the **Options** dialog, then the actions assigned there will be executed when notification occurs. For more on Notifications and their associated actions, see “Notifications” on page 248.

To choose one or more of these trigger actions, click the appropriate checkboxes in the **Start Trigger Action** dialog. When you have specified the action(s), click **OK** to return to the ***Triggers*** view of the **Capture Options** dialog.



Start Trigger Action

☑ Notify Severity: Informational

☑ Start capture

Notification Severity Levels drop-down list

Figure 12.3 Start Trigger Action dialog

About stop triggers

A Stop Trigger tells the Capture window to capture packets until a specified event occurs. When you use a Stop Trigger, you should consider what you want to happen if the buffer becomes full before the trigger event occurs.

When a Stop Trigger is active, the message *(Stop Trigger Active)* appears in the status bar at the bottom of the Capture window.

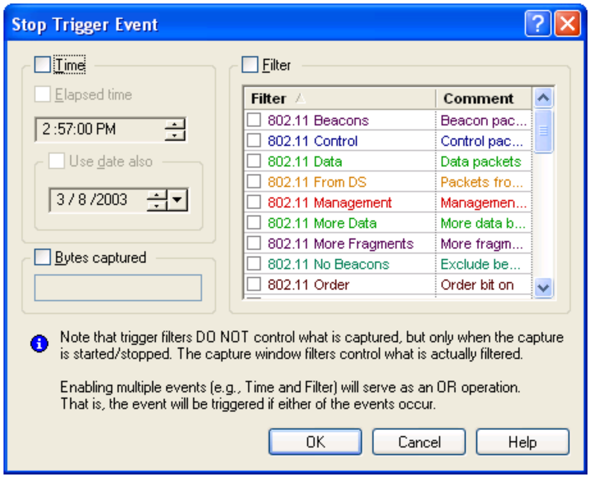
When the trigger event occurs, you can specify that AiroPeek:

- stop capture.
- use a defined notification option to alert you to the trigger event.
- perform both of these actions.

Creating a stop trigger

The process of creating a Stop Trigger is virtually identical to the one described for “Creating a start trigger” above. Click the *Stop trigger* checkbox in the ***Triggers*** view of the **Capture Options** dialog. **Trigger Event…** offers the same choices as presented for Start Triggers above, with two important additions. The Stop Trigger event can be based on *Elapsed time*, specified in the form *00d 00h 00m 00s*, for days, hours, minutes, and seconds from the moment the Stop Trigger is enabled. You can also base the Stop Trigger on the number of *Bytes captured*. Check the checkbox beside either or both of these parameters and fill in the text entry box in the appropriate format.

Tip If you choose *Bytes captured*, AiroPeek has the intelligence to capture all the bytes in the last packet -- the packet that causes the counter to reach your *Bytes captured* limit. Because of this, the number of bytes actually captured will be the value you set in *Bytes captured*, minus as little as one byte, plus the length of the last packet captured.



Stop Trigger Event

□ Time

□ Elapsed time

2:57:00 PM

□ Use date also

3/8/2003

□ Bytes captured

□ Filter

Filter	Comment
□ 802.11 Beacons	Beacon pac...
□ 802.11 Control	Control pac...
□ 802.11 Data	Data packets
□ 802.11 From DS	Packets fro...
□ 802.11 Management	Managemen...
□ 802.11 More Data	More data b...
□ 802.11 More Fragments	More fragm...
□ 802.11 No Beacons	Exclude be...
□ 802.11 Order	Order bit on

Note that trigger filters DO NOT control what is captured, but only when the capture is started/stopped. The capture window filters control what is actually filtered.

Enabling multiple events (e.g., Time and Filter) will serve as an OR operation. That is, the event will be triggered if either of the events occur.

Figure 12.4 Stop Trigger Event dialog

In **Trigger Action…** for a Stop trigger, instead of the possible action of starting to capture packets, you can click the *Stop capture* checkbox to stop capturing packets when the specified event occurs.

Alarms

Alarms query a specified Monitor statistics function approximately once per second, testing for the user-specified alarm condition(s), and/or for the user-specified alarm resolution condition. On matching any of these tests, the alarm function sends a notification of a user-specified severity.

Unlike triggers, filters and Analysis Modules, alarms do not query all incoming packets directly. Instead, alarms query statistics functions, looking for the occurrence of the user-specified statistical values and their persistence over a specified length of time. This allows multiple alarms to be set without adding packet processing overhead, thus speeding program performance.

Alarms can be created for items in the **Node**, **Protocol**, and **Summary Statistics** windows and for items in the ***Channels*** view of the **Channel Statistics** window. You can also create an alarm from items in the ***Node***, ***Protocol***, ***Channel***, and ***Summary*** views of any Capture window or Packet File window, or from any open statistics **Graph** window.

Important! No matter where or how an alarm is created, it only watches Monitor statistics. This means the **Monitor Statistics** option under the **Monitor** menu must be enabled in order for alarms to work.

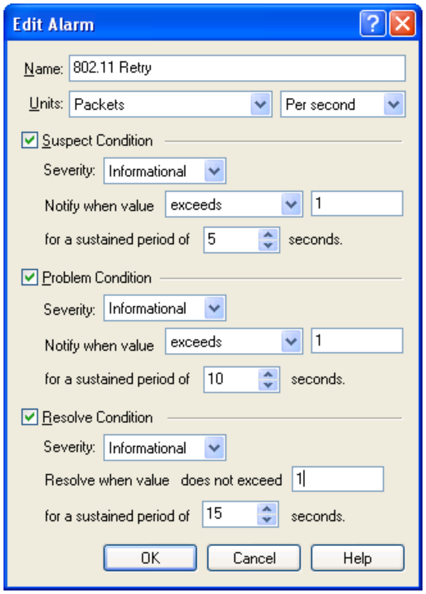
Predefined alarms

AiroPeek includes two sets of ready-made alarms for your convenience. The first set is loaded on installation. These are located in the Alarms directory where you installed AiroPeek, in a file called Default Alarms.alm. A second, larger set of alarms is included in a file in the same directory called Additional Alarms.alm. The default set of alarms covers the most frequently encountered network problem conditions. The additional alarms generally include normal network conditions which you may want to monitor for particular purposes. You can load these or any other saved set of alarms using the **Import** button in the **Alarms** window.

Creating and editing alarms

To create a new alarm:

1. Open one of the statistics windows, statistics views, or statistics graphs offering the Make Alarm function. Alarms can be created for items in the **Node**, **Protocol**, or **Summary Statistics** windows; or from items in the analogous views of any Capture window or Packet File window; or from any open statistics **Graph** window.
2. Select the item to be monitored.
3. Click the **Alarms** button at the top of the window, or right-click on the item and choose **Make Alarm…** from the context menu, to open the **Make Alarm** dialog (Figure 12.5).
4. Fill in the parameters for the alarm, following the usage shown in Table 12.1. Note that a single alarm can test for two distinct levels, identified in the **Make Alarm** dialog as *Suspect Condition* and *Problem Condition*. Both sets of conditions share the same *Resolve Condition*. This allows you to create a yellow alert / red alert / stand down for the same statistics parameter in a single alarm. Alternatively, you can specify only the *Suspect Condition* or only the *Problem Condition* for this alarm.
5. When you have chosen all the parameters, click **OK** to create and enable the alarm, or click **Cancel** to close the **Make Alarm** dialog without creating the alarm.



Name: 802.11 Retry

Units: Packets Per second

☑ Suspect Condition

Severity: Informational

Notify when value exceeds 1

for a sustained period of 5 seconds.

☑ Problem Condition

Severity: Informational

Notify when value exceeds 1

for a sustained period of 10 seconds.

☑ Resolve Condition

Severity: Informational

Resolve when value does not exceed 1

for a sustained period of 15 seconds.

Figure 12.5 Make Alarm dialog

The following table (Table 12.1) lists the user-definable elements in the **Make Alarm** dialog (and the identical **Edit Alarm** dialog), and describes their usage.

Table 12.1 Make Alarm and Edit Alarm dialog parameters

Parameter	Usage
Name	The name by which this alarm will be known in the **Alarms** window, and which will be used in the message portion of any notifications. The dialog is context aware. By default, any new alarm is named for the statistical item to be monitored. You may modify or add to this name.

Table 12.1 **Make Alarm and Edit Alarm dialog parameters (continued)**

Parameter	Usage
Units	This two part entry sets the units in which the statistical value for which the alarm is testing will be measured. The dialog is context sensitive and the choices in the first drop-down list change according to the statistical parameter chosen. Typical choices are: *Count*, *Packets*, or *Bytes*. Alarms created in the **Node Statistics** window add the concept of direction, giving *Bytes From*, *Bytes To*, *Total Bytes*, and the same for packets. The second drop-down list (on the right) determines whether these units are to be counted *Per second* or in *Total* over the time periods set for each *Condition* below. In general, only alarms set to watch statistics which are themselves already measured in units per second should be set to *Total*. Alarms for all other statistics should be set to the default *Per second*.
Suspect Condition	Check this checkbox to specify the parameters for a *Suspect Condition* for the current statistics parameter. Suspect conditions are typically used to note less severe states.
Severity	Choose the severity of the notification to be sent when the Suspect conditions are met. For more about notifications, see “Notifications” on page 248.
Notify when value	Choose *exceeds* or *does not exceed* from the drop-down list and enter a value in the adjacent text entry box.
for a sustained period of **[***number***]** *seconds*	Enter a value in *seconds.*
Problem Condition	Check this checkbox to specify the parameters for a *Problem Condition* for the current statistics item. Problem conditions are typically used to note more severe states.
Severity	Choose the severity of the notification to be sent when the Suspect conditions are met. For more about notifications, see “Notifications” on page 248.

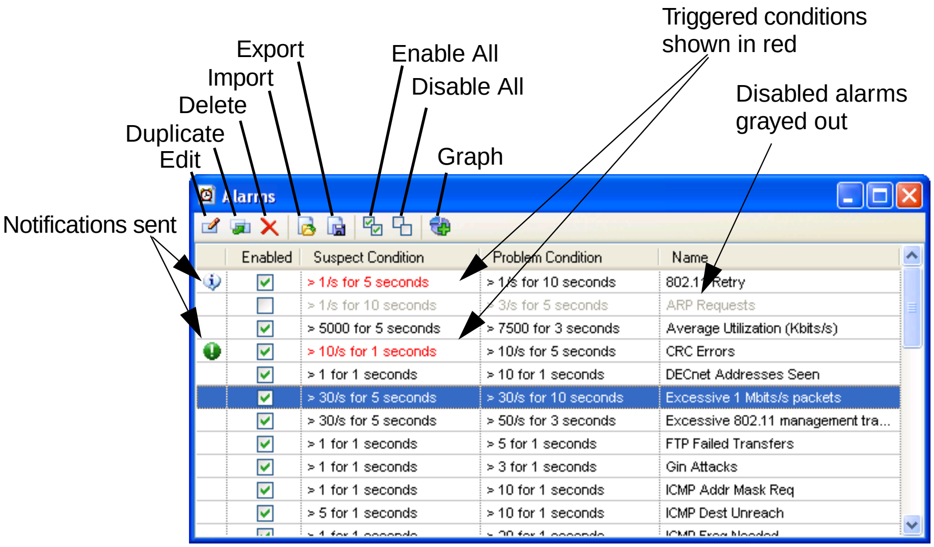
Table 12.1 Make Alarm and Edit Alarm dialog parameters (continued)

Parameter	Usage
Notify when value	Choose *exceeds* or *does not exceed* from the drop-down list and enter a value in the adjacent text entry box.
for a sustained period of **[***number***]** *seconds*	Enter a value in *seconds.*
Resolve Condition	When these conditions are met, the alarm is “stood down” or resolved. The resolve condition is identical for either or both the *Suspect Condition* and *Problem Condition* in a given alarm.
Severity	Choose the severity of the notification to be sent when the resolve conditions are met. For more about notifications, see “Notifications” on page 248.
Resolve when value exceeds **/** *does not exceed*	The wording and sense of this resolve condition is automatically set to the opposite sense entered for the *Suspect Condition* and *Problem Condition* in a given alarm. Enter a value in the text entry box.
for a sustained period of **[***number***]** *seconds*	Enter a value in *seconds.*

Important! Alarms set to watch the *Total* value of a statistic which never goes down in value will not resolve until the statistics buffer is cleared, either automatically when AiroPeek is restarted or manually by choosing **Reset Statistics** under the **Monitor** menu. Only a few statistics, such as *Average Utilization (kbits/s)* in **Summary Statistics** and some of the statistics captured by Analysis Modules such as WebStats require the use of the *Total* feature. Most statistics require the default value of *Per second* when setting the conditions for any alarm.

The alarms window

When an alarm is first created, it is automatically enabled. To review the existing alarms, to enable or disable, duplicate, modify or delete them, or to create a real-time graph of the Monitor statistics parameters they are monitoring; open the **Alarms** window by choosing **Alarms** under the **View** menu.



	Enabled	Suspect Condition	Problem Condition	Name
ℹ	☑	> 1/s for 5 seconds	> 1/s for 10 seconds	802.11 Retry
	☐	> 1/s for 10 seconds	> 3/s for 5 seconds	ARP Requests
	☑	> 5000 for 5 seconds	> 7500 for 3 seconds	Average Utilization (Kbits/s)
❗	☑	> 10/s for 1 seconds	> 10/s for 5 seconds	CRC Errors
	☑	> 1 for 1 seconds	> 10 for 1 seconds	DECnet Addresses Seen
	☑	> 30/s for 5 seconds	> 30/s for 10 seconds	Excessive 1 Mbits/s packets
	☑	> 30/s for 5 seconds	> 50/s for 3 seconds	Excessive 802.11 management tra...
	☑	> 1 for 1 seconds	> 5 for 1 seconds	FTP Failed Transfers
	☑	> 1 for 1 seconds	> 3 for 1 seconds	Gin Attacks
	☑	> 1 for 1 seconds	> 10 for 1 seconds	ICMP Addr Mask Req
	☑	> 5 for 1 seconds	> 10 for 1 seconds	ICMP Dest Unreach
	☑	> 1 for 1 seconds	> 20 for 1 seconds	ICMP Frag Needed

Figure 12.6 Alarms window

The **Alarms** window (Figure 12.6) has five columns. The first or left-most column is unlabeled. From left to right, the remaining columns are: ***Enabled***, ***Suspect Condition***, ***Problem Condition***, and ***Name***.

The first column (unlabeled) displays the icon for the type of notification sent by any alarm that is in a triggered state.

The ***Enabled*** column shows a checkmark if the alarm is enabled. Check the checkbox in this column to enable or uncheck to disable individual alarms. When an alarm is disabled it is shown in grey.

The ***Suspect Condition*** and ***Problem Condition*** columns show a shorthand version of the statistics measurements required to trigger this part of the alarm. This value is set in the **Make Alarm** dialog and can be modified in the **Edit Alarm** dialog. Alarm conditions which have been triggered are shown in red.

The ***Name*** column shows the name of the alarm, which by default is the name of the statistic to be monitored. This value is set in the **Make Alarm** dialog and can be modified in the **Edit Alarm** dialog.

Double-click on any alarm to open the **Edit Alarm** dialog with all that alarm's properties shown and ready to edit. You can also open the **Edit Alarm** dialog by selecting an alarm from the list and clicking the **Edit** button at the left of the **Alarms** window. The **Edit Alarm** dialog is identical to the **Make Alarm** dialog in appearance and function.

To make a copy of an alarm, select the alarm in the **Alarms** window and click the **Duplicate** button. To delete an alarm, select the alarm in the **Alarms** window and click the **Delete** button. To create a graph showing the current values for the statistics being monitored by any alarm, select the alarm from the **Alarms** window and click the **Graph** button. Graphs created from an alarm will show a red line indicating the value set as the alarm's Problem Condition and an orange line for its Suspect Condition. All of these functions plus *Enable All* and *Disable All* are available from a context menu by right-clicking on any alarm.

Importing and exporting alarms

You can save and reload the whole contents of the **Alarms** window, using the **Export** and **Import** buttons in the **Alarms** window. When you load an alarms file, you can choose whether to add to the existing list or replace it with the contents of the new file.

Note: If you re-install AiroPeek, neither the Default nor the Additional alarms will be loaded if the **Alarms** window already contains entries.

Notifications

Notifications are messages sent from triggers, alarms, Analysis Modules and other parts of the program to announce and describe the occurrence of specified events. Under the default settings, all notifications are sent using the same method or Action—they use an Action called *Log* to send their notifications to the Log file. This section describes how to use the ***Notifications*** view of the **Options** dialog to create other Actions and to associate these Actions with notifications of a particular severity. These Actions can be used either in addition to or instead of the standard Action of writing to the Log file.

Four types of Actions can be configured and associated with notifications in the ***Notifications*** view of the **Options** dialog. They are:

Log	Sends the notification to the Log File.
Email	Sends the notification in email.

Execute	Launches a program of your choice.
Sound	Plays a specified *.wav file on the local machine.

Individual sections following this introduction describe how to create each of these types of actions.

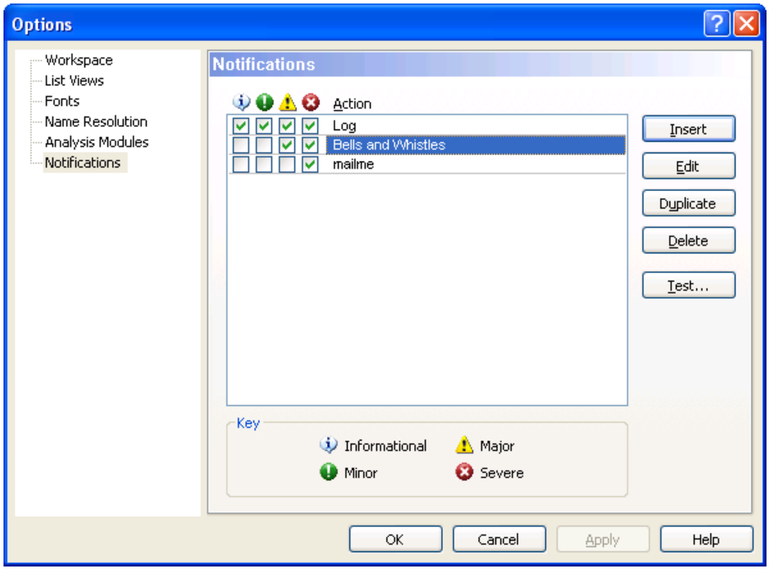
Notifications have an attribute called *level of severity*. Notifications can have one of four levels of severity. From least to greatest, they are:

- Informational
- Minor
- Major
- Severe

The level of severity is set by the function generating the notification. For triggers, alarms and some Analysis Modules the user can set the level of severity directly. Other Analysis Modules are coded to always assign a certain severity to notifications of a particular event. Analysis Modules can also be limited to a capped range of severities, overriding their internal coding. Please see these other sections ("Triggers" on page 236, "Alarms" on page 242, and "Analysis Modules" on page 257) for details about how each of these other functions generates notifications.

The ***Notifications*** view of the **Options** dialog controls how notifications of a given severity will be delivered, where they will be sent, and what (if any) other actions will be taken.

To open the ***Notifications*** view of the **Options** dialog, choose **Options…** from the **Tools** menu. Click the *Notifications* item in the navigation pane to bring up the ***Notifications*** view, shown in Figure 12.7.



ℹ	●	⚠	✖	Action
☑	☑	☑	☑	Log
☐	☐	☑	☑	Bells and Whistles
☐	☐	☐	☑	mailme

Figure 12.7 Notifications view of the Options dialog

The main pane of the ***Notifications*** view shows all the defined notification Actions, one Action per line. The name of each Action is shown in the column labeled ***Action***. The four left-most column headings are icons of the various levels of severity. Their meanings are shown in the *Key* at the bottom of the dialog. From left to right, the icons represent: ***Informational***, ***Minor***, ***Major***, and ***Severe***.

When a checkbox under one of these levels of severity is checked, the notification Action on that line will be invoked each time a notification of that severity is generated by any other function in the program. If the checkbox is unchecked, then a notification of that level of severity will not invoke the Action shown on that line.

When you first open the ***Notifications*** view of the **Options** dialog in AiroPeek, the only ***Action*** that is defined is called *Log* and the checkboxes under all four levels of severity are checked. This means that the *Log* action will be invoked when a notification of any of the four severity levels is generated from any source.

On the right hand side are five buttons used to maintain the notification actions. From top to bottom, they are as shown in Table 12.2 below.

Table 12.2 **Notifications view buttons**

Button	Description
Insert	Opens an **Edit Action** dialog with *Action* (the name of the Action) set to "*Untitled Action*" and the *Type* parameter set to the default *Log*. Select the type of action you want to create from the *Type* drop-down list. The **Edit Action** dialog view for that type of Action will appear, ready to be filled in.
Edit	Opens an **Edit Action** dialog for the selected Action, with all the information for that Action already filled in. (Double-clicking on an Action also opens the **Edit Action** dialog.)
Duplicate	Creates a copy of the selected Action.
Delete	Deletes the selected Action.
Test	Opens a dialog which allows you to edit the long and short messages of a sample notification, set the severity of the test notification, then test the notification settings for that severity level.

To create a new notification Action:

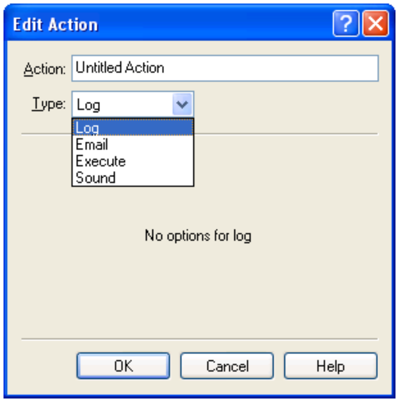
1. Choose **Options…** from the **Tools** menu to open the **Options** dialog.
2. Click the *Notifications* tab to open the ***Notifications*** view.
3. Click **Insert** to open the **Edit Action** dialog.
4. Use the *Type* drop-down list to choose the type of Action you wish to create. Your choices are *Log*, *Email*, *Execute*, or *Sound*.
5. Fill in the parameters for the Action. The following sections describe the parameters for each of the possible types of notification Actions.
   - Write the notification to the log file
   - Send the notification as email
   - Execute a program upon notification

- Play a sound file upon notification

6. When you have filled in the parameters for the particular type of Action, click **OK** in the **Edit Action** dialog to close the dialog and return to the ***Notifications*** view, where your new Action will appear under the name you assigned.
7. Choose the levels of severity of notification for which this Action should be invoked. Check the checkbox under each level of severity that should use this Action.
8. Click **Apply** to implement your changes and leave the dialog open, or click **OK** to accept your changes and close the **Options** dialog.

Write the notification to the log file

The Log type action writes notifications to the AiroPeek Log. When the notification is generated by an event associated with a particular window, the Log type action will also write the notification to the ***Log*** view of that Capture window or Packet File window.



Edit Action

Action: Untitled Action

Type: Log

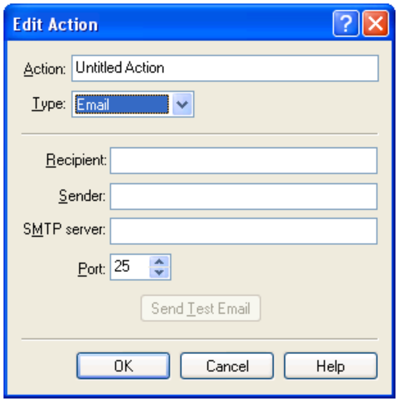
No options for log

Figure 12.8 Insert brings up the Edit Action dialog in default Log view

If you select the Action called *Log* and click the **Edit Action** button, it will bring up the **Edit Action** dialog in the correct view for this action. You will see that, as its name suggests, the Action is of the *Type Log*. Its name (in the box labeled *Action*) is *Log*, and there are, as the message says, “*No options for log*” type actions.

Send the notification as email

The Email type Action sends notifications as email messages whose text is the text of the notification.



Action: Untitled Action
Type: Email
Recipient:
Sender:
SMTP server:
Port: 25

Figure 12.9 Edit Action dialog for Email action type

To create an Action of the type Email:

1. Click the **Insert** button and in the **Edit Action** dialog that appears, use the pull-down menu for the *Type* parameter to select *Email* to switch to the ***Email*** view of the **Edit Action** dialog (Figure 12.9).
2. Fill in the options for the Email type action as shown in Table 12.3

Table 12.3 Options for Email type notification action

Option	Description
Recipient	Fill in the address to which you want the notifications to be sent.
Sender	Fill in the return address of the email message.
SMTP Server	Fill in the mail server on your network.
Port	The port on which the SMTP services are offered. The standard port for SMTP is port 25.

Tip You can use the *Sender* portion of the notification emails to sort the messages in the email program at the receiving end.

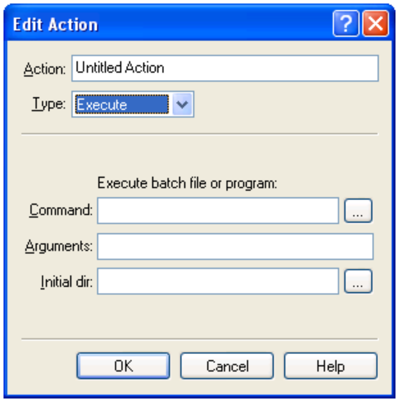
3. Optionally, you can test the email notification by clicking the **Send Test Email** button.
4. Give this Action a name (in the box labeled *Action*) and click **OK** to add it to the list of possible actions in the ***Notifications*** view.
5. Select which levels of severity of notification you would like to automatically perform this action, using the checkboxes to the left of the Action's name. Alternatively, you can leave all the checkboxes unchecked to simply hold this action in reserve without applying it at the moment to any Notifications.

Execute a program upon notification

You can run a program of your choice either instead of or in addition to any other notification actions.

To create an Action of the type Execute:

1. Click the **Insert** button and in the **Edit Action** dialog that appears, use the pull-down menu for the *Type* parameter to select *Execute* to open the ***Execute*** view of the **Edit Action** dialog (Figure 12.10).



Action: Untitled Action

Type: Execute

Figure 12.10 Edit Action dialog for Execute action type

2. Fill in the *Command* text entry box or click the button on the right marked with the ellipses **...** to browse your system to locate and select the program or batch file you wish to run when this Action is invoked.

3. Use the *Arguments* text entry box to specify any argument or command line parameters to use in invoking this program.

4. If the program requires an initial directory, you can specify this in the *Initial Dir* text entry box, or use the button marked with the ellipses **...** to browse your system to locate and select the initial directory.

5. Give this Action a name (in the box labeled *Action*) and click **OK** to add it to the list of possible actions in the ***Notifications*** view.

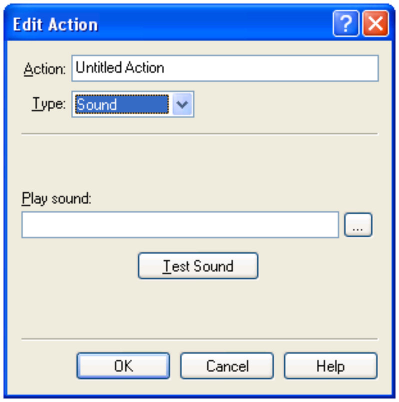
6. Select which levels of severity of notification you would like to automatically perform this action, using the checkboxes to the left of the Action's name. Alternatively, you can leave all the checkboxes unchecked to simply hold this action in reserve without applying it at the moment to any Notifications.

Play a sound file upon notification

You can play a sound of your choice in *.wav file format, either instead of or in addition to any other notification actions. The system on which AiroPeek is running must have the ability to play sound files in *.wav format in order to use this type of Action.

To create an Action of the type Sound:

1. Click the **Insert** button and in the **Edit Action** dialog that appears, use the pull-down menu for the *Type* parameter to select *Sound* to open the ***Sound*** view of the **Edit Action** dialog (Figure 12.11).



Action: Untitled Action

Type: Sound

Figure 12.11 Edit Action dialog for Sound action type

2. Fill in the *Play sound* text entry box or click the button on the right marked with the ellipses **...** to browse your system to locate and select the *.wav file you wish to play when this Action is invoked.
3. Give this Action a name (in the box labeled *Action*) and click **OK** to add it to the list of possible actions in the ***Notifications*** view.
4. Select which levels of severity of notification you would like to automatically perform this action, using the checkboxes to the left of the Action's name. Alternatively, click no checkboxes to simply hold this action in reserve without applying it at the moment to any Notifications.

Analysis Modules

Analysis Modules are external modules that provide additional highly focused analysis features to the program. An Analysis Module tests network traffic and provides detailed summaries and counts of key parameters of one specific type of traffic, posting its results in the **Summary Statistics** window and/or in the ***Summary*** column of the ***Packets*** view of Capture windows and Packet File windows.

Enabled Analysis Modules are applied to traffic captured in real-time and to packets in the buffer of a Capture window or a Packet File window. You can enable and disable Analysis Modules individually. In addition, many Analysis Modules have user-configurable options, which can be used to further refine the data you collect about your network.

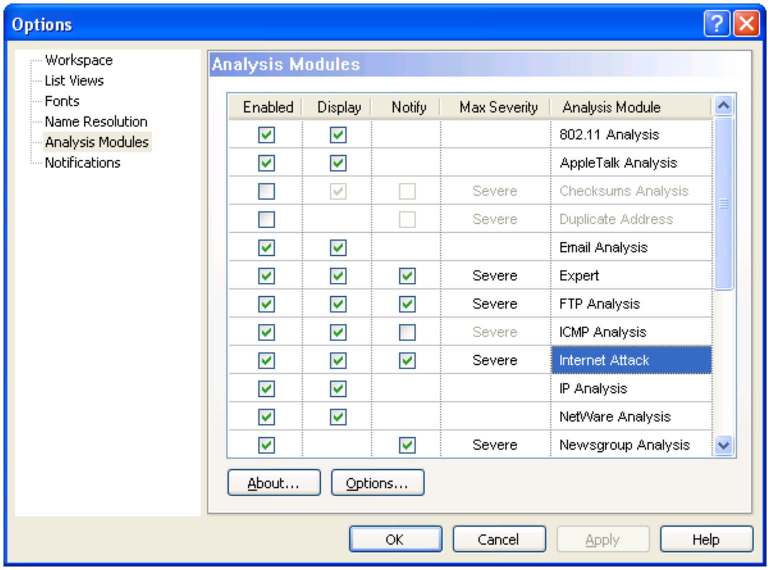
The Analysis Modules shipped with AiroPeek cover a wide range of the most common protocols and network applications. Users with some programming knowledge can use the accompanying SDK to write their own Analysis Modules, for example, to report on proprietary protocols or applications, or to present statistics of particular interest in their environment.

This chapter describes how to use Analysis Modules, and describes each of the Analysis Modules shipped with AiroPeek in detail.

In this Chapter:

Enabling and configuring analysis modules

To open the ***Analysis Modules*** view of the **Options** dialog, choose **Options…** from the **Tools** menu and click the *Analysis Modules* item in the navigation pane. The ***Analysis Modules*** view of the **Options** dialog shows a list of available Analysis Modules.



Enabled	Display	Notify	Max Severity	Analysis Module
☑	☑			802.11 Analysis
☑	☑			AppleTalk Analysis
☐	☑	☐	Severe	Checksums Analysis
☐		☐	Severe	Duplicate Address
☑	☑			Email Analysis
☑	☑	☑	Severe	Expert
☑	☑	☑	Severe	FTP Analysis
☑	☑	☐	Severe	ICMP Analysis
☑	☑	☑	Severe	Internet Attack
☑	☑			IP Analysis
☑	☑			NetWare Analysis
☑		☑	Severe	Newsgroup Analysis

Figure 13.1 Analysis Modules view of the Options dialog for AiroPeek NX

Important! Unlike triggers, capture buffers, and many other functions in AiroPeek, Analysis Modules are enabled and disabled *globally*. When an Analysis Module is enabled in the ***Analysis Modules*** view of the **Options** dialog, it is enabled simultaneously for any function in AiroPeek that could use the Analysis Module's added functionality. This includes Monitor statistics, Capture windows and Packet File windows.

Analysis Modules process packets each time the packets are loaded into a buffer. This means the same Analysis Module may process the same packet several times, but with the results posted to different places in AiroPeek, depending on which buffer is involved. AiroPeek maintains one buffer for Monitor statistics, and separate buffers for individual Capture windows or Packet File windows.

The buffer for Monitor statistics is the simplest, in that it is either on or off. Any time **Monitor Statistics** is enabled and an adapter is selected for Monitor statistics, AiroPeek captures Monitor statistics, and does so continuously while the program is running. The buffer for Monitor statistics is not affected by filters or packet slicing. It is simply on or off. Any enabled Analysis Module will have the opportunity to process the packets in this buffer exactly once: when they first enter the buffer.

The buffers for individual Capture windows and Packet File windows are different. Any enabled Analysis Modules are applied to packets as they arrive in the Capture window buffer from the network, or as they are loaded into a Packet File window buffer from a file. Analysis Modules are also re-applied each time the contents of the buffer is changed in any of these windows by hiding or unhiding packets. Filters can restrict which packets are accepted into the buffer of a Capture window. Packet slicing, by capturing only a part of each packet, can limit the information available to Analysis Modules.

Enable/disable the analysis module

To enable or disable an Analysis Module, check or uncheck the left-most checkbox beside its name, in the column labeled ***Enabled***.

Analysis module info in packet list summary columns

To allow the Analysis Module to write details about the packet to the ***Summary*** column of any Capture window or Packet File window, check the checkbox in the column labeled ***Display***.

Enable/disable notification

Enable notifications by checking the checkbox in the column labeled ***Notify***. This tells the Analysis Module to send notifications when it detects certain events. For more on associating notifications with actions, see “Notifications” on page 248. Notifications can be set to perform one or more of the following types of actions:

Log	Sends the notification to the Log File.
Email	Sends the notification in Email.
Execute	Executes a program of your choice.
Sound	Plays a sound file in *.wav file format on the local machine.

Set maximum severity of notification

Each Analysis Module assigns its own level of severity to each type of event it is able to detect. It tries to assign that pre-determined severity to any notification of that event. The last column of the ***Analysis Modules*** view of the **Options** dialog, labeled ***Max severity*** allows you to set an upper limit for the severity of the notifications coming from each particular Analysis Module, regardless of the level of severity the Analysis Module itself might have assigned to some event. The four levels of severity, from least to greatest are: *Informational*, *Minor*, *Major*, and *Severe*. If you enable notification for an Analysis Module and set the maximum severity to *Minor*, then notifications coming from that Analysis Module will be capped at *Minor*. If the Analysis Module then tries to send notifications of *Severe*, *Major*, or *Minor* severity; they will *all* be treated as *Minor*. If the Analysis Module sends a notification with a severity of *Informational*, it will be treated as *Informational*.

This capability is important for keeping notifications to a manageable level when many Analysis Modules are enabled. It also provides essential flexibility in using notifications to launch a variety of actions. For instance, although many administrators might find it convenient to have a log of all Web URLs accessed in the course of a day, few would want to be paged each time a new URL or web page is seen on the network. They might, however, want to be paged in the event of a notice of *Severe* from the InternetAttack Analysis Module. Please see “Notifications” on page 248 for more detail on associating notification severity levels with the different types of actions available in AiroPeek.

Configuring options for an analysis module

Some Analysis Modules have configurable options. For example, the Duplicate Address Analysis Module allows you to suppress redundant reports and, through its options, to enter physical addresses that you would like to have ignored. When any of these Analysis Modules with user-configurable options is highlighted, the **Options…** button at the bottom of the ***Analysis Modules*** view of the **Options** dialog will no longer be greyed out. Click the **Options…** button to open the **Options** dialog for the selected Analysis Module.

Quick info on analysis modules

The **About…** button in the lower left of the ***Analysis Modules*** view of the **Options** dialog displays an About Box for the selected Analysis Module. For information on the capabilities of each Analysis Module, see “Analysis modules shipped with AiroPeek” on page 262.

Apply analysis module command

Normally, Analysis Modules are applied to packets as they arrive in the buffer from the network, or as they are loaded from a file. Analysis Modules are also re-applied each time the contents of the buffer is changed by hiding or unhiding packets.

There are circumstances where it is useful to be able to apply Analysis Modules to one or more packets that are already in the buffer without having to re-apply all Analysis Modules to all packets.

For example, if you have just enabled a particular Analysis Module and you want to see its results for a group of packets but do not want to re-apply all enabled Analysis Modules to all packets in the buffer, select the packets to which you would like to apply the new Analysis Module, right click and choose that Analysis Module's name from the **Apply Analysis Module** list in the context menu.

A second reason to use the **Apply Analysis Module** command has to do with the mechanics of how Analysis Modules operate with respect to the ***Summary*** column in the ***Packets*** view of a Capture window or a Packet File window. There is only room for information from a single Analysis Module in the ***Summary*** column. When multiple Analysis Modules are enabled, they are applied in order, and the first Analysis Module to write to the ***Summary*** column is the only one whose information actually appears there. For example, the Web Analysis Module is normally applied before the IP Analysis Module. If both are enabled, you would normally not see any IP Analysis information for any packet that showed information in the ***Summary*** column provided by the Web Analysis Module. To overcome this, you can use the **Apply Analysis Module** command.

To apply the IP Analysis Module to selected packets in a Packet List:

1. Select the packet(s) to which you would like to apply the IP Analysis Module.
2. Right click, choose the **Apply Analysis Module** command from the context menu and select **IP Analysis** from the sub-menu.
3. This applies the IP Analysis Module to the selected packet(s) and allows the Analysis Module to write to the ***Summary*** column. Any other actions specified for this Analysis Module will also be taken, based on the results of processing the selected packets.
4. A message dialog appears showing the number of your selected packets which were processed by the Analysis Module you applied. If the dialog shows less than the whole number (for example *2 of 3 packets applied*), it means that the Analysis Module you

applied did not find the information for which it was designed to test in some of the packets you selected.

5. Click **OK** to close the message dialog.

Note: The order in which Analysis Modules are applied for purposes of writing to the ***Summary*** column, depends on how far into the packet the Analysis Module must reach to find the information for which it is testing. The deeper into the packet the Analysis Module must reach (or the larger the offset of the data for which the Analysis Module is testing), the earlier the Analysis Module is applied. The closer to the beginning of the packet (or the lower the offset of) the data for which the Analysis Module is testing, the later it will be applied.

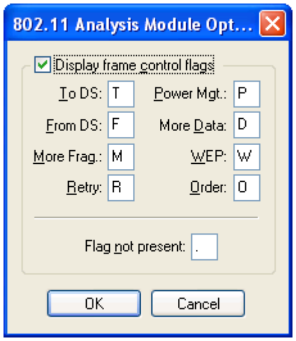
For information on using Analysis Modules to select captured packets, see “Select based on analysis modules” on page 315.

Analysis modules shipped with AiroPeek

Note: Registered users of AiroPeek are provided with a Software Development Kit for Analysis Modules. Analysis Modules can be written by any user with some programming knowledge. If you are interested in writing your own Analysis Modules, you can find the Analysis Modules SDK in the Documents directory in the directory where you installed AiroPeek.

802.11 analysis module

The 802.11 Analysis Module displays and logs the values found in the one-bit frame control fields of the 802.11 WLAN MAC headers. The **802.11 Analysis Module Options** dialog allows you to *Display frame control flags* in the ***Summary*** column of the ***Packets*** view of any Capture window or Packet File window by checking the checkbox at the top of the dialog. Uncheck this checkbox to disable display of these flag characters. The dialog allows you to assign the character AiroPeek will use as the flag character for each of the frame control parameters monitored by the Analysis Module. To change the character, type a new value in the text edit box beside any of the listed parameters. You can also assign a character to indicate null values for any of the frame control parameters by entering the character in the *Flag not present* text box. For a detailed description of the parameters contained in the frame control section, see “802.11 MAC header” on page A-27.



☑ Display frame control flags

To DS: T
Power Mgt.: P
From DS: F
More Data: D
More Frag.: M
WEP: W
Retry: R
Order: O

Flag not present: .

Figure 13.2 802.11 Analysis Module Options dialog

AppleTalk analysis module

The AppleTalk Analysis Module keeps track of and displays information about AARP requests, AARP responses, AARP probes, unanswered AARP requests, and the number of AppleTalk multicasts on your network. In addition, the AppleTalk Analysis Module shows details for NBP, ATP, and ASP. The AARP request shows AppleTalk address requested. The AARP response shows address and name. An ATP request shows transaction ID and Bitmap. An ATP response shows transaction ID and sequence number. ASP shows transaction ID, sequence number, and session ID. The results of the AppleTalk Analysis Module are displayed in the ***Summary*** column of the ***Packets*** view of any Capture window or Packet File window, and its counts are also used as some of the key baseline traffic elements provided in the **Summary Statistics** window.

Checksums analysis module

Many network error detection and correction techniques are based on checksums. The sender performs a computation on the data to be sent and the result, the checksum, is included with the transmission. The receiver performs the same computation on the data it receives and compares its results to the sender’s checksum. If a difference exists, the data is most likely corrupted, and the sender is asked to retransmit the data.

The Checksums Analysis Module verifies checksums and keeps track of the total number of invalid checksums for IP headers and data (including ICMP, IGMP, TCP, and UDP), and AppleTalk DDP data. Invalid checksums can be displayed in Capture and Packet File windows. This Analysis Module can send Notifications.

Note: In AiroPeek NX only, the Checksums Analysis Module is disabled by default, as the ***Expert*** view provides an overlapping functionality.

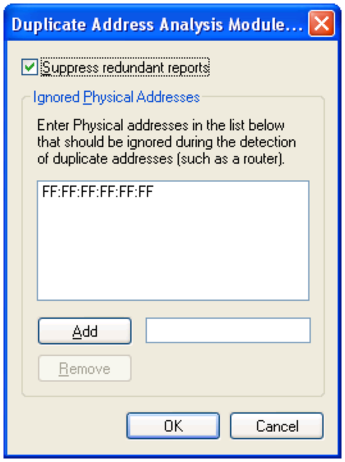
Conversations

The *Conversations* which appears in the ***Analysis Modules*** view of the **Options** dialog in AiroPeek standard is the ***Conversations*** view of Capture windows and Packet File windows. While not an Analysis Module in the ordinary sense, the ***Conversations*** view makes use of the Analysis Modules architecture to allow users to selectively enable and disable ***Conversations*** view functionality.

For complete details about the use of the ***Conversations*** view in AiroPeek standard, please see “Conversations” on page 183.

Duplicate address analysis module

The Duplicate Address Analysis Module displays and logs instances when two or more network devices are using the same IP address. When two distinct and separate physical addresses are noted by the Duplicate Address Analysis Module to be using the same logical IP address, the Analysis Module produces a Notification. The Duplicate Address Analysis Module also adds a count of duplicate IP addresses detected to the **Summary Statistics** window.


Duplicate Address Analysis Module...

☑ Suppress redundant reports

Ignored Physical Addresses

Enter Physical addresses in the list below that should be ignored during the detection of duplicate addresses (such as a router).

FF:FF:FF:FF:FF:FF

Figure 13.3 Duplicate Address Analysis Module Options dialog

To change options for this Analysis Module, select it in the ***Analysis Modules*** view of the **Options** dialog and click the **Options** button. To suppress redundant reports, enter the physical addresses of devices that should be ignored. By default, duplicate reports for the physical hardware broadcast address are suppressed.

The Duplicate Address Analysis Module is disabled by default. For the most accurate results, you should use the Name Table to identify routers on the local segment before enabling the Duplicate Address Analysis Module.

Note: Duplicate IP address notifications are usually caused by multiple routers. Because routers forward traffic from other networks at OSI Layer 3, the logical address (IP) is forwarded unchanged but the physical address (MAC) is changed to that of the router doing the forwarding. When there is more than one router on the local segment, AiroPeek may see multiple physical addresses associated with a single logical address, and send a Duplicate Address notification accordingly. To prevent these notifications from being triggered by legitimate traffic from local routers, you have two choices. You can enter the physical address of each router in the **Duplicate Address Analysis Module Options** dialog *Ignored Physical Addresses* list and check the *Suppress redundant reports* checkbox. Alternatively, you can use the Name Table to identify each router as such by assigning it a *Node Type* of *Router* in the **Edit Name** dialog. Please see Chapter 7, “Name Table” on page 129 for details. The program checks the Name Table for nodes identified as routers before generating a duplicate address notification.

Email analysis module

The Email Analysis Module displays SMTP and POP3 commands that can be helpful in debugging Internet mail problems. The Email Analysis Module reports on client/server connections by counting the number of mail transfers initiated, the number of successful transfers, and the number of failed transfers. It then delivers this information to the ***Summary*** column in the ***Packets*** view of any Capture window or Packet File window, and to the **Summary Statistics** window.

SMTP specifies the exact format of messages a client on one machine uses to transfer mail to a server on another. Communication between a client and a server consists of readable ASCII text.

First, the client establishes a reliable stream connection to the server and then waits for the server to send a 220 READY FOR MAIL message. If the server is overloaded, it may delay sending the 220 message temporarily. Once the 220 message is received by the client, the client sends a HELO command.

The server responds by identifying itself. Once communication has been established, the sender can transmit one or more mail messages, terminate the connection, or request the server to exchange the roles of sender and receiver so messages can flow in the opposite direction. The receiver must acknowledge each message. It can also suspend the entire connection or the current message transfer.

Mail transactions begin with the MAIL command that provides the sender identification as well as a FROM: field that contains the address to which errors should be reported. A recipient prepares its data structures to receive a new mail message and replies to a MAIL command by sending the response 250, which means all is well. The full response consists of the text 250 OK. As with other application protocols, programs read the abbreviated commands and 3-digit numbers at the beginning of lines; the remaining text is intended to help debug mail software.

After a successful MAIL command, the sender issues a series of RCPT commands that identify recipients of the mail message. The receiver must acknowledge each RCPT command by sending 250 OK or by sending the error message 550 No Such User Here.

After all RCPT commands have been acknowledged, the sender issues a DATA command. In essence, a DATA command informs the receiver that the sender is ready to transfer a complete mail message. The receiver responds with message 354 Start Mail Input and specifies the sequence of characters used to terminate the mail message. The termination sequence consists of 5 characters: carriage return, line feed, period, carriage return, and line feed.

Although clients can suspend the delivery completely if an error occurs, most clients do not. Instead, they continue delivery to all valid recipients and then report problems to the sender.

Usually, the client reports errors using electronic mail. The error message contains a summary of the error as well as the header of the mail message that caused the problem.

Once the client has finished sending all the mail messages to a particular destination, the client may issue the TURN command to turn the connection around. If it does, the server responds 250 OK and assumes control of the connection. With the roles reversed, the side that was originally the server sends back any waiting mail messages. Whichever side controls the interaction can choose to terminate the session by issuing a QUIT command. The other side responds with command 221, which means it agrees to terminate. Both sides then close the TCP connection.

Expert

The *Expert* which appears in the ***Analysis Modules*** view of the **Options** dialog in AiroPeek NX is the ***Expert*** view of Capture windows and Packet File windows. While not an Analysis Module in the ordinary sense, the ***Expert*** view makes use of the Analysis Modules architecture to allow users to selectively enable and disable part or all of the Expert Analysis functionality.

For complete details about the use of Expert Analysis in AiroPeek NX, please see Chapter 5, “Expert View and Expert ProblemFinder” on page 103.

FTP analysis module

The FTP Analysis Module provides the ability to:

- Report the number of successful file transfer initiations, completions and failures.
- Report and display the names of files that are being uploaded or downloaded.
- Report and display ftp commands (for example, ls, cd, and so forth).

The FTP Analysis Module also watches FTP control traffic for status messages that signal the successful start and end of a file transfer. A count is then added to the **Summary Statistics** window for these values. The FTP Analysis Module can also write these control messages to the ***Summary*** column of the ***Packets*** view of Capture windows and Packet File windows.

FTP can send an unsuccessful termination message. This condition is rare, but can be of interest to a network manager, especially if there is a high incidence of terminated sessions. Normally, failed FTP transactions are due to unexpected network delays or disruptions. Because a status packet does not usually accompany termination, the only way for a network manager to be aware of this condition is by monitoring the difference between the successful start and end of file transfers. A high discrepancy can signal not only potential network problems, but also additional loss of bandwidth due to unsuccessful transfers.

Network conditions specified by the FTP Analysis Module can be posted to the ***Summary*** column in the ***Packets*** view of any Capture window or Packet File window. In addition, the Analysis Module also produces notifications. The **Summary Statistics** window will also display key traffic elements relating to the processed output of the FTP Analysis Module.

ICMP analysis module

ICMP (Internet Control Message Protocol) is defined as a maintenance protocol that handles error messages to be sent when packets are discarded or when systems experience congestion. For instance, the classic TCP/IP test command is PING. It sends an ICMP Echo Request to a remote system. If the system responds, the link is operational. If it fails to respond to repeated pings, something is wrong.

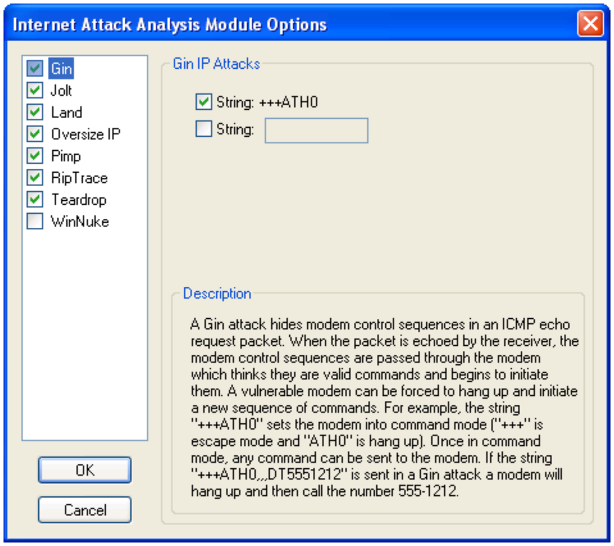
Another important function of ICMP is to provide a dynamic means to ensure that your system has an up-to-date routing table. ICMP is part of any TCP/IP implementation and is enabled automatically. ICMP messages provide many functions, including route redirection. If your workstation forwards a packet to a router, for example, and that router is aware of a shorter path to your destination, the router sends your workstation a redirection message informing it of a shorter route.

The ICMP Analysis Module keeps track of and displays information about ICMP destination unreachables, ICMP redirects, ICMP address mask replies, ICMP source quenches, and more. The Analysis Module can display ICMP type and code in the ***Summary*** column of the ***Packets*** view of any Capture window or Packet File window, as well as in the **Summary Statistics** window. This Analysis Module can send Notifications.

To change options for this Analysis Module, select it in the ***Analysis Modules*** view of the **Options** dialog and click the **Options** button. You can choose to log or to ignore ping (echo) packets because they are quite common. The default is to ignore echo packets, and the option is therefore unchecked.

InternetAttack analysis module

The InternetAttack Analysis Module collects eight common types of attacks and their variations into a single multi-view dialog. The **InternetAttack Analysis Module Options** dialog allows you to enable testing for all attacks, or to enable or disable individual parts of the Analysis Module. For flexibility of application, some attack Analysis Modules feature user-definable test parameters.



☑ Gin
☑ Jolt
☑ Land
☑ Oversize IP
☑ Pimp
☑ RipTrace
☑ Teardrop
□ WinNuke

Gin IP Attacks

☑ String: +++ATH0
□ String:

Description

A Gin attack hides modem control sequences in an ICMP echo request packet. When the packet is echoed by the receiver, the modem control sequences are passed through the modem which thinks they are valid commands and begins to initiate them. A vulnerable modem can be forced to hang up and initiate a new sequence of commands. For example, the string "+++ATH0" sets the modem into command mode ("+++" is escape mode and "ATH0" is hang up). Once in command mode, any command can be sent to the modem. If the string "+++ATH0,,,DT5551212" is sent in a Gin attack a modem will hang up and then call the number 555-1212.

Figure 13.4 InternetAttack Analysis Module Options dialog, Gin IP Attacks view

The InternetAttack Analysis Module can write to the ***Summary*** column in the ***Packets*** view of any Capture window or Packet File window. This Analysis Module can send Notifications.

The InternetAttack Analysis Module also adds a count of packets for each enabled type of attack to the **Summary Statistics** window.

Each type of attack covered by the Analysis Module is described below. Each section shows the protocol used, the date when the attack first appeared, and the types of systems reported as vulnerable to the attack. (These vulnerable systems are generally specified in the source code of the attack as tested by the author of the each attack. These were not tested and verified by WildPackets.) For each type of attack the description shows the incidence of false positives—legitimate traffic which happens to match the test criteria. Each describes the working of the attack and its results, then lists the packet characteristics and contents which will generate a positive match. These criteria are listed in the order in which they will be tested. All of the listed test criteria must be met, for the Analysis Module to respond with a notification of an attack of this type.

To change the options for the InternetAttack Analysis Module:

1. Select it in the ***Analysis Modules*** view of the **Options** dialog and click the **Options** button to open the **InternetAttack Analysis Module Options** dialog (Figure 13.4).
2. Enable or disable testing for each individual attack type, by checking or unchecking the checkbox next to the name of each.
3. Highlight the name of any individual attack to bring up all user-definable parameters for that test, along with a brief description of the type of attack.
4. Make any changes to the parameters for individual attack tests. Please see the description of the attack in the following section for details of user-definable parameters.
5. Click **OK** to accept your changes and close the **InternetAttack Analysis Module Options** dialog.

Gin IP attacks

Protocol: ICMP (Internet Control Message Protocol) **Date**: June 6, 1999

Vulnerable system configurations:

Systems on which all of the following are true:

- The system does not filter ICMP echo request (Ping) packets.
- The system knows how to reply to ICMP echo request (Ping) packets.
- The system is using a modem.
- The modem's guard time is set extremely low.

False Positives: None, for default character string. Modem control sequences are not a legitimate part of ICMP packets.

Description: A Gin attack hides modem control sequences in an ICMP echo request packet. When the packet is echoed by the receiver, the modem control sequences are passed through the modem which thinks they are valid commands and begins to act on them. A vulnerable modem can be forced to hang up and initiate a new sequence of commands. Once in command mode, any command can be sent to the modem, including instruction to dial any number.

Results: Attacker control of the defender’s modem.

Analysis Module tests for:

- ICMP packet

- ICMP Echo Request
- The character string “+++ATH0” (user definable)

Jolt IP attacks

Protocol: ICMP (Internet Control Message Protocol) **Date**: 1997

Vulnerable system configurations:

- Windows 95
- Old versions of Mac OS

False Positives: Very Rare. Any fragmented ICMP packet with the specific values of Identifier = 4321 and Fragmentation Offset = 45216 bytes (or the values defined by the user) will be marked as a Jolt attack. False positives are possible but unlikely, since only 1 in 536,870,912 fragmented ICMP packets will randomly have these values.

Description: A Jolt attack sends a large number of spoofed, fragmented, oversized ICMP packets. To deal with possible future variations on this attack, two key parameters are user definable.

Results: System freeze.

Analysis Module tests for:

- ICMP packet
- Fragmentation flag = 1
- Identifier = 4321 (user definable)
- Fragmentation Offset = 45216 bytes (user definable)

Land TCP attacks

Protocol: TCP/IP **Date**: November 20, 1997

Vulnerable system configurations:

- BSDI 2.1 (vanilla)
- FreeBSD 2.2.2-RELEASE
- FreeBSD 2.2.5-RELEASE
- FreeBSD 2.2.5-STABLE
- FreeBSD 3.0-CURRENT

- HP-UX 10.20
- MacOS 8.0 (TCP/IP stack crashed)
- NetBSD 1.2
- NeXTSTEP 3.0
- NeXTSTEp 3.1
- OpenBSD 2.1
- Solaris 2.5.1 (conflicting reports)
- SunOS 4.1.4
- Windows 95 (vanilla)
- Windows 95 + Winsock 2 + VIPUPD.EXE

Not vulnerable:

- BSDI 2.1 (K210-021,K210-022,K210-024)
- BSDI 3.0
- Digital UNIX 4.0
- IRIX 6.2
- Linux 2.0.30
- Linux 2.0.32
- Novell 4.11
- OpenBSD 2.2 (Oct31)
- SCO OpenServer 5.0.4

False Positives: Rare. TCP/ IP packets should not have their source and destination addresses set to the same value. Packets detected by this Analysis Module may not be Land attacks, but they are still improperly formed.

Description: A Land attack is a flood of packets with the Synchronize (SYN) flag set and the source IP Address and Port Number spoofed to be the same as the destination. Vulnerable systems can neither resolve these circular synchronize requests nor discard them quickly enough to avoid overload. When a large number of TCP open requests are left in the SYN state, TCP networking locks up on affected systems. UDP, including ICMP, continues to work, however.

There are three variations of the Land attack: Land, Blat, and LaTierra. In addition to setting the SYN flag, Blat also sets the Urgent (URG) flag and LaTierra also sets the Push (PSH) flag.

Results: TCP networking locks up.

Analysis Module tests for:

Land:

- TCP/IP packet
- Source and Destination IP Addresses are the same
- Source and Destination Ports are the same
- Synchronize flag (SYN) = 1

Blat (same as LAND, plus):

- Urgent flag (URG) = 1

LaTierra (same as LAND, plus):

- Push flag (PSH) = 1

Oversize IP attacks

Protocol: IP **Date**: January, 1997

Vulnerable system configurations:

- Older (pre-1998) operating systems
- Older (pre-1998) TCP/IP stacks

False Positives: None. The existence of oversized packets may not constitute an attack, but it is always an error.

Description: An oversize IP packet occurs when a packet's IP data size + Fragmentation Offset is greater than 65535. When attempting to reassemble such packets, some operating systems and TCP/IP stacks crash.

The maximum size of an IP packet is (2^16)-1 octets, or 65535 bytes. Because many network systems cannot accept packets this large (Ethernet, for example, sets a maximum packet size of 1500 bytes), IP allows packets to be fragmented and reassembled at the receiving end. Each fragment is assigned an offset to define its place in the original packet. The offset of the first fragment is 0, the offset of the second fragment is the length (in bytes) of the first fragment, and so on. It is possible to create a fragment which is itself of a normal size, but which has an offset such that the size of the rogue packet plus its offset is greater than 65535 bytes. Many older implementations of TCP/IP do not attempt to reassemble packets until all the fragments have been received. When these systems attempt to reassemble an oversized packet, processing overflows occur which freeze or otherwise derange the system.

Early Microsoft implementations of the Ping (ICMP echo request) tool were likely to generate such illegally large IP packets. Other versions of these tools could easily be modified to do so deliberately. Although oversize IP packets and the attacks built around them are certainly not limited to Ping, these events from around 1996 and 1997 gave the name “Ping of Death” to this type of attack.

Results: Varies by system: system crash, system freeze, reboot, etc.

Analysis Module tests for:

- IP packet
- IP data size + Fragmentation Offset > 65535

Pimp IP attacks

Protocol: IGMP (Internet Group Management Protocol) **Date**: June 4, 1999

Vulnerable system configurations:

- Windows 95

False Positives: Rare. Any fragmented IGMP packet with the specific values of IP Address equal to 96.37.250.127, Identifier equal to 17664, and Fragmentation Offset equal to 7400 bytes (or the values defined by the user) will be marked as a Pimp attack. False positives are possible but unlikely, since only 1 in 2.30 x10^18 fragmented IGMP packets will randomly have these values.

Description: A Pimp attack sends a large number of spoofed, fragmented, oversized, IGMP packets. The default values represent the version of this attack seen today, but several key values are user-definable to enable the Analysis Module to be modified to address possible future variations on this attack.

Results: System crash

Analysis Module tests for:

- IGMP packet
- Identifier = 17664 (user definable)
- Fragmentation Offset = 7400 bytes (user definable)
- IP Address = 96.37.250.127 (user definable)

RipTrace IP attacks

Protocol: UDP (User Datagram Protocol) **Date**: 1997

Vulnerable system configurations:

- Linux 2.0.x
- RedHat - Routed checks if RIP packet comes from a valid router. Can always spoof the router's IP.

Not vulnerable:

- Solaris 2.6 - ignores the packet and returns the following error:
  `in.routed[6580]: trace command from 1.2.3.4 - ignored`

False Positives: None, for default character string.

Description: A RipTrace attack is a special RIP (Router Information Protocol) packet that commands routed (the UNIX routing daemon) to be in debug mode. Once in this mode, routed can be commanded to append to any file on the file system. By default, the Analysis Module tests for the “/” character used to begin a UNIX file path. To accommodate other operating systems and environments, this value is user definable.

Results: Any file on the attacked system can be appended to. Extremely dangerous!

Analysis Module tests for:

- UDP
- Source port = 520 (RIP)
- Destination port = 520 (RIP)
- Trace mode is on
- The character string “/” (the beginning of a file path) (user definable)

Teardrop IP attacks

Protocol: UDP (User Datagram Protocol) **Date**: March 11, 1997

Vulnerable system configurations:

- Windows 95
- Windows NT 4.0 w/ Service Pack 3
- Linux (1.x - 2.x, including the development kernels)

False Positives: Rare. A fragmentation offset less than 6 is valid but extremely unlikely. A fragmentation offset of 6 would mean the packet passed over a network segment with a *maximum* frame size of 42 bytes. This is less than Ethernet's *minimum* frame size of 64 bytes.

Description: A Teardrop attack sends two fragmented packets designed such that the fragmentation offset plus the UDP data size of the second packet is less than the size of the first packet. Thus, the end of the second packet is inside the first packet.

The attack is successful on systems that reassemble packet fragments without carefully checking the end points. These systems blindly subtract the second endpoint from the first, which, in this attack, results in a negative number. The computer considers the negative number unsigned, which means it is actually so large that it overflows the memory buffer set aside for packet fragment reassembly.

Results: System crash.

There are several variations of the Teardrop attack:

Analysis Module tests for:

- Teardrop: UPD packet, UDP Length =48, Fragmentation Offset = between 0 and 6
- Newtear: UPD packet, Fragmentation Offset = between 0 and 6
- SSPing: UPD packet, Fragmentation Offset = 1, Type of Service (ToS) =%00000000 (Precedence: Routine, Normal Delay, Normal Throughput, Normal Reliability)
- Flushot: UPD packet, Fragmentation Offset = 1, Type of Service (ToS) =%00000010 (Maximum Reliability)
- Nestea: UPD packet, Fragmentation Offset = 6
- Bonk: UPD packet, Port = 53, Fragmentation Offset = 4
- Boink: UPD packet, Fragmentation Offset = 4

WinNuke TCP attacks

Protocol: TCP/IP **Date**: May 7, 1997

Vulnerable system configurations:

- Windows 95 without Windows Sockets Version 3
- Windows NT 3.51 without Service Pack 5 and the “oob-fix” hot fix

- Windows NT 4.0 without Service Pack 3 and the “teardrop2-fix” hot fix

False Positives: Likely. The use of Out of Band data is valid, and the TCP protocol provides for this with the Urgent flag. Such packets are a normal if not frequent part of network traffic. If no vulnerable machines are on the network, the Analysis Module can and probably should be disabled.

Description: A WinNuke attack sends a few bogus TCP/IP packets followed by one with the Urgent (URG) flag set. Windows networking did not handle URG flags and either lost connection to the network or crashed the whole system.

The Urgent flag, along with the Urgent Pointer, are the TCP mechanism for sending “Out of Band” (OOB) data which provides a way for a packet to hop the queue and be immediately processed. This is a useful way of allowing an interrupt signal to stop the processing of network data, or for control commands to be sent to an application while its buffers are full.

A WinNuke attack must be sent to an open port on the defender's computer. This is usually port 139 (NetBIOS) but can be any open port. Other commonly attacked ports are 113 (Ident) and 135 (Epmap). WinNuke is also referred to as WinBlow, which is a version of WinNuke written to run on Windows, to attack other Windows OS machines.

Results: Lost network connection or system crash.

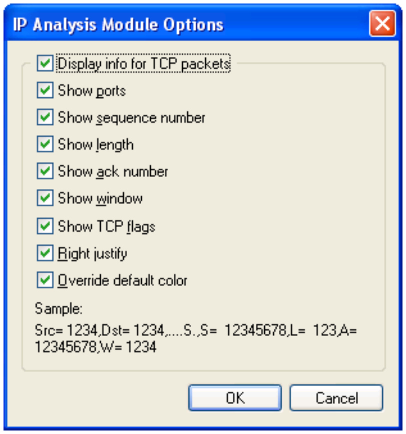
Analysis Module tests for:

- TCP/IP packet
- Urgent flag (URG) = 1

Note: Because of the relatively higher chance of false positives, the WinNuke is disabled by default.

IP analysis module

The IP Analysis Module keeps track of and displays information about requests and responses from ARP, RARP, DHCP, and DNS; and TCP sequence numbers, acknowledgement numbers, windows, and flags, as well as TCP and UDP port numbers. Address Resolution Protocol (ARP) dynamically discovers the physical address of a device, given its IP address. Reverse Address Resolution Protocol (RARP) enables a device to discover its IP address by broadcasting a request on the network. Dynamic Host Configuration Protocol (DHCP) provides clients with a dynamically assigned IP address and other network configuration setting parameters. Domain Name System (DNS) is a set of distributed databases providing information such as the IP addresses corresponding to network device names, and the location of mail servers.



☑ Display info for TCP packets
☑ Show ports
☑ Show sequence number
☑ Show length
☑ Show ack number
☑ Show window
☑ Show TCP flags
☑ Right justify
☑ Override default color

Sample:
Src= 1234,Dst= 1234,....S.,S= 12345678,L= 123,A= 12345678,W= 1234

Figure 13.5 IP Analysis Module Options dialog

A Sequence number is a 32-bit field of a TCP header. If the segment contains data, the Sequence number is associated with the first octet of the data. TCP requires that data is acknowledged (given an Acknowledgement number) before it is considered to have been transmitted safely. TCP maintains its connections within a series of TCP windows established by the protocol. TCP packets may contain flags to denote a variety of conditions or protocol functions.

Results of the IP Analysis Module are displayed in the ***Summary*** column in the ***Packets*** view of any Capture window or Packet File window, and its counts are used as some of the key baseline traffic elements provided in the **Summary Statistics** window.

Options for this Analysis Module, all of which are enabled by default, are to show: ports, sequence number, length, ack number, window and TCP flags. Also enabled by default are the display options of *Right justify*, which makes the numbers line up correctly when seen in the ***Packets*** view, and *Override default color*, which shows information from this Analysis Module in grey in the ***Summary*** column of the ***Packets*** view.

NetWare analysis module

The NetWare Analysis Module provides information on unanswered RIP, SAP, and NCP requests to the **Summary Statistics** window and displays hop and tick counts for RIP packets, Sequence and Acknowledgement numbers for SPX, function and return codes for NCP packets, and service names for SAP packets in the ***Summary*** column in the ***Packets*** view of any Capture window or Packet File window.

Newsgroup analysis module

The Newsgroup Analysis Module displays and logs accesses to newsgroups and provides these counts to **Summary Statistics**. Anytime a newsgroup is accessed over the network by way of NNTP, the Analysis Module will generate a Notification noting the specific newsgroup name and the date and time of the access event.

Peer map

The *Peer Map* which appears in the ***Analysis Modules*** view of the **Options** dialog in AiroPeek NX is the ***Peer Map*** view of Capture windows and Packet File windows. While not an Analysis Module in the ordinary sense, the ***Peer Map*** view makes use of the Analysis Modules architecture to allow users to selectively enable and disable Peer Map functionality.

For complete details about the use of the ***Peer Map*** view in AiroPeek NX, please see Chapter 6, “Peer Map” on page 121.

RADIUS analysis module

The RADIUS Analysis Module provides statistics and decode summaries for Remote Access Dial-up User Services (RADIUS) and RADIUS accounting packets, including summaries for Access Request, Accept, and Reject packets; Accounting Request and Response packets; Access Challenge; and RADIUS Start and Stop packets.

RFGrabber

The *RFGrabber* which appears in the ***Analysis Modules*** view of the **Options** dialog in AiroPeek is the built-in software support for configuring, controlling, and communicating with the separately purchased RFGrabber Probe. You can enable or disable the RFGrabber functionality in AiroPeek as a whole from within AiroPeek by enabling or disabling the *RFGrabber* item in the ***Analysis Modules*** view of the **Options** dialog.

For complete details about the RFGrabber probe and how it is used in AiroPeek, please see Chapter 14, “RFGrabber Probe” on page 283.

SMB analysis module

The SMB Analysis Module tracks many of the most common commands, status messages, and other responses for the Server Message Block protocol. It displays information about these SMB transactions in the ***Summary*** column of the ***Packets*** view of any Capture window or Packet File window. SMB is essentially an extended and enhanced file management protocol. Conceptually, the protocol treats files, printers, and named pipes as file objects which can be opened, closed, and modified.

Check the checkbox in the **SMB Analysis Module Options** dialog to *Show SMB command descriptions* in the ***Summary*** column in the ***Packets*** view and in the **Summary Statistics** window.

SQL analysis module

The SQL Analysis Module provides decode summaries for TNS and TDS traffic. Structured Query Language (SQL) is a widely used standard for querying databases. When using SQL over a network, the queries and data are carried within special protocols, where the type of protocol used depends on the type of database environment. Oracle environments use Transparent Network Substrate (TNS). Sybase and Microsoft SQL Server environments use the Tabular Data Stream protocol (TDS).

The module provides TDS descriptions including Login, RPC, and SQL summary strings. For TNS, the module provides decode summaries for TNS Connect, Accept, Refuse, Redirect, Data, Abort, Resend, Marker, and Control packets.

Telnet analysis module

The Telnet Analysis Module displays the contents of telnet sessions in the ***Summary*** column in the ***Packets*** view of any Capture window or Packet File window.

Telnet is a TCP/IP protocol that enables a terminal attached to one host to log in to other hosts and interact with their resident applications.

VoIP analysis module

The VoIP Analysis Module provides detailed information on traffic related to Voice over IP (VoIP). Specifically, the module provides statistics and decode summaries for MGCP, SIP, RTCP, G.723, H.323, H.225, G.711 traffic. The VoIP Analysis Module also follows

H.245 connections based on H.323 port/IP connection data to provide statistics and decode summaries.

Web analysis module

The Web Analysis Module displays and logs access to World Wide Web resources. Anytime a Web URL is accessed over the network, the specific website location can be logged in the log file, noting date and time, and an email can be sent to inform the network manager of the access event (all by way of Notifications). The results can also be displayed in the ***Summary*** column in the ***Packets*** view of any Capture window or Packet File window.

The Web Analysis Module also adds a count of URLs accessed in the **Summary Statistics** window.

Tip Double-click on any URL posted to the Log file by the Web Analysis Module to open that resource in your default browser.

Note: In environments with significant Web traffic, the Web Analysis Module can write substantial amounts of information to the AiroPeek Log. You may want to disable the Web Analysis Module in such cases to prevent the Log file from growing too large, too quickly.

RFGrabber Probe

This chapter explains how to set up and configure the separately purchased RFGrabber Probe hardware, and how to use the probe to extend AiroPeek's monitoring and analysis capabilities.

The RFGrabber Probe is an Ethernet connected device that acts like a "listen-only" access point, allowing you to capture and monitor WLAN traffic in a remote location and stream the results to AiroPeek via TCP/IP. You can connect to any network accessible RFGrabber Probe just as you would to any other network adapter: by selecting it in the ***Adapter*** view of either the **Monitor Options** or the **Capture Options** dialog.

In this Chapter:

RFGrabber Overview

With RFGrabber, you can capture 802.11b WLAN packets at a remote RFGrabber Probe connected anywhere along your wired network, and stream those packets (encapsulated in UDP) back to a copy of AiroPeek running on any network accessible computer.

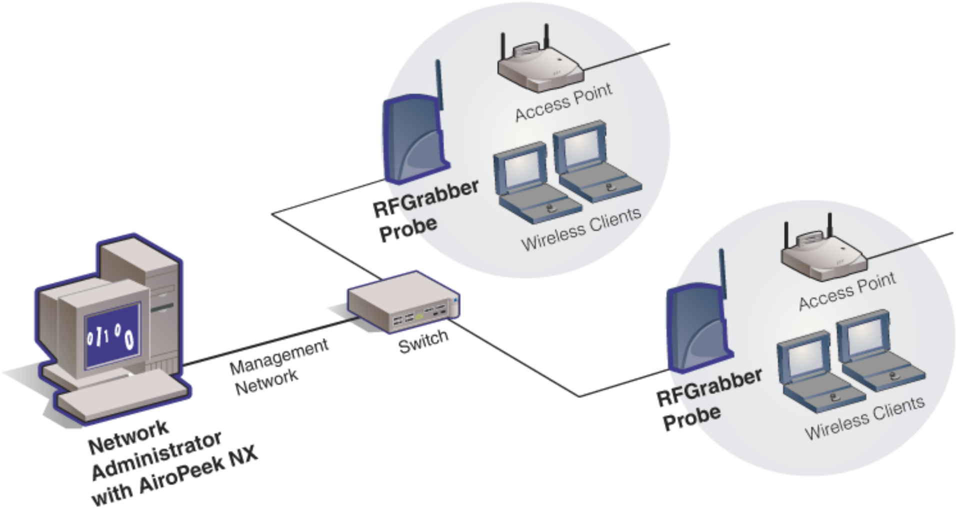


Figure 14.1 AiroPeek NX with two RFGRabber Probes

How RFGrabber works

The RFGrabber Probe acts like a “listen-only” 802.11b WLAN access point that captures local 802.11b WLAN traffic and streams it back to AiroPeek. The captured packets are encapsulated in UDP. AiroPeek treats each RFGrabber Probe as a network adapter, allowing you to use the probe as a source for Monitor statistics, Capture window(s), or both simultaneously.

The RFGrabber Probe connects to your existing Ethernet network and communicates with AiroPeek using IP. You can use AiroPeek to configure an individual probe, setting the probe’s use of channels, channel scanning, WEP decryption, and a basic set of filters. Traffic matching the probe configuration is streamed back to AiroPeek, encapsulated in UDP. AiroPeek unwraps the packets and treats them like the traffic found on any other adapter.

System requirements

The RFGrabber Probe requires either AiroPeek 2.0 or AiroPeek NX 2.0 in order to configure and use the device. In addition, the RFGrabber Probe uses IP over Ethernet to communicate. The probe is equipped with a 10 Mbps Ethernet adapter, allowing you to use an inexpensive 10 Mbps hub or 10/100 Mbps switch to connect it to your network. The probe must be connected to an Ethernet network, and the machine on which AiroPeek is running must be able to communicate with the probe via TCP/IP.

RFGrabber as an analysis module

AiroPeek uses the Analysis Modules architecture to interact with the RFGrabber Probe. The *RFGrabber* which appears in the ***Analysis Modules*** view of the **Options** dialog in AiroPeek is the built-in software support for configuring, controlling, and communicating with the RFGrabber Probe. You can enable or disable the RFGrabber functionality in AiroPeek as a whole from within AiroPeek using this view. Choose **Options…** from the **Tools** menu to open the **Options** dialog, then click the *Analysis Modules* item in the navigation pane to open the ***Analysis Modules*** view. To enable or disable RFGrabber, check or uncheck the left-most checkbox beside its name, in the column labeled ***Enabled***. Click **OK** to accept your changes and close the dialog.

Assembling and Configuring the RFGrabber Probe

This section describes how to assemble a new RFGrabber Probe, how to configure the probe for its first use, and how to use other options to change the probe’s configuration after it is deployed, how to set filters on the probe, and more.

New probes ship with the same settings for name, address, and other parameters. You will want to use AiroPeek to configure each new probe before you deploy it on your network.

Important! Probes set to the factory defaults use an Autocol protocol for probe discovery and are set to get their IP address from DHCP. In order to configure a probe that is set to factory defaults, AiroPeek must be in the same broadcast domain as the new probe. Additionally, if DHCP is not available, you must use AiroPeek to give the probe a static IP address.

Hardware setup

Unpack your RFGrabber Probe from the box. You should find:

- RFGrabber Probe main unit

- external antenna
- power supply (US)
- short Ethernet cable

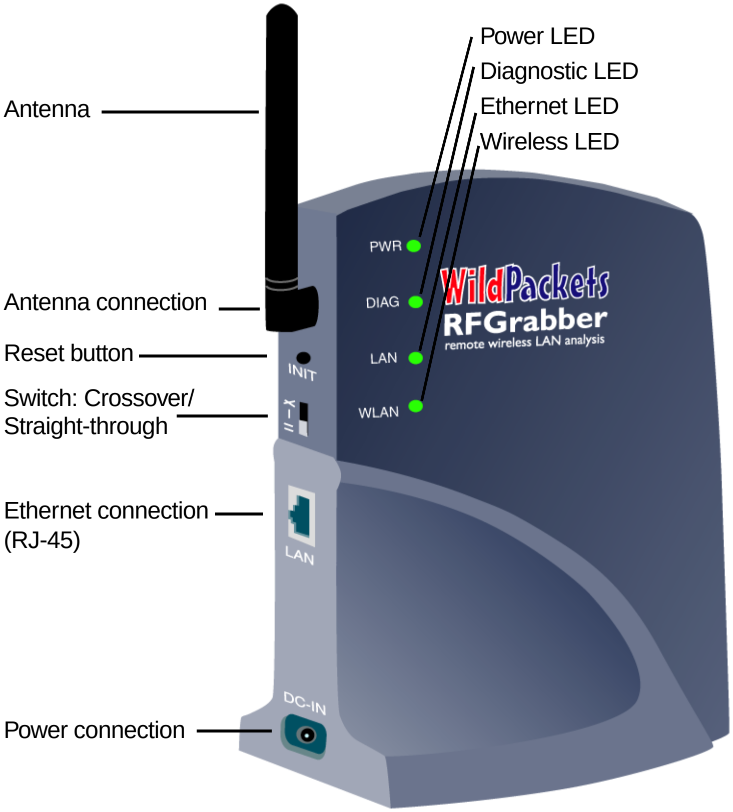


Figure 14.2 The RFGrabber Probe

1. Connect the antenna to the main unit by screwing it onto the gold connector.

   To initially configure your RFGrabber Probe, it should be connected to the same local network broadcast segment as the computer on which AiroPeek is running.

2. Connect one end of a standard Ethernet cable to the back of the RFGrabber Probe and the other end to a 10 Mbps hub or switch port on the same local segment as the computer on which AiroPeek is running. Alternatively, you can connect the RFGrabber Probe directly

to the AiroPeek PC. Please see “Direct connection using the crossover switch” below for details.

3. Plug in the power supply and connect it to the back of the RFGrabber Probe.

CAUTION! It is important to use the supplied power supply, or an equivalent 5V DC, 1A center positive power supply. Connecting a different power supply may damage your RFGrabber Probe and be a fire risk.

4. You should see the green **PWR** light turn on. After a brief delay both the **WLAN** and **LAN** lights should go green as well. The **DIAG** LED will not go on at this time.
5. The RFGrabber Probe is now ready to be configured using AiroPeek.

   If the **LAN** indicator does not go on, this may be because the Ethernet cable is not connected, or the cable type is incorrect. On the back of the RFGrabber Probe is a switch to allow selection of a straight-through (||) or crossover (X) Ethernet connection. Try moving the switch to the other setting. Using an ordinary Ethernet cable, this switch should be in the straight-through position to connect to a hub or switch.

Direct connection using the crossover switch

To configure a probe, you can connect the RFGrabber Probe directly to the PC running AiroPeek. On the back of the RFGrabber Probe is a switch which will allow you to select between a crossover connection (marked X) or a straight-through connection (marked ||). Use the crossover setting to connect the RFGrabber Probe directly to another PC using an ordinary Ethernet cable. Use the straight-through setting when the RFGrabber Probe is connected to an Ethernet network in the ordinary way, such as through a hub, switch, or router.

Adding a probe on the local network

AiroPeek (version 2.0) includes all the software you need to configure and use the RFGrabber Probe. You must use AiroPeek to manage and use your RFGrabber Probe.

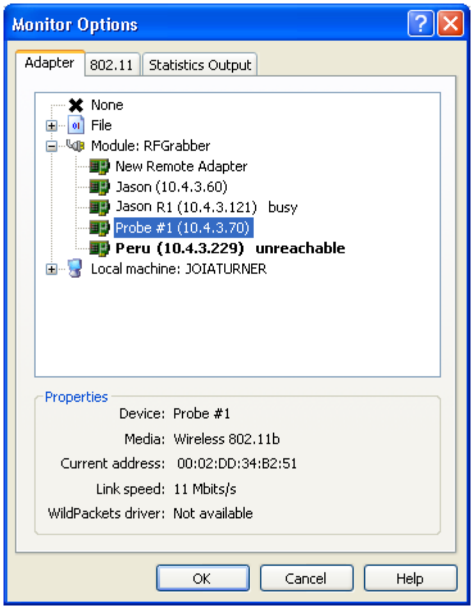
To add a new RFGrabber Probe to AiroPeek for the first time:

1. Assemble the RFGrabber Probe, connect it to the network, and power it up, following the instructions above.

2. Using a computer that is on the same local Ethernet segment as the new RFGrabber Probe, launch AiroPeek (version 2.0).

   AiroPeek treats the RFGrabber Probe as an adapter which can be used by Monitor statistics, Capture windows, or both. In order to use or configure the RFGrabber Probe, you must first add the probe to the ***Adapter*** view of either the **Monitor Options** or the **Capture Options** dialog. The ***Adapter*** view of both dialogs is identical and provides the same functions. Changes made to an individual RFGrabber Probe in either dialog will affect all uses of that probe, whether for Monitor statistics or Capture window(s) or both.

3. Choose **Select Monitor Adapter…** from the **Monitor** menu to open the **Monitor Options** dialog with the ***Adapter*** view displayed.

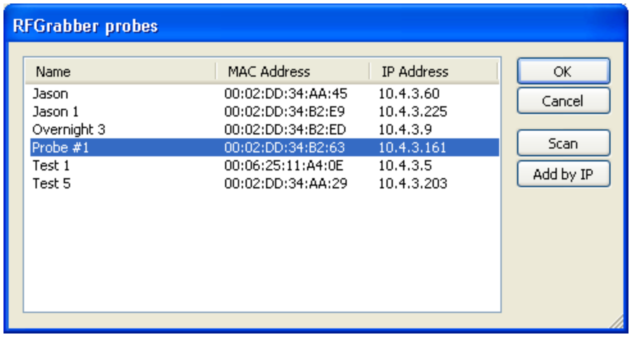


Device: Probe #1
Media: Wireless 802.11b
Current address: 00:02:DD:34:B2:51
Link speed: 11 Mbits/s
WildPackets driver: Not available

Figure 14.3 Adapter view of the Monitor Options dialog, showing RFGrabber Probe

4. In the list of adapters, expand the *Module: RFGrabber* item to display the *New Remote Adapter* item. Any previously added RFGrabber Probes will also be shown here, under the names you assigned to them.

5. Double-click on *New Remote Adapter* to open the **RFGrabber Probes** dialog (Figure 14.4).



Name	MAC Address	IP Address
Jason	00:02:DD:34:AA:45	10.4.3.60
Jason 1	00:02:DD:34:B2:E9	10.4.3.225
Overnight 3	00:02:DD:34:B2:ED	10.4.3.9
Probe #1	00:02:DD:34:B2:63	10.4.3.161
Test 1	00:06:25:11:A4:0E	10.4.3.5
Test 5	00:02:DD:34:AA:29	10.4.3.203

Figure 14.4 RFGrabber Probes dialog, showing available probes

6. When you open the **RFGrabber Probes** dialog, AiroPeek automatically scans for RFGrabber Probes on the local network and displays the results in the table. The new probe should appear under its default name: *Probe #1*.

Tip If the probe does not appear, click the **Scan** button to ask AiroPeek to search for probes again. Verify that the RFGrabber Probe is connected to the same network segment as the PC and that the **PWR**, **LAN**, and **WLAN** lights on the RFGrabber Probe are all green.

7. Highlight the new probe in the **RFGrabber Probes** dialog and click the **OK** button to add the probe to AiroPeek.

8. AiroPeek checks an attribute of the probe address properties called the *Community* string before adding the selected probe to the ***Adapter*** view. If the community string is still set to its default value (*public*), the probe will be added without challenge. If any other community string is discovered, AiroPeek will present a dialog asking you for the community string of the selected RFGrabber Probe. You must enter the correct *Community* string in order for AiroPeek to add the RFGrabber Probe to the ***Adapter*** view.

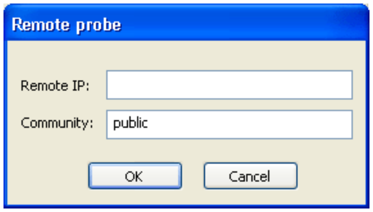
   Now that the probe is added to the ***Adapter*** view, you can set its name, address, and other properties. At a minimum, you will want to give the probe a new name. For a complete description of how to set probe properties, please see “Setting RFGrabber Probe properties” on page 292.

Important! If you do not have DHCP enabled on your network, or if you anticipate accessing the probe from outside a local broadcast domain, then you *must* set a static IP address for the probe in its initial configuration. Please see “Using static IP addresses” below for details.

It is only necessary to add a new probe once; AiroPeek will remember the probe from then on. Multiple probes can be added by repeating the preceding steps. For more on adding multiple probes, see “Support for multiple probes” on page 301.

Adding a probe on a remote network

The automatic probe discovery protocol used by AiroPeek will only work within a network broadcast domain. If you want to add a probe from another network to AiroPeek, you need to specify the probe’s IP address. In the **RFGrabber Probes** dialog, click the **IP Address** button to open the **Remote Probe** dialog (Figure 14.5). Type in the *Remote IP* address or host name of the probe, enter the *Community* string (the default is *public*), and click **OK**. If the probe can be reached, it will be added to the list in the **RFGrabber Probes** dialog and you can select it as normal. If the probe cannot be reached, the **RFGrabber Probes** dialog will report *Probe not found*.



Community: public

Figure 14.5 Remote Probe dialog

Firewall considerations

The RFGrabber Probe uses three different protocols to communicate with AiroPeek, all of which are carried in UDP packets. These protocols are shown in Table 14.1.

If the probe is on the WAN side of the NAT (Network Address Translation) device, and AiroPeek is on the LAN side, then the probe will work without any special consideration. If the probe is on the LAN side, and AiroPeek is on the WAN side, then port forwarding (virtual server) entries must be created, as shown in Table 14.1.

Table 14.1 **Protocols used by RFGrabber Probe**

Autocol	(AUTOmatic device discovery protoCOL) This protocol is used to discover RFGrabber Probes and configure their IP address. It uses IP broadcasts and UDP port 44033. This protocol cannot discover probes through NAT (Network Address Translation) devices.
public port	44033
private port	44033
private address	probe IP address
protocol	UDP
SNMP	(Simple Network Management Protocol) Used to configure the RFGrabber Probe. Uses UDP port 161.
public port	161
private port	161
private address	probe IP address
protocol	UDP
TZSP	(TaZmen Sniffer Protocol): Uses port 37008. Transports captured packets from probe to PC, and keep alive packets from PC to probe.
public port	37008
private port	37008
private address	probe IP address
protocol	UDP

In addition to the protocols listed above, the RFGrabber Probe firmware upgrade function uses TFTP (Trivial File Transfer Protocol), which uses port 69.

Using static IP addresses

The RFGrabber Probe can use either a DHCP assigned IP address or a static IP address. By default, the RFGrabber Probe is set to use DHCP. When AiroPeek and the probe are on the same local Ethernet segment, this will work very well. If you want to access the probe from outside the local broadcast domain, however, we recommend that you assign the probe a static IP address. One reason for this is that the Scan function cannot look beyond the local broadcast domain. If a probe is outside the local broadcast domain, you will need to know its IP address in order to access the probe from AiroPeek.

In order to set the name and address properties for a probe, you must first list the probe in the ***Adapter*** view of either the **Monitor Options** or the **Capture Options** dialog. If the probe is not already listed there, scan for and add the probe, following the steps above. Please see “Adding a probe on the local network” on page 287.

To configure a probe to use a static IP address:

1. Select the probe in the ***Adapter*** view of either the **Monitor Options** or the **Capture Options** dialog.
2. Right click and choose **Properties** from the context menu.
3. Click the *Address* tab to open the ***Address*** view of the **Remote Probe Properties** dialog.
4. Click the radio button beside *Use the following IP address*.
5. Enter a valid *IP address* in dotted decimal notation.
6. You may also enter a *Subnet mask* and *Default gateway,* as appropriate.
7. Click the **Apply** button to make your changes without closing the dialog or click **OK** to accept the changes and close the dialog.

Setting RFGrabber Probe properties

You can change the name and address properties and set filters on any RFGrabber Probe shown in the ***Adapters*** view of either the **Capture Options** or the **Monitor Options** dialog.

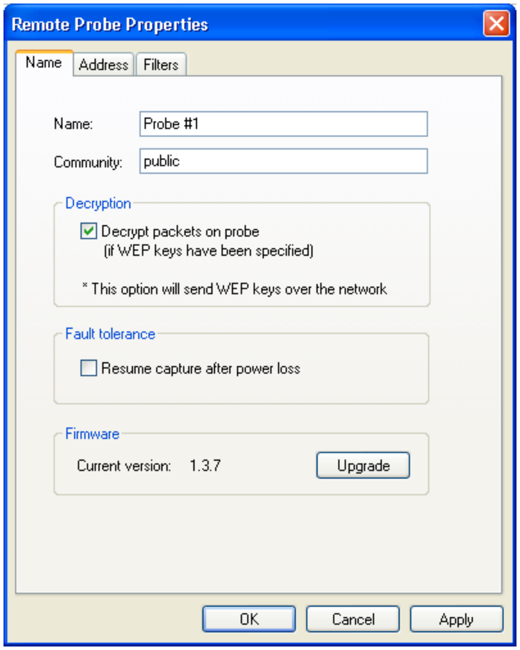
In the ***Adapter*** view, select the probe whose properties you wish to change. Right-click and choose **Properties** from the context menu to open the **Remote Probe Properties** dialog for that probe. The **Remote Probe Properties** dialog has three views: ***Name***, ***Address***, and ***Filter***. Each of these views is described in detail in the following sections.

Use the labeled tabs to switch between views. When you have made your changes, click the **Apply** button to make your changes without closing the dialog or click **OK** to accept the changes and close the dialog.

Name properties

In the ***Name*** view (Figure 14.6), you can set the *Name*, *Community* string, use of *Decryption*, and *Fault tolerance* properties for the probe. This view also provides the mechanism for updating the *Firmware* on a probe.

Enter a *Name* and/or a *Community* string for the probe in the appropriate text entry boxes. The *Name* is the name under which the probe will appear in the ***Adapters*** view. The default name is *Probe #1*. The default *Community* string for a new RFGrabber Probe is *public*. When you select a remote probe, the *Community* string you enter in the **Remote Probe** dialog must match the value entered here. If there is a mismatch, the probe will not permit a connection. This provides a very modest level of security.



Name: Probe #1

Community: public

Decryption

☑ Decrypt packets on probe
(if WEP keys have been specified)

* This option will send WEP keys over the network

Fault tolerance

□ Resume capture after power loss

Firmware

Current version: 1.3.7

Figure 14.6 Remote Probe Properties dialog, Name view

You can set the RFGrabber Probe to perform decryption of WEP encrypted packets before they are streamed to AiroPeek. When you check the checkbox beside *Decrypt packets on probe*, AiroPeek will check the settings in the ***802.11*** view of the current options dialog (**Monitor Options** or **Capture Options**) and relay the key set defined and selected there to the current RFGrabber Probe. The RFGrabber Probe supports both 64 bit and 128 bit WEP keys.

Note: Unlike AiroPeek, the RFGrabber Probe does not remember WEP keys from one session to the next. If you wish to decrypt packets on the probe, you must re-assign WEP keys for each new capture session with the RFGrabber Probe.

Important! When you select the *Decrypt packets on probe* option, WEP keys are sent to the RFGrabber Probe in the clear. If you are using a probe outside your local network, you should perform any WEP decryption on AiroPeek rather than on the probe.

The *Fault tolerance* section of the ***Name*** view lets you *Resume capture after power loss* on the RFGrabber Probe by checking that checkbox. When fault tolerance is enabled, all the probe properties assigned in the **Remote Probe Properties** dialog are burned to flash ROM on the probe each time they are updated. When fault tolerance is enabled, the RFGrabber Probe will return to the settings last flashed to ROM any time the power to the probe is cut and restored. If AiroPeek is still attempting to stream packets from the probe when the probe’s power is restored, the probe will resume the session with the previously saved configuration.

Important! Flash ROM is an expendable resource. You can update the Flash ROM a large, but finite, number of times. To avoid expending this capability unnecessarily, we recommend that you only enable fault tolerance when performing an extended capture, or in other circumstances where the feature is really needed.

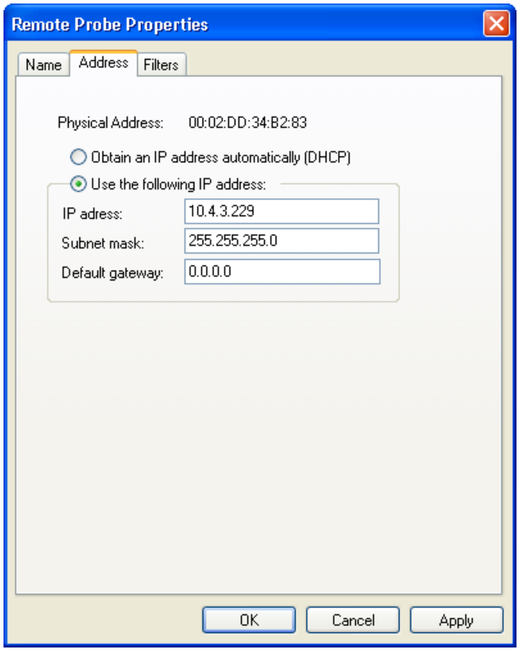
Note: The probe stores its own user-assigned address settings in ROM whether or not the *Enable fault tolerance* item is checked.

The firmware for the RFGrabber Probe is field upgradeable. The *Current version* number is shown in the *Firmware* section of the ***Name*** view of the **Remote Probe Properties** dialog. When new firmware is available, it is distributed in a *.bin file. To upgrade the firmware for a probe, select the probe in any ***Adapter*** view and choose **Properties** from the right click context menu to open the **Remote Probe Properties** dialog. In the *Firmware* section of the ***Name*** view, click the **Upgrade** button. This presents a file **Open** dialog. Navigate to the location of the appropriate *.bin file and select it. Click **OK**. The firmware is upgraded automatically. When the upgrade completes, the new version number should appear as the *Current version*. The firmware upgrade process uses TFTP (Trivial File Transfer Protocol), which uses port 69. We recommend that you only upgrade the firmware when the target RFGrabber Probe is on the same local network as the machine running AiroPeek.

Address properties

The ***Address*** view (Figure 14.7) shows the *Physical Address* of the probe and lets you set IP address parameters for the probe. Use the radio buttons to choose whether to *Obtain an IP address automatically (DHCP)* or to *Use the following IP address*. If you do not use DHCP, you must enter a valid *IP address* in dotted decimal notation, and you may also enter a *Subnet mask* and *Default gateway*, as appropriate.

Each time you start AiroPeek, the ***Adapter*** view of either the **Monitor Options** or the **Capture Options** dialog retrieves information about recently used probes from the Windows registry. If a probe is no longer reachable at the address stored in the registry, the probe will be shown in the ***Adapter*** view as *Not found*. This can happen when DHCP assigns a different address to a probe, or when the probe address has been changed using a copy of AiroPeek running on a different computer. The Windows registry only reflects changes to probe address made from the local computer.



Physical Address: 00:02:DD:34:B2:83

○ Obtain an IP address automatically (DHCP)

● Use the following IP address:

IP adress: 10.4.3.229

Subnet mask: 255.255.255.0

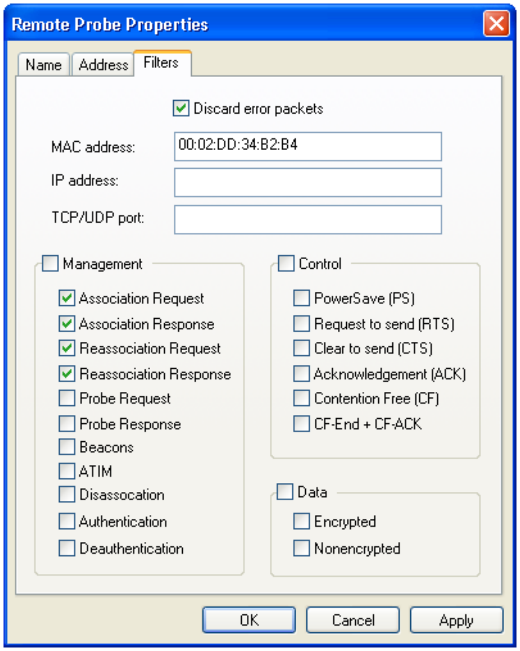
Default gateway: 0.0.0.0

Figure 14.7 Remote Probe Properties dialog, Address view

If a probe’s address has been changed by DHCP or by a copy of AiroPeek running on another machine, you will need to delete the now non-existent probe from the ***Adapter*** view of the local machine and add the probe under its new address in order to access the probe. To delete a probe listed in the ***Adapter*** view, right click on the probe and choose **Delete** from the context menu. For instruction on how to add a probe, please see “Adding a probe on the local network” on page 287, or for probes outside the local network, see “Adding a probe on a remote network” on page 290.

Filter properties

In the ***Filters*** view (Figure 14.8), you can set filters for the RFGrabber Probe itself. The probe sends only those packets which match the filter parameters you set in the ***Filters*** view of the **Remote Probe Properties** dialog. The probe supports only a relatively simple set of filters which are completely distinct from the filters in AiroPeek. The main advantage of applying filters at the RFGrabber Probe is that it can greatly reduce the number of packets that must be streamed back to AiroPeek.



☑ Discard error packets

MAC address: 00:02:DD:34:B2:B4

IP address:

TCP/UDP port:

□ Management
- ☑ Association Request
- ☑ Association Response
- ☑ Reassociation Request
- ☑ Reassociation Response
- □ Probe Request
- □ Probe Response
- □ Beacons
- □ ATIM
- □ Disassocation
- □ Authentication
- □ Deauthentication

□ Control
- □ PowerSave (PS)
- □ Request to send (RTS)
- □ Clear to send (CTS)
- □ Acknowledgement (ACK)
- □ Contention Free (CF)
- □ CF-End + CF-ACK

□ Data
- □ Encrypted
- □ Nonencrypted

Figure 14.8 Remote Probe Properties dialog, Filters view

You can apply probe filters on the probe, and/or AiroPeek filters in AiroPeek, or set filters for both or neither. The filters applied on the probe take effect first. Any filters enabled in AiroPeek are applied to the packets streamed back by the probe, as they arrive.

You can use the same probe as the source for Monitor statistics and for multiple Capture windows simultaneously. Note, however, that any filters set in the ***Filters*** view of the **Remote Probe Properties** dialog for a particular probe will affect all uses of the probe.

The ***Filters*** view of the **Remote Probe Properties** dialog creates a single complex (multi-stage) filter. Only packets which match the filter’s parameters will be accepted by the probe and streamed to AiroPeek. The first stage of the filter is represented by the *Discard error packets* check box at the top of the view. Check the box to discard error packets or uncheck to have error packets streamed to AiroPeek.

The three text entry items (*MAC address*, *IP address*, and *TCP/UDP port*) plus the net result of the tests within any of the three packet type categories (*Management*, *Control*, or

Data) are connected by a logical AND. That is, a packet must meet all of the tests in order to pass the filter and be sent to AiroPeek.

Within each individual packet type category (*Management*, *Control*, or *Data*), the individual filter tests are connected by a logical OR. For example, when several types of management packets have been checked (enabled), a packet matching any one of those criteria will pass the *Management* filter test.

Important! Be careful not to construct a filter that has no possible match. No single packet is both a management and a control packet, or a management and a data packet. No management or control packet also includes IP information, such as IP address or TCP/UDP port number. The dialog will allow you to set such a filter, but the result will be no packets, since no packets can ever match these criteria.

To test for a *MAC address*, enter the physical address in the text entry box, using hexadecimal notation. You may use colon characters to separate values, but the filter will ignore them, reading only the hexadecimal characters (0-9, a-f, A-F). To test for an *IP address*, enter a valid IP address in dotted decimal notation. To test for a *TCP/UDP port*, enter a valid TCP/UDP port number in the text entry box. When any of these text boxes is empty, that parameter is not a part of the filter.

Resetting to default properties

To reset the RFGrabber Probe to its factory defaults:

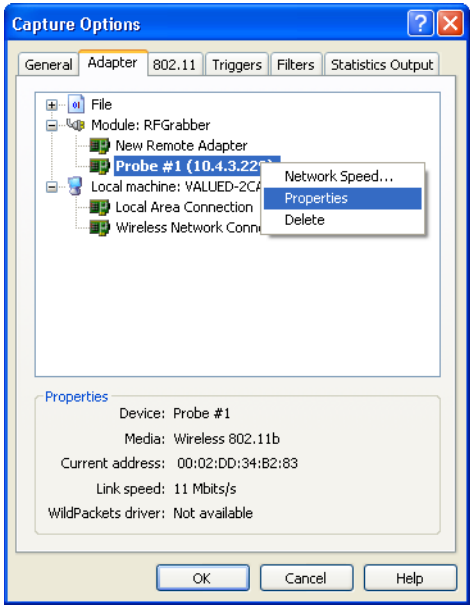
1. Unplug the power cable from the probe.
2. Using a paper clip, hold down the reset button on the back of the RFGrabber Probe. This is a recessed button marked INIT.
3. Continue to hold down the reset button, and plug in the power cable.
4. When the WLAN light starts to blink (in approximately 3 seconds), release the reset button.

   All configuration options will be returned to their factory defaults.

Using RFGrabber

Now that you have installed your RFGrabber Probe, you are ready to use RFGrabber to capture some 802.11 packets remotely.

1. Create a new Capture window in AiroPeek by choosing **Start Capture** from the **Capture** menu or clicking the **New Capture** button on the ***Start Page***. The **Capture Options** dialog will appear.



Device: Probe #1
Media: Wireless 802.11b
Current address: 00:02:DD:34:B2:83
Link speed: 11 Mbits/s
WildPackets driver: Not available

Figure 14.9 Adapter view of Capture Options dialog

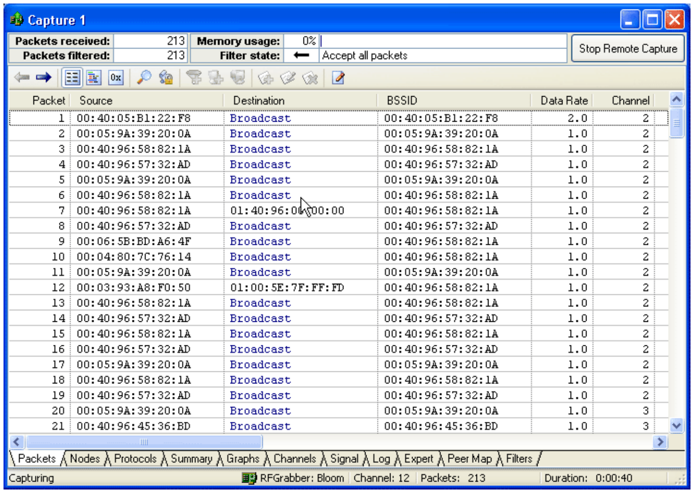
2. Set the options in the ***General*** view, making sure the options for buffer usage and capture timing match your expectation of traffic streamed back from the RFGrabber Probe. For a detailed discussion of how to use this view, see “Capture options: general” on page 56.

3. Click on the *Adapter* tab to open the ***Adapter*** view. Expand the *Module: RFGrabber* item to see a list of all available RFGrabber Probes, each identified by its user-assigned name and its IP address.

4. Select the probe from which you wish to capture, by highlighting its name in the list.

5. To open the new Capture window with the current settings for all views and this adapter as the capture adapter, double-click on the name of the probe or click **OK**. Alternatively, you may set options in the other views of the **Capture Options** dialog before clicking **OK** to open the new Capture window. At a minimum, you will probably want to set or review the channel options in the ***802.11*** view.

6. Click the *802.11* tab to open the ***802.11*** view.
7. When an RFGrabber Probe is selected as the adapter in the ***Adapter*** view, the options available in the ***802.11*** view change. You cannot direct the probe to search for an *ESSID* or *BSSID*, and these options are grayed out. If you choose to scan across several channels, the **Channel Scanning Options** dialog shows a single drop down list constraining the *Duration (msec)* of the scan for each channel to the same value. The minimum duration is *200* milliseconds.
8. Set the options in the ***802.11*** view, noting the limitations above. Also note that any changes you make to the settings in the ***802.11*** view for a given RFGrabber Probe will affect all uses of that probe, whether for Monitor statistics or Capture windows. For more details on using the ***802.11*** view, please see “802.11 view” on page 21.
9. In the ***Triggers*** view of the **Capture Options** dialog you can set triggers in the normal way for a Capture window that is using an RFGrabber Probe as its adapter. Note that triggers are set for the local Capture window and not on the remote probe. This means packets will begin to stream back to AiroPeek as soon as you click the **Start Trigger** button. Please see “Triggers” on page 236 for details.
10. You can set filters on the Capture window as well as a distinct set of filters on the probe itself. For information on filters you can set for the Capture window, see Chapter 11, “Filters” on page 207. For information on filters set on the RFGrabber Probe, see “Filter properties” on page 296.
11. You can automatically output statistics from a Capture window that is using an RFGrabber Probe as its adapter, just as you would from any other Capture window. Please see “Output from statistics” on page 187.
12. You can save to a capture template (*.ctf) file the settings of any Capture window that is using an RFGrabber Probe as its adapter. Capture templates allow you to create a fully configured Capture window in a matter of a few clicks. Note that if the IP address of the RFGrabber Probe is different than the one specified in the capture template, even if the probe’s name is the same, the capture template will consider the adapter not found and present the ***Adapter*** view of the **Capture Options** dialog and wait for user input.
13. The new Capture window appears, ready to begin capture. Click the **Start Remote Capture** button in the new Capture window to start the remote capture. The button changes to **Stop Remote Capture**.
14. As the packets are streamed back, you will see packets being received into the Capture window (Figure 14.10).



Packets received: 213
Packets filtered: 213
Memory usage: 0%
Filter state: Accept all packets

Packet	Source	Destination	BSSID	Data Rate	Channel
1	00:40:05:B1:22:F8	Broadcast	00:40:05:B1:22:F8	2.0	2
2	00:05:9A:39:20:0A	Broadcast	00:05:9A:39:20:0A	1.0	2
3	00:40:96:58:82:1A	Broadcast	00:40:96:58:82:1A	1.0	2
4	00:40:96:57:32:AD	Broadcast	00:40:96:57:32:AD	1.0	2
5	00:05:9A:39:20:0A	Broadcast	00:05:9A:39:20:0A	1.0	2
6	00:40:96:58:82:1A	Broadcast	00:40:96:58:82:1A	1.0	2
7	00:40:96:58:82:1A	01:40:96:00:00:00	00:40:96:58:82:1A	1.0	2
8	00:40:96:57:32:AD	Broadcast	00:40:96:57:32:AD	1.0	2
9	00:06:5B:BD:A6:4F	Broadcast	00:40:96:58:82:1A	1.0	2
10	00:04:80:7C:76:14	Broadcast	00:40:96:58:82:1A	1.0	2
11	00:05:9A:39:20:0A	Broadcast	00:05:9A:39:20:0A	1.0	2
12	00:03:93:A8:F0:50	01:00:5E:7F:FF:FD	00:40:96:58:82:1A	1.0	2
13	00:40:96:58:82:1A	Broadcast	00:40:96:58:82:1A	1.0	2
14	00:40:96:57:32:AD	Broadcast	00:40:96:57:32:AD	1.0	2
15	00:40:96:58:82:1A	Broadcast	00:40:96:58:82:1A	1.0	2
16	00:40:96:57:32:AD	Broadcast	00:40:96:57:32:AD	1.0	2
17	00:05:9A:39:20:0A	Broadcast	00:05:9A:39:20:0A	1.0	2
18	00:40:96:58:82:1A	Broadcast	00:40:96:58:82:1A	1.0	2
19	00:40:96:57:32:AD	Broadcast	00:40:96:57:32:AD	1.0	2
20	00:05:9A:39:20:0A	Broadcast	00:05:9A:39:20:0A	1.0	3
21	00:40:96:45:36:BD	Broadcast	00:40:96:45:36:BD	1.0	3

Capturing | RFGrabber: Bloom | Channel: 12 | Packets: 213 | Duration: 0:00:40

Figure 14.10 Remotely captured packets are streamed into the Capture window

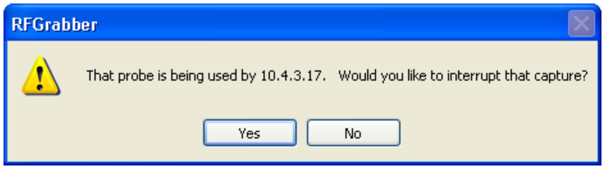
Support for multiple probes

AiroPeek treats the RFGrabber Probe like any other adapter. You can collect Monitor statistics and have multiple Capture windows using the same RFGrabber Probe simultaneously, or use multiple probes for multiple simultaneous Capture windows. The main limitation is the bandwidth available on the wired network connection to the probes. A single probe streaming at full speed may reach 7 MB/second. Such a rate corresponds to heavy traffic on the monitored 802.11b WLAN, but it does give some indication of the impact of multiple simultaneous streams from multiple probes. If the RFGrabber Probes are connected over a separate management network, then there will be no impact on ordinary network traffic.

The number of RFGrabber Probes your wireless environment needs will depend on your goals for remote wireless network analysis. For a full discussion, please refer to the WildPackets white paper, “Remote Analysis of a Wireless LAN Environment,” available at http://www.wildpackets.com/support/white_papers.

Multiple users

You can connect to the probe from a wide range of locations, and many users can connect to the same probe in sequence, but not simultaneously. Only one copy of AiroPeek can be connected to an individual RFGrabber Probe at any one time. If you attempt to connect to a probe and the probe believes it is already in use by another copy of AiroPeek at a different IP address, AiroPeek will display a warning dialog asking if you wish to displace the current user of the probe. Click the **Yes** button to take over the probe and replace the current session with your own. Click **No** to abandon your attempt to connect to the probe, allowing the current user to continue with their capture.



That probe is being used by 10.4.3.17. Would you like to interrupt that capture?

Figure 14.11 RFGrabber connection warning dialog

Troubleshooting

This section provides pointers for troubleshooting your RFGrabber Probe.

No packets are received when I click the start capture button.

There are several things to check:

1. Does the channel specified in AiroPeek actually have activity on it?
2. Did you set filters on the RFGrabber Probe which result in no packets being captured? (for example, setting an IP address AND one or more 802.11 Management or Control packets -- a logical impossibility, since these packet types can never contain IP protocol data).
3. Are any filters enabled in AiroPeek which may be rejecting the packets captured at the probe?

AiroPeek finds my RFGrabber Probe, but after I add the probe it does not work.

You may not have a DHCP server on your network, so although the RFGrabber Probe can be discovered, AiroPeek cannot communicate with it because the probe does not have a valid IP address. In the ***Adapter*** view, select the probe and choose **Properties** from the right click context menu. In the ***Address*** view of the **RFGrabber Probes** dialog, give the probe a static IP address. Please see “Using static IP addresses” on page 292.

Does the RFGrabber Probe transmit any WLAN packets?

No. The RFGrabber Probe does not transmit any 802.11b packets over the airwaves, so it cannot interfere with WLAN traffic and is not detectable by other wireless packet analyzers.

I seem to be getting the same packets over and over in some sort of feedback loop.

If the computer on which you are running AiroPeek is connected to your wired network, and hence to the RFGrabber Probe, through a wireless connection, you can create a loop by moving into the same BSS as the probe. If the filters on the probe are set so as to include the data packets in which the traffic is streamed back, and your computer is receiving that stream from an AP at a location and channel being monitored by the RFGrabber Probe, then the packets sent to you by the AP will become part of the traffic captured and streamed back by the probe, creating a loop.

There are three solutions:

1. Connect to the probe over the wired network (using an Ethernet adapter).
2. If you connect to the network wirelessly, associate with an AP that is out of range of the probe, or operating on a different channel.
3. If you must connect to the network using an AP that is within range of the RFGrabber Probe, set the probe so that it does not capture the streamed data being sent by that AP. Either set filters on the probe so it will not capture data packets, or set the probe to listen only on the channels not used by the nearby AP.

Table 14.2 RFGrabber Probe Specifications

Parameter		Specification
Operating Range		
	Indoors	Up to 50 m (164 ft.) @ 11 Mbps
		Up to 80 m (263 ft.) @ 5.5 Mbps or lower
	Outdoors	Up to 150 m (492 ft.) @ 11 Mbps
		Up to 300 m (984 ft.) @ 5.5 Mbps or lower

Table 14.2 **RFGrabber Probe Specifications (continued)**

Parameter		Specification
Hardware		
	Height	135mm ($5^{5}/_{16}$")
	Depth	103mm ($4^{1}/_{16}$")
	Width	29mm ($1^{1}/_{8}$") at top, 60mm ($2^{3}/_{8}$") at base
	Unit Weight	0.2 kg (7.1 oz.)
	Power	Requires a 5V, 1A, DC power supply (US power supply included)
	4 LEDs	“PWR”, “LAN”, “WLAN”, and “DIAG”
	Certifications	FCC Class B, CE Mark
	Operating Temp.	0^{o} C to 50^{o} C (32^{o} F to 122^{o} F)
	Storage Temp.	-25^{o} C to 70^{o} C (-13^{o} F to 158^{o} F)
	Operating Humidity	10% to 90% Non-Condensing
	Storage Humidity	10% to 90% Non-Condensing

Post-capture Analysis

Much of the work of troubleshooting problems on a network is a process of narrowing down the possibilities, examining first one set of clues and then another. AiroPeek provides a number of tools for analyzing packets, for selecting, grouping, and sorting them by a variety of attributes. This chapter starts with the most basic selection methods and concludes with the more sophisticated tools for evaluating groups of packets.

The statistical, ***Expert***, and ***Peer Map*** views of Capture windows and Packet File windows are recalculated and redrawn each time there is a change in the visible packets in the ***Packets*** view. By selecting, hiding and unhiding packets, a user can perform sophisticated analysis on captured traffic quickly and easily.

This chapter explains how to select, group, manipulate and process captured packets in Packet File windows and in Capture windows.

In this Chapter:

Saving captured packets

The techniques described in this chapter are applied to packets that have already been captured and are in the buffer of either a Packet File window or of a Capture window. While it is possible to use some of these techniques to select and sort packets while capture is still under way (the basic selection techniques, for example), it is assumed that capture has been stopped.

The simplest way to save packets from a Capture window is to choose **Save All Packets…** from the **File** menu to bring up the **Save** dialog and save them to a file of the default AiroPeek format. The **Save All Packets…** command saves all packets currently visible in the active window, whether selected or not. Any hidden packets will *not* be saved.

If any packets are currently selected in the active window, the **File** menu will offer the choice of **Save Selected Packets…**. This will open the same **Save** dialog where you can create a file containing only the packets highlighted in the ***Packets*** view of the active window.

To delete all packets, including any hidden packets, from a window, choose **Clear All Packets** from the **Edit** menu or press **Ctrl + B**.

Using basic select and hide functions

When items are *selected*, that state is shown by the fact that they are highlighted. You can select items in any of the following views of a Capture window or a Packet File window:

- ***Packets***
- ***Nodes***
- ***Protocols***
- ***Conversations*** (this view exists in AiroPeek standard only)
- ***Expert*** (this view exists in AiroPeek NX only)
- ***Peer Map*** (this view exists in AiroPeek NX only)

While you can select the line entries in any of these views, the only place that *packets* are actually selected is in the Packet List pane of the ***Packets*** view. (Please see “Select related packets” on page 308, below.)

Basic selection

You can use all the standard selection techniques to choose items in any of the windows that allow selection. To highlight a single item, click on it. Clicking on another item highlights it instead. To highlight multiple items, hold down the **Ctrl** key when you click. To unhighlight any one item, hold down the **Ctrl** key and click on it again. To highlight a contiguous group of items, click on the first item, then hold down the **Shift** key when you click on the last item in the sequence. Everything between the two clicks (inclusive) will be highlighted.

The **Edit** menu adds a few more simple techniques. To highlight everything in the view, choose **Select All** from the **Edit** menu or press **Ctrl + A**. To remove all highlighting, choose **Select None** from the **Edit** menu or press **Ctrl + D**.

Choose **Invert Selection** from the **Edit** menu to reverse the highlighting.

Hide and unhide

Hiding packets removes them from view without actually deleting them. It is a handy way to quickly reduce the clutter of the ***Packets*** view. Hide functions are disabled for Capture windows when capture is under way.

Hidden packets are not processed by Analysis Modules or statistics, are not printed when the contents of the window are printed, and are not saved when you choose **Save All Packets…** from the **File** menu. They are, however, deleted when you select **Clear All Packets** from the **Edit** menu or press **Ctrl + B**.

To hide the selected packets, choose **Hide Selected Packets** from the **Edit** menu or press **Ctrl + H**. Alternatively, you can choose **Hide Unselected Packets** or type **Ctrl + Shift + H**. To restore all hidden packets to view, choose **Unhide All Packets** from the **Edit** menu or type **Ctrl + U**. You can continue to add to the hidden packets, hiding some now and more later, but there is no way to selectively unhide.

Note: Hiding or Unhiding causes all packets in the Capture window or Packet File window to be reprocessed by any enabled Analysis Modules and causes statistics to be recalculated based on the changed visible contents of the window’s buffer.

Hidden packets are a part of the total packets, but are not processed by any Analysis Modules, statistics, or further selections.

Navigating within selections

The **Go To…** and **Go To Next Selected** functions open the next packet in the selection in the **Packet Decode** window. They also move to that packet's listing in the ***Packets*** view of the active Capture window or Packet File window. Choose **Go To…** from the **Edit** menu or press **Ctrl + G** to bring up the **Go To** dialog. Fill in the number of the packet to which you want to jump. Choose **Go To Next Selected** from the **Edit** menu or press **Ctrl + J** to jump to the next packet in the selection.

Select related packets and find pattern

These more sophisticated selection tools essentially create pattern matching tools and apply them to the packets in the window.

Select related packets

The **Select Related Packets** command allows you to find packets that are like, or related to, the packet or data item currently selected. **Select Related Packets** presents a submenu of choices (shown in Table 15.1) allowing you to define which aspect(s) of the currently selected item you want this new selection to match. **Select Related Packets** creates a detailed set of selection criteria based on the parameter you choose and on the values found in the currently selected item. It then tests all the visible packets in the ***Packets*** view of the Capture window or Packet File window against those criteria and selects the ones that match.

To select related packets:

1. Highlight an item in the ***Packets***, ***Nodes***, or ***Protocols*** view of a Capture window or Packet File window. In AiroPeek standard only, you can also highlight items in the ***Conversations*** view. In AiroPeek NX only, you can also highlight items in the ***Expert***, or ***Peer Map*** views.
2. Choose **Select Related Packets** from the **Edit** menu, or right click and choose **Select Related Packets** from the context menu.
3. From the submenu (shown in Table 15.1), choose the particular parameter set by which you want to define the relationship. Note that the submenu is context-sensitive and will only show the parameters that make sense for the item you initially highlighted.
4. If the current Capture window or Packet File window contains any related packets, the **Selection Results** dialog will open, showing the number of *packets selected*.

5. Use the **Selection Results** dialog to **Hide Selected** or **Hide Unselected**, or to do neither by clicking on **Close**.

Table 15.1 **Submenu choices for Select Related Packets command**

Parameter	Action
By Source	Chooses packets with matching source address.
By Destination	Chooses packets with matching destination address.
By Source and Destination	Chooses packets with matching source and destination addresses.
as Source or Destination	Unique to the ***Peer Map*** view (available in AiroPeek NX only), chooses packets showing the current node as either the source or destination address.
By Protocol	Chooses packets with matching protocol.
By Port	Chooses packets with matching port.
By Conversation	Chooses packets sent between two nodes (in either direction), using the matching protocol and port.
By Problem Type	Unique to the Problem Summary pane of the ***Expert*** view (available in AiroPeek NX only), this chooses all packets flagged with the particular problem highlighted in the Problem Summary.

Table 15.1 Submenu choices for Select Related Packets command

Parameter	Action
Selected Entries	Unique to the Problem Log pane of the ***Expert*** view (available in AiroPeek NX only), this item chooses only the individual packet identified with each highlighted entry in the Problem Log. The Problem Log shows one packet with one problem in each log entry. Multiple log entries may be highlighted at once.
Selected Entries + “See” or “From Pkt”	Unique to the Problem Log pane of the ***Expert*** view (available in AiroPeek NX only), this item chooses the individual packet identified with each highlighted entry in the Problem Log, plus any packet referred to in the log entry in a phrase which begins “*See Packet…*” or “*From Packet…*.” These log entries refer to another packet in the same conversation, such as a response or request packet, for example.

The **Select Related Packets** sub-menu of commands is available from the **Edit** menu, or from the context menu (right-click) where applicable. Not every submenu choice is available in every view. When you highlight a particular item in a statistical view, the **Select Related Packets** sub-menu items will change to match the context. AiroPeek standard and AiroPeek NX offer different views. Table 15.2 shows which sub-menu commands may be available in each of the four views found in AiroPeek standard: ***Packets***, ***Nodes***, ***Protocols***, and ***Conversations***. Table 15.3 shows which sub-menu commands may be available in each of the five views found in AiroPeek NX: ***Packets***, ***Nodes***, ***Protocols***, ***Expert***, and ***Peer Map***. As a more general guide, remember that the highlighted item must contain some value for the parameter by which you wish to select. This explains why you cannot select **By Source** address when you have highlighted an item in the ***Protocols*** view, nor select **By Protocol** when you have highlighted an item in the ***Nodes*** view.

Table 15.2 **Select related packets, parameter availability by view**

AiroPeek standard	*Packets*	*Nodes*	*Protocols*	*Conversations*
By Source	yes	yes		
By Destination	yes	yes		
By Source and Destination	yes	yes		yes
By Protocol	yes		yes	
By Port	yes			
By Conversation	yes			yes

Table 15.3 **Select related packets, parameter availability by view**

AiroPeek NX	*Packets*	*Nodes*	*Protocols*	*Expert*	*Peer Map*
By Source	yes	yes			modified*
By Destination	yes	yes			modified*
By Source and Destination	yes	yes		yes	modified*
By Protocol	yes		yes		
By Port	yes				
By Conversation	yes			yes	
By Problem Type				yes	

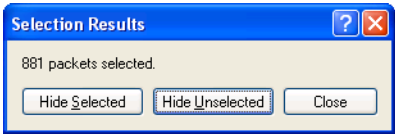
Table 15.3 **Select related packets, parameter availability by view**

AiroPeek NX	*Packets*	*Nodes*	*Protocols*	*Expert*	*Peer Map*
Selected Entries				**yes**	
Selected Entries + “See” or “From Pkt”				**yes**	

***** The ***Peer Map*** view offers a modified version of the Select Related Packets function. You can use the highlighted node **as Source**, **as Destination**, or **as Source or Destination** for a Select Related Packets function. Note that there is no selection **By Source and Destination**, only selection using the current node **as Source or Destination**.

The **Select Related Packets** command creates the most specific match it knows how to make, based on the parameters you chose and the item you selected. For example, if you highlight a single ARP request packet in ***Packets*** view and choose **Select Related Packets** > **By Protocol**, you will find the selection includes no ARP response packets, only requests. If you go to the ***Protocols*** view and select the ARP protocol itself, which includes both requests and responses, and invoke **Select Related Packets** > **By Protocol** from there, you will find all the ARP traffic highlighted in the ***Packets*** view.

When you use the **Select Related Packets** command, a dialog appears telling how many packets AiroPeek selected and offering to **Hide Selected** or **Hide Unselected**, or to do neither by clicking on **Close**.


Selection Results

881 packets selected.

Figure 15.1 Selection Result dialog offers to hide, or just select with Close

Find pattern and find next

The **Find Pattern** and **Find Next** commands are a matched pair of tools. **Find Pattern** finds matches of a user-defined string at a user-defined location. To open the **Find Pattern** dialog, choose **Find Pattern** from the **Edit** menu or press **Ctrl + F**. You must limit the area and type of search, by choosing from the *Find in* drop-down list. Your choices are:

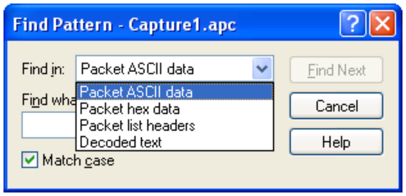
Packet ASCII data Searches for a match with an ASCII string found anywhere in the raw data of the packet.

Packet Hex Data Searches for a match with a hex string found anywhere in the raw data of the packet.

Packet List Headers Searches for a match with a string found in the packet list headers; that is, with the text shown in the current set of columns in the Packet List pane of the ***Packets*** view for that packet.

Decoded Text Searches for a match with a string found in the text of the decoded packet. This is like doing a text search in the ***Decode*** view portion of the text file which would be created by choosing Save Selected Packets as Text for the currently selected packets.

Enter a string and choose whether the search should be case sensitive. The first packet matching these criteria will be highlighted in the ***Packets*** view. To find the next matching packet in sequence, choose **Find Next** from the **Edit** menu or press **F3**.


Find Pattern - Capture1.apc

Find in: Packet ASCII data

☑ Match case

Figure 15.2 The Find Pattern dialog, showing the find in drop-down list

Select dialog: filters, analysis modules and more

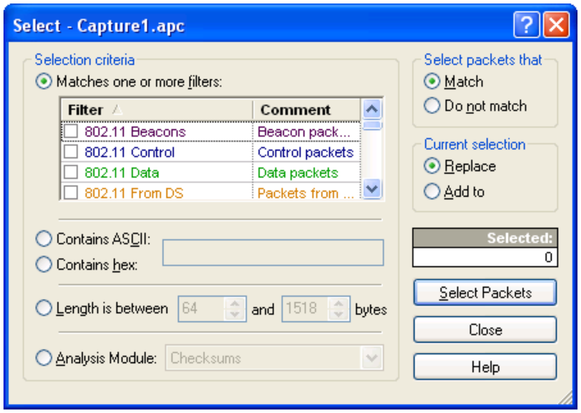
The **Select…** command from the **Edit** menu brings up the **Select** dialog that allows you to use existing filters to select captured packets, to select based on string content or packet length, or to select based on Analysis Modules. You can select either all packets matching your criteria or all those not matching. The **Select** dialog only applies to visible packets in the active Capture window or Packet File window.

The **Select** dialog is also the only selection tool (other than the standard **Ctrl + click**) that allows you to add to an existing selection. Alternatively, you can choose to replace the current selection with the results of the new selection, as is the case with all other selection tools from the **Edit** menu.

Important! Packet slicing can affect the operation of some selection tools. When used from the **Select** dialog, filters, Analysis Modules and other selection tools read packet contents from the *captured* packets to determine protocols, addresses and related information. If the packet slice value was set in such a way as to discard some of the information these tools expect to find, they will not be able to identify packet attributes correctly.

To use the **Select** dialog to select packets in the Packet List of the active window:

1. Choose **Select…** from the **Edit** menu to open the **Select** dialog (Figure 15.3).



Select - Capture1.apc

Selection criteria

● Matches one or more filters:

Filter	Comment
□ 802.11 Beacons	Beacon pack...
□ 802.11 Control	Control packets
□ 802.11 Data	Data packets
□ 802.11 From DS	Packets from ...

○ Contains ASCII:
○ Contains hex:

○ Length is between 64 and 1518 bytes

○ Analysis Module: Checksums

Select packets that
● Match
○ Do not match

Current selection
● Replace
○ Add to

Selected: 0

Figure 15.3 Select dialog

2. In the *Selection criteria* section, use the radio buttons to choose the method you will use to select the packets. Fill in the parameters for the chosen selection criteria. Each of the methods is described in its own section below. Your choices are:
   - Select based on filters
   - Select based on ASCII or hex character string
   - Select based on packet length
   - Select based on analysis modules
3. Use the radio buttons marked *Match* or *Do not match* to choose whether to *Select packets that Match* the criteria you chose or packets that *Do not match* the selection criteria.
4. Use the radio buttons in the *Current selection* section to decide whether the results of this operation will *Replace* or *Add to* the *Current selection*.

5. Click the **Select Packets** button to perform the selection.

   A pane immediately above the **Select Packets** button shows the number of packets *Selected*. If any packets were selected, a **Selection Results** dialog will appear, noting how many packets were selected and offering the option to **Hide Selected**, **Hide Unselected**, or click **Close** to simply close the dialog without further action.

6. You can leave the **Select** dialog open and perform another selection, either adding to or replacing the current selection, or you can close the dialog by clicking the **Close** button.

Select based on filters

To select using one or more existing filters, click the *Matches one or more filters* radio button and check one or more filters from the list to enable them for selection.

Note: When multiple filters are enabled simultaneously, they are considered to be OR'ed together. That is, a packet matching any one of the enabled filters will be considered a match.

Select based on ASCII or hex character string

You can select packets which match a specified string found anywhere within the packet. To create a string selection, choose the appropriate radio button and enter the string for which you want to test. Choose either *Contains ASCII* for a text string, or *Contains hex* for a hexadecimal value.

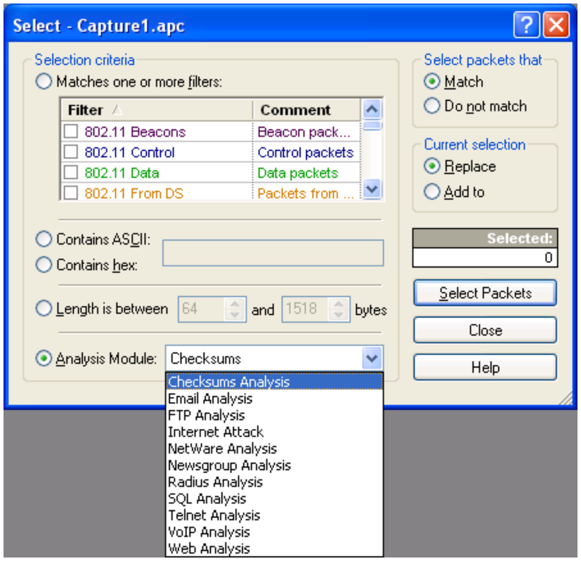
Select based on packet length

Select by Length checks for packet size, measured in bytes. To use this selection method, click the radio button beside *Length is between*. The default values in the dialog are set to *64* bytes and *1518* bytes, the legal minimum and maximum Ethernet packet sizes, respectively. You may set values outside this range if you wish. Setting both values to the same number of bytes selects packets of that length only.

Select based on analysis modules

Analysis Modules can perform many different functions. Not all Analysis Modules support the select feature. Those that do are accessible in the **Select** dialog (Figure 15.4). Choose **Select…** from the **Edit** menu to bring up the **Select** dialog for the active window.

In the *Selection criteria* section, click the *Analysis Module* radio button and choose an Analysis Module from the drop-down list. An Analysis Module will match a packet if it finds any of the data for which it tests in that packet.



Select - Capture1.apc

Selection criteria

○ Matches one or more filters:

Filter	Comment
□ 802.11 Beacons	Beacon pack...
□ 802.11 Control	Control packets
□ 802.11 Data	Data packets
□ 802.11 From DS	Packets from ...

○ Contains ASCII:

○ Contains hex:

○ Length is between 64 and 1518 bytes

● Analysis Module: Checksums

Select packets that

● Match

○ Do not match

Current selection

● Replace

○ Add to

Selected: 0

Figure 15.4 Analysis Module choices in the Select dialog

16

Decoding Packets

When troubleshooting your network, tracking down a security breach, or simply gaining a better knowledge of protocols and network services; looking into the packets themselves is often very useful. When troubleshooting network applications, it is sometimes the only way to identify the real root of a problem.

This chapter describes how to decode packets and read the packet headers, how to customize the way AiroPeek displays packet decodes, navigate through multiple selected packets and reconstruct the threads of network conversations.

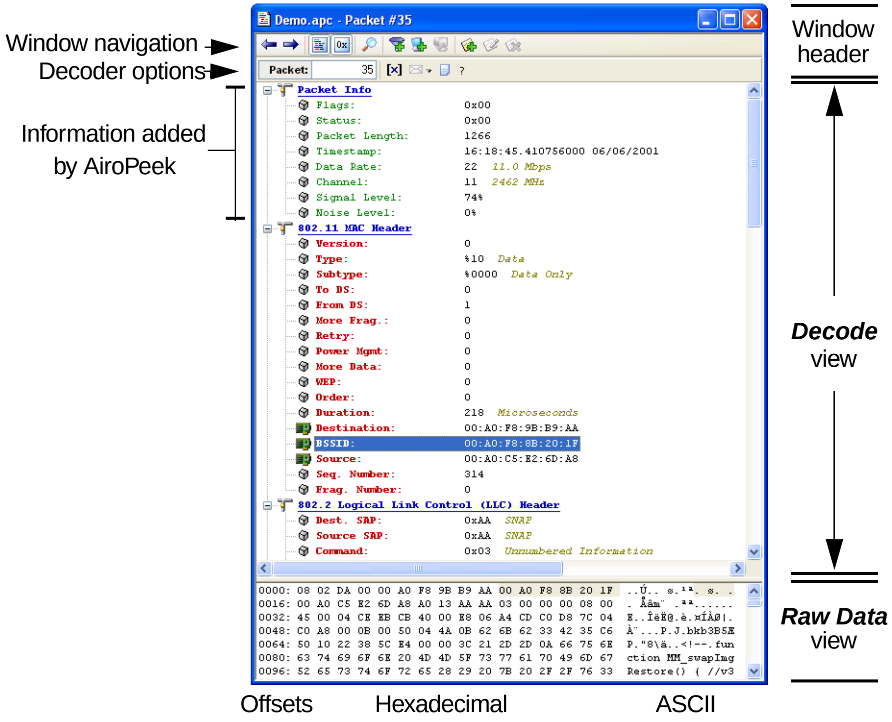
When WEP is enabled, only the headers of the 802.11 WLAN data packets are sent unencrypted. The body of all data packets, including all higher level protocols such as TCP/IP, Appletalk, and so forth, are encrypted to guard against eavesdropping. In order to use AiroPeek to analyze traffic in these higher level protocols where WEP is enabled, AiroPeek must be provided with the WEP key set. Please see “WEP encryption and AiroPeek” on page 24 for detailed instructions on utilizing WEP encryption with AiroPeek. The rest of this chapter assumes that either WEP is not enabled or that AiroPeek has been provided with a key set for the monitored network.

CAUTION! Many protocols, especially the older Internet protocols such as HTTP, POP3, FTP, Telnet, and others transmit packet data in plain ASCII text. Controlling access to AiroPeek should be a normal part of your security routine.

In this Chapter:

The packet decode window

Double-click on any packet in a Packet List to open it in the **Packet Decode** window and see the data it contains as decoded information. The **Packet Decode** window makes packet headers readable and understandable. There are three basic parts to the display of a **Packet Decode** window: the window header, the ***Decode*** view and the ***Raw Data*** view. These are shown in Figure 16.1. Each of the parts of the **Packet Decode** window is described below.



```
Packet Info
    Flags:                    0x00
    Status:                   0x00
    Packet Length:            1266
    Timestamp:                16:18:45.410756000 06/06/2001
    Data Rate:                22   11.0 Mbps
    Channel:                  11   2462 MHz
    Signal Level:             74%
    Noise Level:              0%
802.11 MAC Header
    Version:                  0
    Type:                     %10   Data
    Subtype:                  %0000   Data Only
    To DS:                    0
    From DS:                  1
    More Frag.:               0
    Retry:                    0
    Power Mgmt:               0
    More Data:                0
    WEP:                      0
    Order:                    0
    Duration:                 218   Microseconds
    Destination:              00:A0:F8:9B:B9:AA
    BSSID:                    00:A0:F8:8B:20:1F
    Source:                   00:A0:C5:E2:6D:A8
    Seq. Number:              314
    Frag. Number:             0
802.2 Logical Link Control (LLC) Header
    Dest. SAP:                0xAA   SNAP
    Source SAP:               0xAA   SNAP
    Command:                  0x03   Unnumbered Information
```

```
0000: 08 02 DA 00 00 A0 F8 9B B9 AA 00 A0 F8 8B 20 1F  ..Ú.. ø.¹ª. ø. .
0016: 00 A0 C5 E2 6D A8 A0 13 AA AA 03 00 00 00 08 00  . Åâm¨ .ªª......
0032: 45 00 04 CE EB CB 40 00 E8 06 A4 CD C0 D8 7C 04  E..ÎëË@.è.¤ÍÀØ|.
0048: C0 A8 00 0B 00 50 04 4A 0B 62 6B 62 33 42 35 C6  À¨...P.J.bkb3B5Æ
0064: 50 10 22 38 5C E4 00 00 3C 21 2D 2D 0A 66 75 6E  P."8\ä..<!--.fun
0080: 63 74 69 6F 6E 20 4D 4D 5F 73 77 61 70 49 6D 67  ction MM_swapImg
0096: 52 65 73 74 6F 72 65 28 29 20 7B 20 2F 2F 76 33  Restore() { //v3
```

Figure 16.1 Parts of a Packet Decode window

Packet decode window navigation

The **Packet Decode** window header contains the window title bar and the **Packet Decode** window view and navigation buttons. The window title bar shows the name of the file (Capture window or Packet File window) from which the displayed packet was taken, and the number of the packet in that Packet List.

The buttons immediately below the title bar allow you to move backward and forward through the active Packet List (**Decode Previous** and **Decode Next**), and to control which views of the **Packet Decode** window will be displayed. You can choose to **Show Decode View**, **Show Hex View**, or enable both. Click the **Zoom Pane** button to make the active view (the one with the current active highlight) the only visible view. Click the **Zoom Pane** button again to toggle back to the previous appearance. These window navigation buttons are shown in a detail of a **Packet Decode** window in Figure 16.3.

You can step through the packets in the active Packet List in a number of ways. You can use the **Decode Previous** and **Decode Next** buttons as described above, or you can do the same thing using the function key **F7** or the keyboard short-cuts **Alt + left arrow** to decode the previous packet, or the function key **F8** or the **Alt + right arrow** to decode the next packet. Note that in either case, only the packets visible in the Packet List are considered. Packets hidden using any of the **Hide** functions on the **Edit** menu cannot be decoded in the **Packet Decode** window.

You can open individual **Packet Decode** windows for up to 10 packets at once. When multiple packets are selected in the active Packet List, click **Enter** to open them all. If more than 10 packets are selected, AiroPeek will display a message noting how many packets were selected and reminding you that only the first ten can be opened.

To open and view the contents of selected packets one at a time, select the packets and choose the **Go To…** command from the **Edit** menu, or press **Ctrl + G**. The **Go To** dialog opens, showing the packet number of the first packet in the current selection. Press **ENTER** (or click **OK**) to open the first selected packet. You can then use **Go To Next Selected** in the **Edit** menu or press **Ctrl + J** to close the **Packet Decode** window for the current packet and open a new one for the next packet in sequence in the current selection.

Tip The **Go To…** command finds the first packet of a selection for you. There is no need to scroll and look for it, as its number is displayed in the **Go To** dialog when it opens.

For a more complete view of selection options and techniques for navigating through selected packets, see “Navigating within selections” on page 308.

Decode view

The larger upper view of the **Packet Decode** window (shown in Figure 16.1) contains the ***Decode*** view, including the buttons controlling the application of decoder options. This section describes the ***Decode*** view. The decoder options are described in “Packet decoder options” below.

At the top of the data portion of the ***Decode*** view, the topmost fields are created internally by AiroPeek as it controls the 802.11 WLAN card. Most of these items relate to packet capture or to the state of the 802.11 WLAN card, and are described in Table 16.1, below.

Table 16.1 **Packet Decode information added by AiroPeek**

Parameter	Description
Flags	Denotes errors and frame type.
Status	Indicates any one of several conditions, including that the packet was initially WEP encrypted, that there were errors during decryption (WEP ICV errors), or that the packet was truncated or sliced. Shows a value of *0x00* when the packet does not have any of these other conditions.
Packet Length	The number of bytes that the 802.11 WLAN card retrieved off the network for this packet, including all header information and FCS.
Slice Length	When *Slice Length* appears, it indicates the number of bytes of the packet which were captured. This is shown only if packet slicing was used on a packet, or if data was truncated because it was unavailable.
Timestamp	The time the packet was received.
Data Rate	The data rate at which the body of the packet was transmitted.
Channel	The channel number and radio frequency at which the packet was transmitted.
Signal Level	The signal strength of the transmission in which the packet was received, expressed as the RSSI normalized to a percentage.

Table 16.1 Packet Decode information added by AiroPeek (continued)

Signal dBm	The signal strength of the transmission in which the packet was received, expressed in dBm (decibell-milliWatts). If the packet was captured on an adapter that does not report values for signal level in dBm, this item will not be shown.
Noise Level	The noise level reported in the receipt of this packet, expressed as a percentage. If the packet was captured on an adapter that does not report values for noise, this will show as *0%*.
Noise dBm	The noise level reported in the receipt of this packet, expressed in dBm (decibell milliwatts). If the packet was captured on an adapter that does not report values for noise in dBm, this item will not be shown.

The decoded packet data is presented in byte order from top to bottom. Click on the - minus or + plus signs in the margin to collapse or expand the view of any header section.

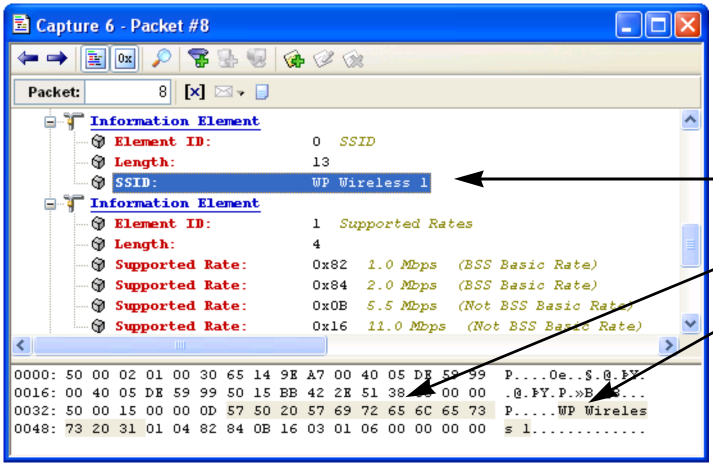
AiroPeek decodes many hundreds of network, transport, application and device control protocols, displaying both the commands and their meaning in English. When the data portion of the packet is listed toward the end of the ***Decode*** view simply as *data*, however, AiroPeek has reached a layer of the packet that it cannot decode with the current or default decoder. For details about selecting an alternative decoder, see “Choose decoder” on page 327. If you are writing your own protocols and wish to write your own decoders, please see “Writing your own decoders” on page 330.

Raw data view: hex and ASCII packet contents

The bottom view pane of the **Packet Decode** window is the ***Raw Data*** view and contains the actual packet contents in raw hexadecimal on the left and its ASCII (or EBCDIC) equivalent on the right.

AiroPeek graphically links the ***Decode*** view with the ***Raw Data*** view for both hex and its ASCII equivalent. When you highlight a section of the ***Decode*** view, the corresponding portion of the hex data and the ASCII data in the ***Raw Data*** view is also highlighted, as shown in Figure 16.2. The reverse is also true. When you highlight an element in the ***Raw Data*** view, the corresponding element is highlighted in the ***Decode*** view.

When you right click in the ***Raw Data*** view, it opens a context-sensitive menu with two sets of alternative display choices. The first permits you to toggle between displaying the text portion of the ***Raw Data*** view as **ASCII** or as **EBCDIC**. The second set of choices changes the notations at the left of the hex portion of the ***Raw Data*** view between **Decimal Offsets** and **Hexadecimal Offsets**.



```
Information Element
    Element ID:            0   SSID
    Length:                13
    SSID:                  WP Wireless 1
Information Element
    Element ID:            1   Supported Rates
    Length:                4
    Supported Rate:        0x82   1.0 Mbps   (BSS Basic Rate)
    Supported Rate:        0x84   2.0 Mbps   (BSS Basic Rate)
    Supported Rate:        0x0B   5.5 Mbps   (Not BSS Basic Rate)
    Supported Rate:        0x16   11.0 Mbps   (Not BSS Basic Rate)
```

```
0000: 50 00 02 01 00 30 65 14 9E A7 00 40 05 DE 59 99  P....0e..§.@.ÞY.
0016: 00 40 05 DE 59 99 50 15 BB 42 2E 51 38 [illegible] 00 00  .@.ÞY.P.»B[illegible]8...
0032: 50 00 15 00 00 0D 57 50 20 57 69 72 65 6C 65 73  P.....WP Wireles
0048: 73 20 31 01 04 82 84 0B 16 03 01 06 00 00 00 00  s 1.............
```

Figure 16.2 Highlights match: Decode, Hex, and ASCII data in a Packet Decode window

Packet decoder options

At the top of the ***Decode*** view of the **Packet Decode** window is a small header section showing the packet number and, to the right of that, buttons controlling the decoder options for the current packet. These buttons and their labels are shown in Figure 16.3. Each of these decoder options is discussed below.

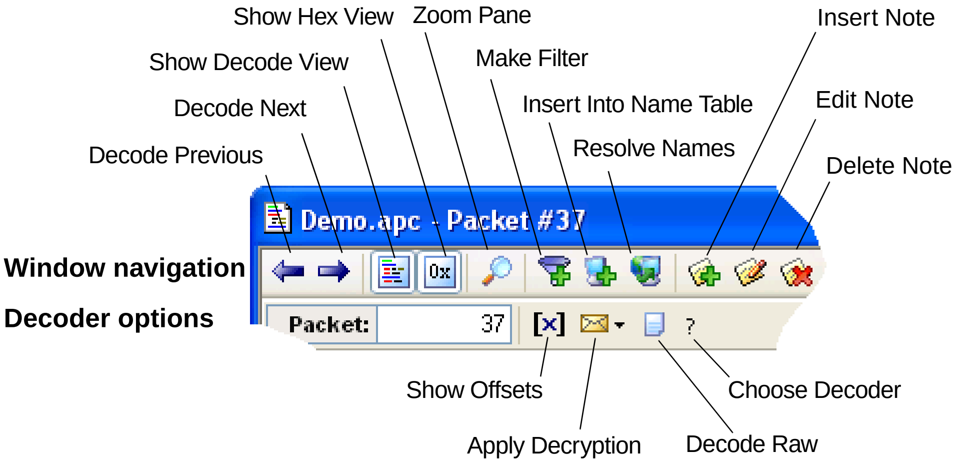


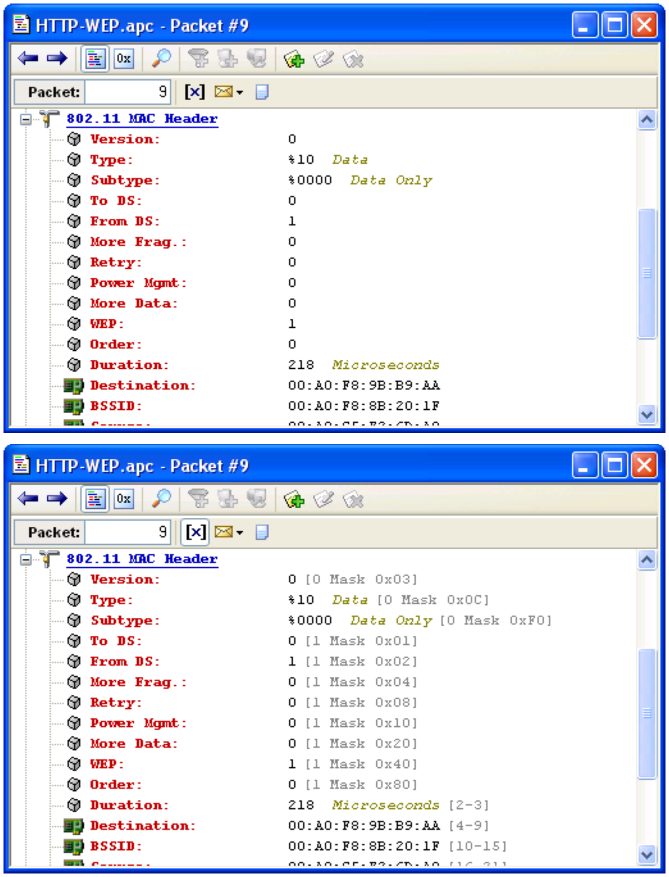
Figure 16.3 Detail of Packet Decode window: navigation and decoder options buttons

Show data offsets

The **Show Offsets** button toggles the display of data offset and mask information for all individual items in the ***Decode*** view. Offset is a measure of location within a packet, counted as the distance in bytes from the first byte of the packet. The offset of the first byte is “0,” that of the second byte is “1,” and so on. The mask is a mathematical way of defining a particular bit or bits within a byte. The offset and mask information is especially useful when developing protocols, constructing filters, and in a variety of other detailed packet analysis tasks.

Tip You can quickly create a filter that matches the value found at a particular point in a packet, directly from the ***Decode*** view or Decode pane. Highlight the item you wish to match and click the **Make Filter** button, or right-click and choose **Make Filter…** from the context menu. This opens the ***Advanced*** view of the **Edit Filter** dialog with a *Value* filter node matching the value, offset, and mask of the item you selected. You can give the new filter a name and click **OK** to save it. If you wish to edit the details of the filter, double-click on the new node to open it in the **Value Filter** edit dialog. For more information about Value filters, please see “Value filter nodes” on page 227.

The same packet is shown first without, and then with offsets in Figure 16.4.



HTTP-WEP.apc - Packet #9

Packet: 9

```
802.11 MAC Header
  Version:              0
  Type:                 %10   Data
  Subtype:              %0000   Data Only
  To DS:                0
  From DS:              1
  More Frag.:           0
  Retry:                0
  Power Mgmt:           0
  More Data:            0
  WEP:                  1
  Order:                0
  Duration:             218   Microseconds
  Destination:          00:A0:F8:9B:B9:AA
  BSSID:                00:A0:F8:8B:20:1F
```

Show Data Offsets
Disabled

HTTP-WEP.apc - Packet #9

Packet: 9

```
802.11 MAC Header
  Version:              0 [0 Mask 0x03]
  Type:                 %10   Data [0 Mask 0x0C]
  Subtype:              %0000   Data Only [0 Mask 0xF0]
  To DS:                0 [1 Mask 0x01]
  From DS:              1 [1 Mask 0x02]
  More Frag.:           0 [1 Mask 0x04]
  Retry:                0 [1 Mask 0x08]
  Power Mgmt:           0 [1 Mask 0x10]
  More Data:            0 [1 Mask 0x20]
  WEP:                  1 [1 Mask 0x40]
  Order:                0 [1 Mask 0x80]
  Duration:             218   Microseconds [2-3]
  Destination:          00:A0:F8:9B:B9:AA [4-9]
  BSSID:                00:A0:F8:8B:20:1F [10-15]
```

Show Data Offsets
Enabled

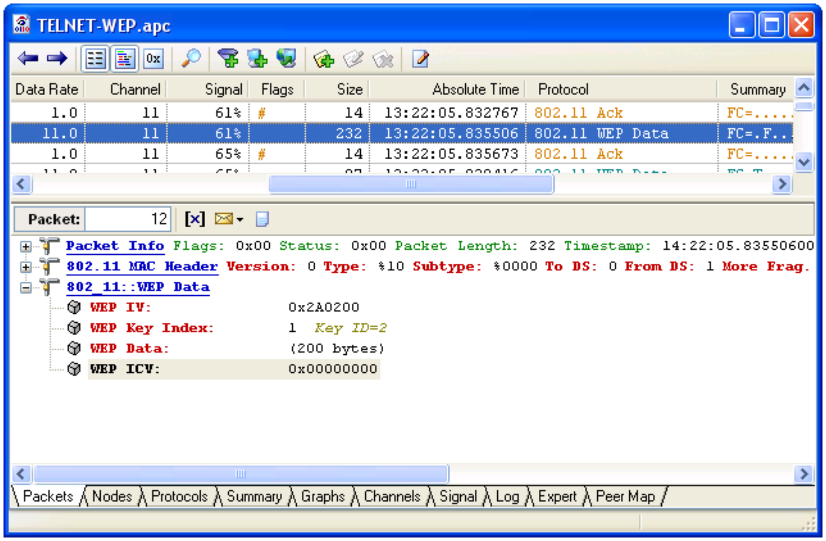
Figure 16.4 Show Data Offsets—disabled above, enabled below

Apply WEP decryption

If you have created a WEP key set for your network and enabled it in the Options dialog, these key sets can be used to decrypt packets in the ***Decode*** view of the **Packet Decode** window or in the Decode pane of the ***Packets*** view of a Capture window or a Packet File window. For information about WEP and how to enable key sets for use in WEP decryption, please see “WEP encryption and AiroPeek” on page 24.

Open a WEP-encrypted packet, click the **Apply Decryption** button and choose the key set to apply to this packet from the list. Alternatively, you can choose *none* to return to the WEP-encrypted view of the current packet. If the key set you chose matches the one used to encrypt the current packet, AiroPeek decrypts the original packet and displays a plaintext copy in the ***Decode*** view. This decrypted copy appears as the packet would have if it had been sent without WEP encryption.

Figure 16.5 shows the same packet before and after the application of decryption using the correct WEP key set.



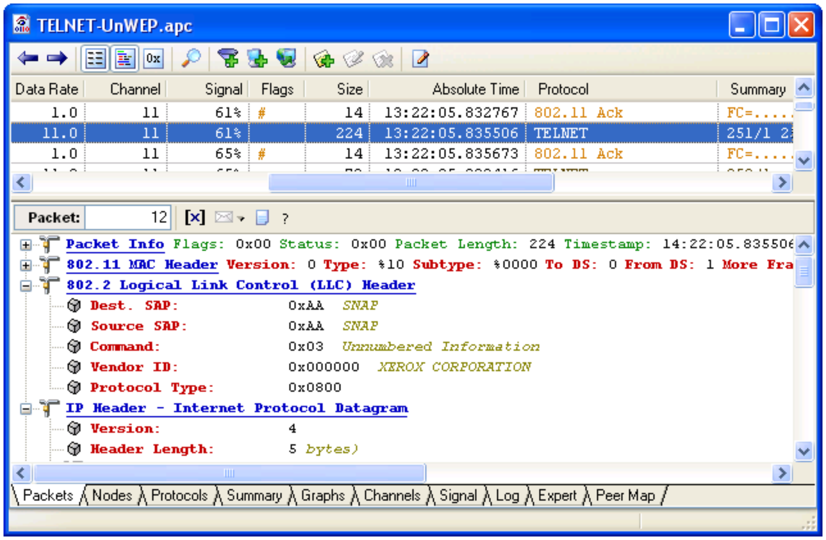
TELNET-WEP.apc

```
Data Rate  Channel  Signal  Flags  Size   Absolute Time    Protocol          Summary
      1.0       11     61%  #        14  13:22:05.832767  802.11 Ack        FC=.....
     11.0       11     61%          232  13:22:05.835506  802.11 WEP Data   FC=.F..
      1.0       11     65%  #        14  13:22:05.835673  802.11 Ack        FC=.....
```

Packet: 12

```
⊞ Packet Info Flags: 0x00 Status: 0x00 Packet Length: 232 Timestamp: 14:22:05.83550600
⊞ 802.11 MAC Header Version: 0 Type: %10 Subtype: %0000 To DS: 0 From DS: 1 More Frag.
⊟ 802_11::WEP Data
      WEP IV:            0x2A0200
      WEP Key Index:     1  Key ID=2
      WEP Data:          (200 bytes)
      WEP ICV:           0x00000000
```

WEP-encrypted



TELNET-UnWEP.apc

```
Data Rate  Channel  Signal  Flags  Size   Absolute Time    Protocol          Summary
      1.0       11     61%  #        14  13:22:05.832767  802.11 Ack        FC=.....
     11.0       11     61%          224  13:22:05.835506  TELNET            251/1 2
      1.0       11     65%  #        14  13:22:05.835673  802.11 Ack        FC=.....
```

Packet: 12

```
⊞ Packet Info Flags: 0x00 Status: 0x00 Packet Length: 224 Timestamp: 14:22:05.835506
⊞ 802.11 MAC Header Version: 0 Type: %10 Subtype: %0000 To DS: 0 From DS: 1 More Fra
⊟ 802.2 Logical Link Control (LLC) Header
      Dest. SAP:         0xAA   SNAP
      Source SAP:        0xAA   SNAP
      Command:           0x03   Unnumbered Information
      Vendor ID:         0x000000   XEROX CORPORATION
      Protocol Type:     0x0800
⊟ IP Header - Internet Protocol Datagram
      Version:           4
      Header Length:     5  bytes)
```

Decrypted

Figure 16.5 WEP-encrypted and decrypted views of the same packet

Decode raw data only

Click the **Decode Raw** button to present only the raw data found in the packet. Ordinarily, when you choose **Print Selected Packets…** from the **File** menu, or use **File** > **Save Selected Packets…** and choose any of the *Decoded Packets* formats, only the contents of the ***Decode*** view is printed or saved. If you wish to print or save the hexadecimal and ASCII contents of the Raw Data pane of a packet, first click the **Decode Raw** button. Only the information added by AiroPeek and the contents of the Raw Data pane will be printed or saved.

Choose decoder

You can open the **Select Decoder** window for certain packets by clicking the **Choose Decoder** button. The **Choose Decoder** button appears as a question mark (?) when this option is available for the current packet.

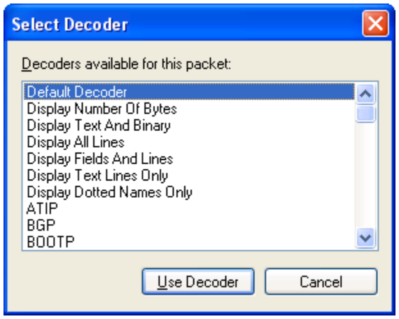


Figure 16.6 Select Decoder dialog

The **Select Decoder** window shows a context-sensitive list of decoders which can be applied to the current packet. If the packet contains TCP or UDP, this list will include generic line decoders such as *Display Number Of Bytes*. See Table 16.2 for a list of the available line decoders and their behavior. Alternatively or in addition, the **Select Decoder** window may present decoders for protocols which, because of their lack of uniquely identifying attributes, can often be mistaken for one another. Examples include particular types of RPC (Remote Procedure Call), TFTP (Trivial File Transfer Protocol), and others.

To use a particular decoder to decode the current packet *and all subsequent packets of the same type*, select the decoder from the list presented in the **Select Decoder** window and click the **Use Decoder** button at the bottom of the window.

If you wish to apply a different decoder to the same packet, or to all subsequent packets of this type, click the **Choose Decoder** button to re-open the **Select Decoder** window, choose the new decoder, and click **Use Decoder**. When the program believes that it knows how to decode the current packet properly, the **Select Decoder** window will present the *Default Decoder* choice at the top of the list of available decoders. You can choose this decoder to apply or re-apply the program's default decode behavior to the current packet (and all subsequent packets of the same type) at any time.

Note: Decoders only affect the display of data in the ***Decode*** view of **Packet Decode** windows and the Decode pane of Capture windows and Packet File windows. The ***Raw Data*** view or Raw Data pane always shows the actual packet data in hex and ASCII.

The **Choose Decoder** function is particularly useful in environments where new protocols are under development, or where TCP or UDP applications are using non-standard ports.

Table 16.2 Line decoders for TCP and UDP packets

Decoder	Shows
Default Decoder	When you select this decoder, the program returns to its default behavior when decoding packets of the current type. Use this selection to stop using any decoder previously selected in the **Select Decoder** window and restore the program's ability to choose its own decoder.
Display Number Of Bytes	This line decoder displays only the number of bytes in the UDP or TCP payload of the packet.
Display Text And Binary	This line decoder displays 0x00 through 0x1F as their code equivalents (0x00, for example, is *<NULL>*), displays (non-extended) ASCII characters as ASCII text, and displays any other values as a dot (.). In comparison, the ASCII part of the ***Raw Data*** view displays the extended ASCII character set (which includes accented characters, for example) and displays all non-ASCII values as dots.

Table 16.2 **Line decoders for TCP and UDP packets (continued)**

Decoder	Shows
Display All Lines	This line decoder displays only (non-extended) ASCII characters, plus line feed / carriage return (0x0D and 0x0A). When it encounters the first value outside this set, the decoder stops and displays the number of bytes remaining in the payload portion of the UDP or TCP packet.
Display Fields And Lines	This line decoder searches for lines containing semi-colons (;). Each line with a semi-colon is split in two, with the part before the semi-colon treated as the label and the part to the right of the semi-colon treated as the data. Lines containing text without semi-colons are treated as for the *Display All Lines* decoder above. That is, non-extended ASCII text is displayed until the first non-ASCII character is reached. The decoder then displays the number of bytes remaining in the payload of the TCP or UDP packet. This decoder is particularly useful in quickly scanning through the Label;Value pairs found in HTTP and FTP packets, particularly when the transactions are taking place on ports other than the default port 80 (HTTP) or port 21 (FTP).
Display Text Lines Only	This line decoder displays all the non-enhanced ASCII characters, plus line feeds and carriage returns (LF/CR), ignoring all other characters. If no LF/CR is encountered, lines are automatically wrapped at 120 characters.
Display Dotted Names Only	This line decoder searches for lines of non-extended ASCII text containing the period character(.). It displays each such line. All other lines are ignored. This decoder is useful when scanning for file names and IP names and addresses that use dotted notation.

Important! When you choose a decoder in the **Select Decoder** window, AiroPeek will continue to use that decoder every time it encounters a packet of the same type. To restore the program's ability to choose its own decoder, select a packet of the same type, open the **Select Decoder** window, choose *Default Decoder* from the list, and click the **Use Decoder** button.

Writing your own decoders

If you find proprietary protocols on your network for which AiroPeek does not supply decoders, or if you are developing your own protocols, you may want to write your own decoders for use with AiroPeek.

AiroPeek lets you write your own packet decoders and add them to the Decodes directory for use with the application. Documentation on writing decoders is included in the Documents directory in the directory where you installed AiroPeek.

Note: Writing packet decoders requires programming knowledge.

Printing, saving and copying

To print decoded packets, open a **Packet Decode** window and make it the front-most or active window. From the **File** menu choose **Print** to print out a formatted version of *only* the ***Decode*** view of the **Packet Decode** window. An alternative is to save the decoded packets as RTF or HTML and print them from another application that can read and print those file types. This alternative preserves the formatting of the **Packet Decode** window. To print the decode portion of multiple packets as a single file, select the packets and choose **Print Selected Packets…** from the **File** menu.

To save packets in their decoded form, select the packets (highlight them) in the Packet List pane of the ***Packets*** view of a Capture window or a Packet File window. From the **File** menu, choose **Save Selected Packets** to open the **Save** dialog. In the **Save** dialog, choose a file type of plain text, RTF or HTML. Give the file a name and click **Save** to save the files to your chosen location.

To save or print the hexadecimal and ASCII contents of the Raw Data pane, click the **Decode Raw** button before saving or printing. For details, see “Decode raw data only” on page 327.

You can copy an individual line from any pane of a **Packet Decode** window to the clipboard and paste it into another application as plain text by using standard editing keystroke combinations.

Using thread intelligence in AiroPeek

Packets usually contain the information AiroPeek requires to decode them into their protocol components. For some protocols, however, the required information is not contained in the packet itself, but in a previous packet exchanged between the same two nodes. AiroPeek supports thread intelligence for some protocols, including Simple Network Management Protocol (SNMP), Simple Mail Transfer Protocol (SMTP), AppleTalk Session Protocol (ASP), Printer Access Protocol (PAP), NetWare Core Protocol (NCP), and others.

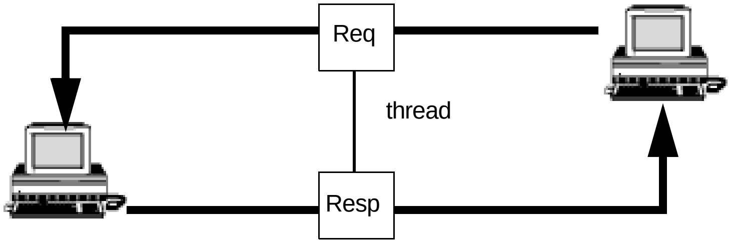


Figure 16.7 Protocol decode thread maintained by AiroPeek

When two or more packets are related to the same session in one of these protocols, AiroPeek can pre-decode them in the order in which they arrived, allowing the Request/ Response pairs to be connected. This provides a richer set of decode information than would otherwise be available. This relationship between packets is called a thread, and the pre-decoding done to establish the thread is called making a thread.

To make threads, select the packets in the Packet List among which you believe threads may exist. You can use **CTRL + A** to select all packets. Right click and choose **Make Threads** from the context menu.

AiroPeek uses threads to keep track of the protocol type in decoding Response packets associated with a particular Request.

There are two ways to employ thread intelligence in AiroPeek:

- The **Select Related Packets** command—to find possibly related threads.
- The **Make Threads** command—to automatically create any threads from packets near the selected packets.

Manually selecting further decode options

When AiroPeek maintains a decode thread, the assumed protocol type is displayed at the top of the **Packet Decode** window for the relevant chosen packet.

If you view the Request packet first, AiroPeek keeps track of the thread when you open the corresponding Response and Release packets. However, if you view a Response packet before you have opened a preceding Request, no thread will have been started, and AiroPeek will simply show a question mark (**?**) instead of the protocol type at the top of the **Packet Decode** window.

You can click on the **Choose Decoder** button (a question mark) to open the **Select Decoder** dialog, and then manually choose the decoder to use.

As an alternative to manually selecting options for further decoding packets, you can instruct AiroPeek to make threads before opening any packets. This ensures that the threads will exist even if you open a Response packet first. To make threads in the background before you open packets, use the **Select Related Packets** command or **Select All Packets** (either from the **Edit** menu or from the context menu), and then choose the **Make Threads** command from the context menu (right click). You can then view packets in any order.

Sending Packets

When you set a valid adapter not used for Monitor statistics or Capture functions as the Send Adapter, AiroPeek can send packets.

You can use the packet transmission feature to generate network traffic or to probe specific computers to observe their reactions. You can also check network connections by using the send function at the computer being checked, while using a second computer running AiroPeek to observe the resulting activity.

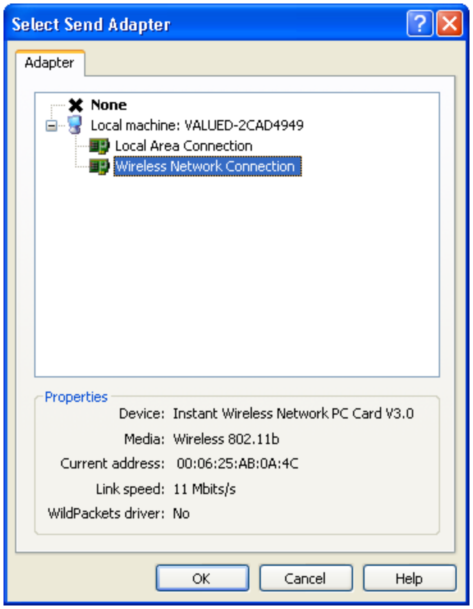
You can send a single packet, a set of bursts at intervals, or a single burst of packets. You can send a generic TCP/IP packet, or select any captured packet as the Send Packet. You can also edit the contents of the Send Packet.

In this Chapter:

About the send function in AiroPeek

The send function in AiroPeek allows you to send data packets onto the wireless network. AiroPeek interacts with the 802.11 WLAN protocol stack at a higher level than does, for example, the WildPackets EtherPeek analyzer with the Ethernet protocol stack. In AiroPeek, the 802.11 WLAN retains control over the construction and use of all control and management packets, as it must to insure network connectivity. When you use the Send function in AiroPeek, any packets you send will become the data payload of 802.11 WLAN packets. These packets will be constructed according to the network set-up defined by your operating system for the selected Send Adapter.

Select send adapter



None
Local machine: VALUED-2CAD4949
Local Area Connection
Wireless Network Connection

Properties
Device: Instant Wireless Network PC Card V3.0
Media: Wireless 802.11b
Current address: 00:06:25:AB:0A:4C
Link speed: 11 Mbits/s
WildPackets driver: No

Figure 17.1 Select Send Adapter dialog

In order for AiroPeek to send packets, you must first select an adapter to use for this purpose. Under the **Send** menu, choose **Select Send Adapter…** to open the **Select Send Adapter** dialog. Select a valid adapter and click **OK** to make your choice. The adapter used to send packets cannot be in RF Monitor mode. That is, it cannot already be selected as the adapter for Monitor statistics or for the use of any Capture window. The **Select Send Adapter** dialog will not change the mode of an adapter being used by these other “listen only” functions.

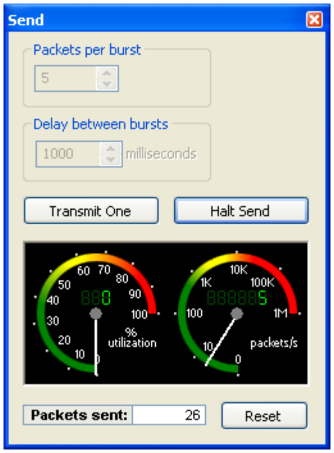
Important! If the adapter you select as the Send Adapter is a valid adapter, the **Select Send Adapter** dialog will let you choose it. But if the Send Adapter is in RF Monitor mode, attempts to use the Send function will silently fail to send packets.

The send packet

AiroPeek ships with a generic Ethernet packet already set as the default Send Packet. Alternatively, you may choose another packet to send onto the network. You can select any packet from the ***Packets*** view of any active window and set it as the Send Packet by selecting the packet and choosing **Set Send Packet** from the **Send** menu.

To send

To send traffic onto the network from AiroPeek or to set the parameters for send events, choose **Send Window** from the **Send** menu.


Send

Packets per burst: 5

Delay between bursts: 1000 milliseconds

Packets sent: 26

Figure 17.2 Send window

At the bottom of the **Send** window (Figure 17.2) are two dials with digital readouts. They show the *% utilization* (percent of utilization of maximum network bandwidth) and *packets/s* (packets per second) represented by the packets being sent in the current send event. The **Send** window also shows the total *Packets sent* in the current send event.

There are several ways to send packets:

- send a single copy of the Send Packet out on the network.
- send bursts of multiple copies of the Send Packet at specified intervals.
- send a selected packet or group of packets in a single burst.

Transmit one

The simplest form of sending a packet is to use **Transmit One**. Select **Transmit One** from the **Send** menu, click the **Transmit One** button in the **Send** window, or simply type **Ctrl + T**. This causes the immediate transmission of exactly one of the specified Send Packet.

Send multiple copies of a packet at specified intervals

The second way to generate traffic is to transmit copies of the Send packet in bursts at specified intervals. Use the text entry boxes in the **Send** window to establish the number of *Packets per burst* and the *Delay between bursts*, in milliseconds. The text entry boxes can be edited directly or you can use the arrows at the right to set these numbers. Note that the minimum delay between bursts is one millisecond.

When you have set these parameters, you can initiate the send process by selecting the **Initiate Send** command from the **Send** menu, clicking the **Initiate Send** button in the **Send** window, or simply typing **Ctrl + I** (letter “i”). When you initiate a send, the **Initiate Send** command in the **Send** menu changes to **Halt Send**.

Sending selected packets

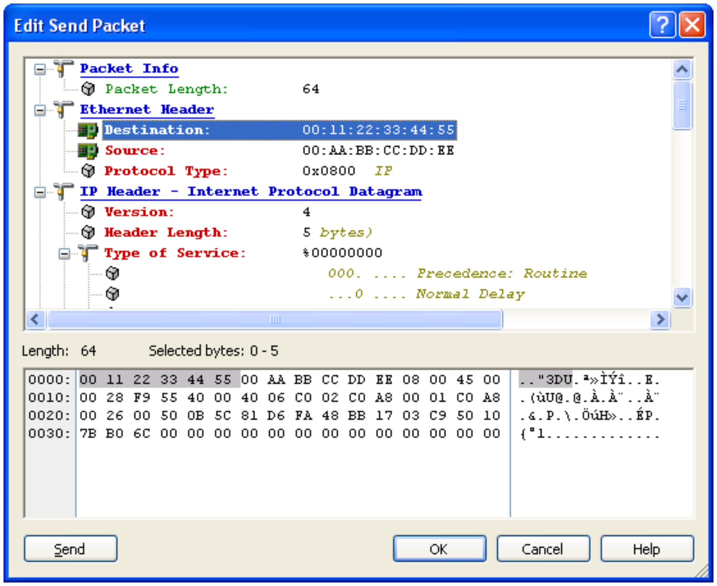
The **Send Selected Packets** command in the **Send** menu is enabled when you are in the ***Packets*** view of a Capture window or a Packet File window and a packet or packets are selected. The selected packets will be sent in a single burst at one millisecond intervals between packets.

Editing send packet contents

AiroPeek ships with a generic Ethernet packet as the default Send Packet. Alternatively, you may select another packet to send onto the network. You can choose any packet from the ***Packets*** view of any active window and set it as the Send Packet by selecting the packet and choosing **Set Send Packet** from the **Send** menu.

To edit the contents of the Send Packet:

1. Choose **Edit Send Packet** from the **Send** menu to open the **Edit Send Packet** window (Figure 17.3).



```
Packet Info
    Packet Length:          64
Ethernet Header
    Destination:            00:11:22:33:44:55
    Source:                 00:AA:BB:CC:DD:EE
    Protocol Type:          0x0800  IP
IP Header - Internet Protocol Datagram
    Version:                4
    Header Length:          5 bytes)
    Type of Service:        %00000000
                              000. ....  Precedence: Routine
                              ...0 ....  Normal Delay
```

Length: 64   Selected bytes: 0 - 5

```
0000: 00 11 22 33 44 55 00 AA BB CC DD EE 08 00 45 00  .."3DU.ª»ÌÝî..E.
0010: 00 28 F9 55 40 00 40 06 C0 02 C0 A8 00 01 C0 A8  .(ùU@.@.À.À¨..À¨
0020: 00 26 00 50 0B 5C 81 D6 FA 48 BB 17 03 C9 50 10  .&.P.\.ÖúH»..ÉP.
0030: 7B B0 6C 00 00 00 00 00 00 00 00 00 00 00 00 00  {°l.............
```

Figure 17.3 Editing a Send Packet

2. The layout of the **Edit Send Packet** window is similar to that of the **Packet Decode** window, with a ***Decode*** view above and a ***Raw Data*** view below. Each line of the ***Raw Data*** view begins at the left with the offset of the first character of that line, followed by 16 bytes of hex data (one two-digit hexadecimal number per byte) followed by the same 16 bytes represented in ASCII characters (one character per byte).

3. Each ASCII character is the equivalent of its corresponding hexadecimal pair on the left hand side. You can edit either of the representations by directly overwriting the contents.

The highlighting in the three parts of the **Edit Send Packet** window makes it easy to keep track of where in the packet your edits are being made.

4. In the display area between the ***Decode*** view and the ***Raw Data*** view, the **Edit Send Packet** window shows the *Length* of the packet (including all headers) and the data offsets of the *Selected bytes*.
5. In the ***Decode*** view of the **Edit Send Packet** window in Figure 17.3 above, the decode still shows an accurate decoding of this part of the packet. As editing proceeds, the ***Decode*** view attempts to update on-the-fly and show an accurate decode of the Send Packet, as edited.
6. When you have finished editing the Send Packet, choose **OK** to use the changes you have made, or click **Cancel** to ignore any changes and leave the Send Packet as it was.

Appendices

Packets and Protocols

This section provides both an explanation of how AiroPeek works and an introduction to the basic concepts and vocabulary of WLAN networking. It also provides a brief overview of the 802.11 WLAN protocol as well as a detailed breakdown of 802.11 WLAN packet headers and 802.2 LLC headers, and the information they contain.

AiroPeek, packets and protocols

This first section explains how AiroPeek works, and offers a brief introduction to the concepts of packets and protocols. For a list of recommended readings on networking topics, please visit http://www.wildpackets.com/support/resources.

How AiroPeek monitors and captures network traffic

AiroPeek takes advantage of a fundamental characteristic of 802.11 WLAN networks. On an 802.11 WLAN, one computer does not send a packet exclusively to another computer. Instead, it puts the address of the desired destination or receiving station in the header of the packet, and puts the packet out onto the airwaves. Each network node within range listens to the transmission and uses the first address in the 802.11 WLAN MAC header to determine if that node should process it. If the packet was intended for a particular computer, that machine captures it, puts it in memory, and then passes it to the next layer of the protocol stack for processing. If the message was received intact, the receiving node typically sends an ACK to acknowledge this.

For example, device A in Figure A.1 transmits a packet addressed to device C. All devices within range receive a packet that contains device C’s address, but devices B, D, and E ignore the packet when they find an address not their own in the first address field of the packet’s MAC header. Only device C, finding its own address in that first field, processes the packet further.

When AiroPeek runs on a workstation, it puts the 802.11 WLAN hardware in *Promiscuous Mode*. In Promiscuous Mode, the workstation running AiroPeek accepts every packet, whether or not it is addressed to that workstation. AiroPeek installs itself parallel to any other stacks on the workstation, telling the driver it wants to see every packet of every description that it finds on the network.

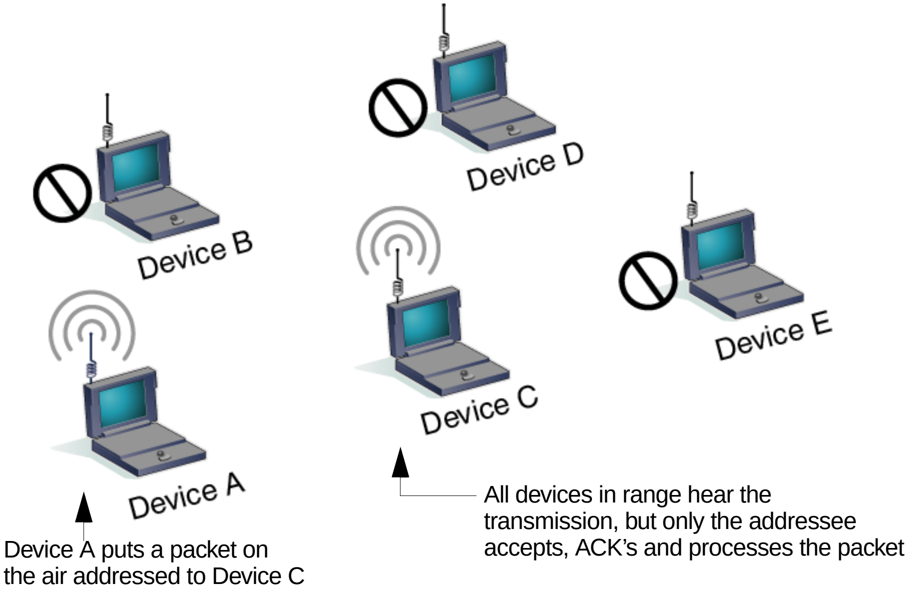

Device B
Device D
Device C
Device E
Device A
Device A puts a packet on the air addressed to Device C
All devices in range hear the transmission, but only the addressee accepts, ACK's and processes the packet

Figure A.1 Packets are received by all devices on the network

For example, if AiroPeek is running on device D in Figure A.2 and device A sends a packet addressed only to device C, both device C *and device D* accept and process the packet.

Device C acknowledges the receipt and processes the packet normally, passing it to the next layer of the protocol software. Device D also captures the transmission and passes the packet to AiroPeek. The machine on which AiroPeek is running will not send any acknowledgement, because Promiscuous Mode is strictly a listening mode. Radio transceivers cannot listen and send at the same time on the same frequencies because their own transmission would drown out any incoming traffic.

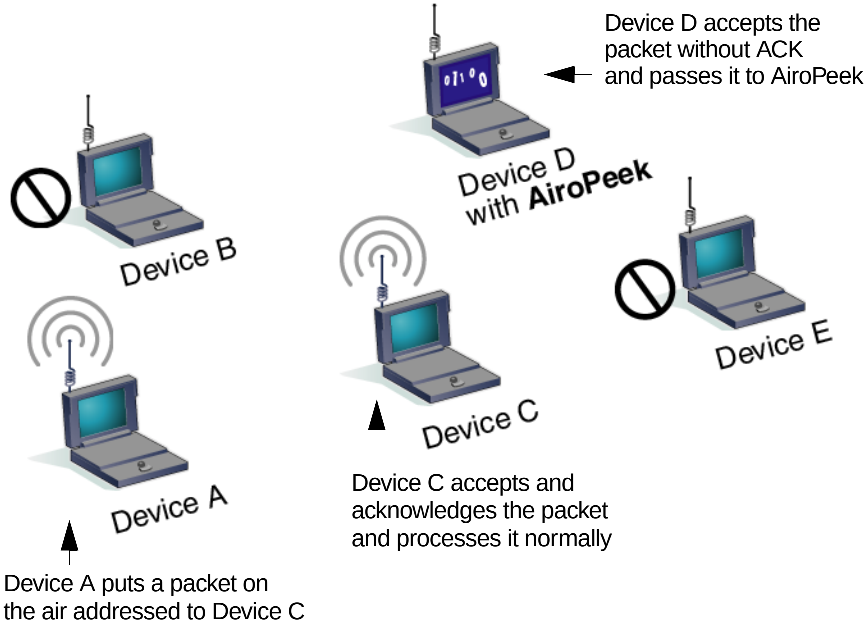

Device D accepts the packet without ACK and passes it to AiroPeek
Device D with AiroPeek
Device B
Device E
Device C
Device A
Device C accepts and acknowledges the packet and processes it normally
Device A puts a packet on the air addressed to Device C

Figure A.2 AiroPeek accepts all packets (Promiscuous Mode) without acknowledgement

Important! Under certain network or program configurations, AiroPeek can enable the user to monitor information that might be considered confidential. For example, some passwords may be viewable from AiroPeek if WEP is not implemented on your network, or if you configure AiroPeek to monitor the network as a peer WEP host. Because of this, you may want to prevent unauthorized access to the program. Consider limiting access to AiroPeek by not installing it on public machines and servers.

What is a packet?

Each piece of information transmitted on an IEEE 802.x network is sent in something called a *packet*. A packet is simply a chunk of data enclosed in one or more wrappers that help to identify the chunk of data and route it to the correct destination. *Destination* in this sense means a particular application or process running on a particular machine. These wrappers consist of *headers*, or sometimes headers and *trailers*. Headers are simply bits of data added to the beginning of a packet. Trailers are added to the end of a packet.

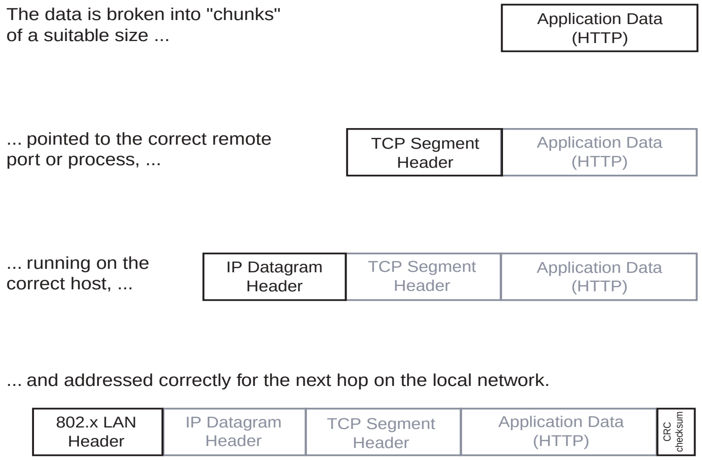
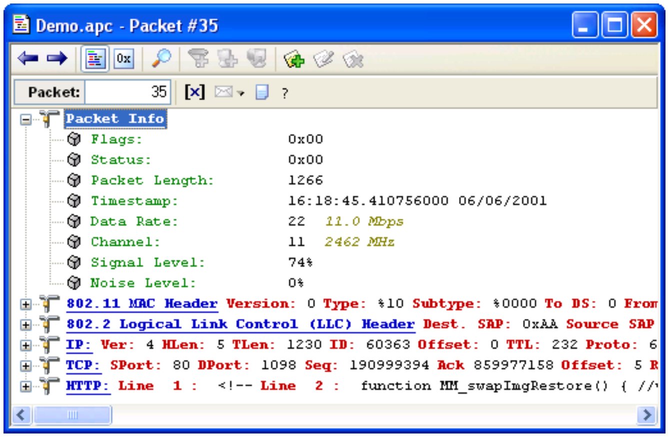

The data is broken into "chunks" of a suitable size ...
Application Data (HTTP)
... pointed to the correct remote port or process, ...
TCP Segment Header
Application Data (HTTP)
... running on the correct host, ...
IP Datagram Header
TCP Segment Header
Application Data (HTTP)
... and addressed correctly for the next hop on the local network.
802.x LAN Header
IP Datagram Header
TCP Segment Header
Application Data (HTTP)
CRC checksum

Figure A.3 Constructing a network data packet (here, a piece of a web page)

Packets are created at the machine sending the information. The application generating the data on the sending machine passes the data to a *protocol stack* running on that machine. The protocol stack breaks the data down into chunks and wraps each chunk in one or more wrappers that will allow the packets to be reassembled in the correct order at the destination. The protocol stack on the sending machine then passes the packets to the network hardware: the *NIC* (Network Interface Card). The network hardware adds its own wrapper (the 802.x header and trailer) to each packet to direct it to the correct destination on the local network.

If the packet’s ultimate destination is somewhere off the local network, the header added by the sending machine will point to a router or switch as its destination address. The router will open the packet, strip off the original wrapper, read far enough to find the ultimate destination address, then re-wrap the packet, giving it a new header that will send it on the next hop of its journey.

At the receiving end, the process is reversed. The packet is read by the NIC at the receiving machine which strips off the network header and passes the packet up to the appropriate protocol stack. The protocol stack reads and strips off its headers and passes the remaining packet contents on up to the application or process to which it was addressed, reassembling the chunked data in the correct order as it arrives.



```
Packet Info
    Flags:                   0x00
    Status:                  0x00
    Packet Length:           1266
    Timestamp:               16:18:45.410756000 06/06/2001
    Data Rate:               22   11.0 Mbps
    Channel:                 11   2462 MHz
    Signal Level:            74%
    Noise Level:             0%
802.11 MAC Header Version: 0 Type: %10 Subtype: %0000 To DS: 0 From
802.2 Logical Link Control (LLC) Header Dest. SAP: 0xAA Source SAP
IP: Ver: 4 HLen: 5 TLen: 1230 ID: 60363 Offset: 0 TTL: 232 Proto: 6
TCP: SPort: 80 DPort: 1098 Seq: 190999394 Ack 859977158 Offset: 5 R
HTTP: Line  1 :  <!-- Line  2 :  function MM_swapImgRestore() { //
```

Figure A.4 AiroPeek decode of an HTTP packet (collapsed view)

The packet diagramed in Figure A.3 above is shown again in a **Packet Decode** window in Figure A.4. The ***Decode*** view shows multiple fields calculated by AiroPeek at the top of the window, then shows each of the layers of the packet. In this view, the "**+**" signs in the margin indicate that the details for each part of the packet are hidden under their headings. AiroPeek displays the packet contents in the same order in which it appears in the packet: 802.11 WLAN header, IP header, then the TCP and the HTTP payload.

What is a protocol?

A *protocol* is a set of rules governing communications.

Networking protocols specify what types of data can be sent, how each type of message will be identified, what actions can or must be taken by participants in the conversation, precisely where in the packet header or trailer each type of required information will be placed, and more.

AiroPeek understands protocols by examining the contents of the packets those protocols create. Each protocol has a variety of forms of headers and sometimes trailers that it uses, either to transmit data for other applications, or to transmit control and information messages that support its own functionality. The exact form of these wrappers or headers tends to be unique, not only among functions within a given protocol, but also across protocols.

AiroPeek tells the network adapter that it wants to see all traffic from *all* of the various protocol stacks: AppleTalk, TCP/IP, DECnet, NetWare or others. AiroPeek decodes the packets in order to identify as precisely as possible what function each packet serves within its protocol. WildPackets’ ProtoSpecs™ technology refers to these various functions as *sub-protocols*. In other, more formal views of networking, TCP and UDP may be seen as protocols in their own right, HTTP may be seen as an application running under TCP/IP, and so on. ProtoSpecs side-steps all these largely formal naming conventions and simply treats all of them—UDP, TCP, and HTTP—as sub-protocols of IP. ProtoSpecs does preserve the correct functional relationships among the various sub-protocols, however. HTTP, for instance, is shown as a sub-protocol of TCP which is itself a sub-protocol of IP.

802.11 WLAN overview

This section presents a detailed overview of the 802.11 WLAN standards. The information is presented under general functional headings. A detailed breakdown of 802.11 WLAN packet headers and of 802.2 LLC headers is presented after the overview.

Development of the IEEE 802.11 WLAN standards

In 1997, IEEE approved 802.11, the first internationally sanctioned wireless LAN standard. This first standard proposed any of three (mutually incompatible) implementations for the physical layer: infrared (IR) pulse position modulation, or radio frequency (RF) signalling in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS). The IR method was never commercially implemented. The RF versions suffered from low transmission speeds (2 Mbps). In an effort to increase throughput, IEEE established two working groups (A and B) to explore alternate implementations of 802.11. A third group, Working Group G, was set up after these two.

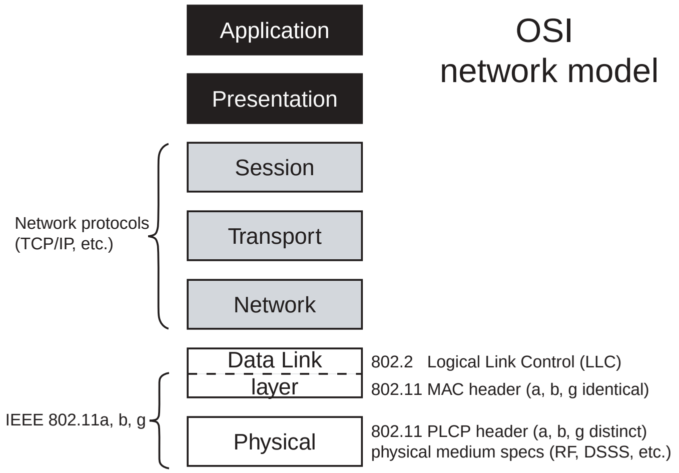

Application
Presentation
Session
Transport
Network
Data Link layer
Physical
OSI network model
Network protocols (TCP/IP, etc.)
IEEE 802.11a, b, g
802.2 Logical Link Control (LLC)
802.11 MAC header (a, b, g identical)
802.11 PLCP header (a, b, g distinct)
physical medium specs (RF, DSSS, etc.)

Figure A.5 802.11 and the 0SI Model

Working Group A explored the 5.0 GHz band, using orthogonal frequency division multiplexing (OFDM) to achieve throughputs in the range of 54 Mbps. The challenges, both to produce low cost equipment operating at such high frequencies and to reconcile competing international uses of this spectrum, kept their 802.11a WLAN standard from reaching the market before mid-2002.

European regulators require 802.11a WLAN devices to support the added functions of dynamic frequency selection (DFS) and transmit power control (TPC). These help to avoid or mitigate interference between 802.11a WLANs and existing 5.0 GHz band uses.

Working Group B explored more sophisticated DSSS techniques in the original 2.4 GHz band. Their 802.11b WLAN standard, published in September 1999, can deliver raw data rates of up to 11 Mbps. The majority of WLAN systems in the market today follow the 802.11b WLAN standard.

The IEEE Working Group G began by exploring a variety of methods to further improve throughput in the 2.4 GHz spectrum used by the 802.11b standard. In May 2001, the FCC removed its ban on the use of OFDM technology in the 2.4GHz band. In November of 2001, Working Group G tabled a draft standard adopting OFDM, the same signalling method used in the 802.11a WLAN standard. The 802.11g WLAN standard is not absolutely finalized at this writing, but the main outlines are clear. One significant aspect of 802.11g is the degree to which it supports backward compatibility with the older 802.11b standard, which uses the same spectrum. When 802.11b nodes are present, 802.11g nodes use the RTS/CTS as a prelude to each packet transmission. Although the maximum raw data rates for 802.11g WLANs are as high as those of 802.11a WLANs, the actual data throughput for 802.11g drops significantly when 802.11b nodes are present. Mixed 802.11b/g networks are possible, but the maximum performance will be much higher in a pure 802.11g WLAN.

The 802.11 WLAN protocols specify the lowest layer of the OSI network model (physical) and a part of the next higher layer (data link). A stated goal of the initial IEEE effort was to create a set of standards which could use different approaches to the physical layer (different frequencies, encoding methods, and so forth), and yet share the same higher layers. They have succeeded, and the Media Access Control (MAC) layers of the 802.11a, b, and g protocols are substantially identical. At the next higher layer still, all 802.11 WLAN protocols specify the use of the 802.2 protocol for the logical link control (LLC) portion of the data link layer. In the OSI model of network stack functionality (see Figure A.5), such protocols as TCP/IP, IPX, NetBEUI, and AppleTalk exist at still higher layers, and utilize the services of the layers underneath.

Radio frequencies and channels

The most striking differences between WLANs and wired networks such as Ethernet are those imposed by the difference in the transmission medium. Where Ethernet sends electrical signals through wires, WLANs send radio frequency (RF) energy through the air. Wireless devices are equipped with a special network interface card (NIC) with one or more antennae, a radio transceiver set, and circuitry to convert between the analog radio signals and the digital pulses used by computers.

Radio waves broadcast on a given frequency can be picked up by any receiver within range tuned to that same frequency. Effective or usable range depends on a number of factors. In general, higher power and lower frequency increase the range at which a signal can be detected. Distance from the signal source and interference from intervening objects or other signals all tend to degrade reception. Filtering, accurate synchronous timing, and a variety of error correcting approaches can help distinguish the true signal from reflections and interference.

Information is carried by modulating the radio waves. In spread spectrum technologies, additional information is packed into a relatively small range of frequencies (a section of bandwidth called a channel) by having both sender and receiver use the same set of codes, such that each small modulation of the set of radio waves carries the greatest possible information. Direct sequence spread spectrum (DSSS) is one particular approach to packing more data into a given piece of RF spectrum. OFDM is another.

The FCC in the United States and other bodies internationally control the use of RF spectrum and limit the output power of devices. The 802.11 WLAN standards attempt to deliver maximum performance within the limits set by these bodies, current radio technology and the laws of physics.

Low output power, for example, limits 802.11 WLAN transmissions to fairly short effective ranges measured in hundreds of feet. Signal quality, and hence network throughput, diminishes with distance and interference. The higher data rates rely on more complex spectrum spreading techniques. These in turn require an ability to distinguish very subtle modulations in the RF signals.

Signal and noise measurement

The electrical energy in radio waves and other electrical signals is often measured in the unit of power Watts or, in the case of 802.11 WLANs, milliWatts (mW). For example, a typical 802.11b WLAN card might have a transmit power of 32 mW. The energy detected at the receiving antenna would be several orders of magnitude smaller than this. The wide range of values encountered in radio engineering could be expressed with exponential notation, but radio engineers came up with a simpler solution. They measure signal strength with a unit called the decibel-milliWatt, or dBm.

A decibel is simply a unit of relationship between two power measurements. It is, in fact, one tenth of the exponent of ten. That is, 10 decibels denotes an increase by a factor of 10, 20 decibels an increase by a factor of 100, and 30 decibels an increase by a factor of 1,000. These correspond to 10 raised to the power of (10/10), 10 raised to the power of (20/10), and 10 raised to the power of (30/10), respectively.

Decibels are dimensionless. By associating decibels with a particular unit, it is possible to write and compare a wide range of power values easily. By the definition of the decibel milliwatt, 0 dBm = 1 mW. Power values larger than 1 mW are positive numbers. Power values smaller than 1 mW are expressed as negative numbers. Remember, this is an exponent. For example, the power output of 32mW mentioned above could be written as 15 dBm. A typical lower limit of antenna sensitivity for an 802.11b WLAN card might be expressed as -83 dBm. A more practical lower limit might be -50 dBm, or 0.00001 mW.

Not all 802.11 WLAN cards report signal strength in dBm. The 802.11 WLAN standard itself calls for makers to implement their own scale of received signal strength, and report that within the protocol as a value called Received Signal Strength Indicator (RSSI). While one manufacturer might use a scale of 0-31, another might use 0-63. AiroPeek regularizes these values to a percentage and reports them as signal strength.

Noise is also a form of electrical energy, and is reported in the same way, either as a percentage or in dBm. The signal to noise ratio is simply the difference between signal and noise.

Transmission rates and channels

To overcome signal degradation problems, 802.11 WLANs can gracefully step down to a slower but more robust transmission method when conditions are poor, then step back up again when conditions improve.

The full set of data rates for all three standards is shown in Table A.1. For 802.11a WLANs, the 6, 12, and 24 Mbps data rates are mandatory, all others are optional. The 802.11g WLANs will support all the same data rates as 802.11a WLANs when communicating with other 802.11g WLAN nodes, but can also use the same rates as the 802.11b WLAN when communicating with nodes using that older standard. In addition, 802.11g WLANs may support rates in the range of 22 Mbps using optional encoding methods such as PBCC.

Table A.1 **Supported data rates by WLAN standard**

802.11a	802.11b	802.11g
	1 Mbps	1 Mbps
	2 Mbps	2 Mbps
	5.5 Mbps	5.5 Mbps
6 Mbps		6 Mbps
9 Mbps		9 Mbps
	11 Mbps	11 Mbps
12 Mbps		12 Mbps
		22 Mbps
24 Mbps		24 Mbps

Table A.1 Supported data rates by WLAN standard (continued)

802.11a	802.11b	802.11g
36 Mbps		36 Mbps
48 Mbps		48 Mbps

The 802.11b WLAN standard uses DSSS in the 2.4 GHz band. Taking 2412 MHz as the center frequency of the first channel, the standard described 14 channels, 5 MHz apart, numbered 1 to 14. In the United States, the FCC allocated bandwidth to support the first 11 channels. Regulatory bodies in other jurisdictions made different allocations from within this same band.

The 802.11g WLAN standard uses the same spectrum and channels as 802.11b WLANs, but uses the OFDM encoding and transmission methods of the 802.11a WLAN standard when communicating with other 802.11g WLAN nodes.

The 802.11a WLAN standard uses OFDM in the 5.0 GHz band. The standard defines channels 1-199, starting at 5.005 GHz, with their center frequencies spaced 5 MHz apart. The FCC in the United States has allocated bandwidth in three parts of the spectrum, as shown in Table A.2. The ETSI and ERM in Europe, MKK in Japan, and other regulatory agencies in other jurisdictions have made their own allocations within this band.

Table A.2 FCC Channels for 802.11a WLANs

Band	Center frequency	Channel number	Maximum power
U-NII low band (5150 MHz to 5250 MHz)			
	5180 MHz	**36**	40 mW
	5200 MHz	**40**	40 mW
	5220 MHz	**44**	40 mW
	5240 MHz	**48**	40 mW

Table A.2 FCC Channels for 802.11a WLANs (continued)

Band	Center frequency	Channel number	Maximum power
U-NII medium band (5250 MHz to 5350 MHz)			
	5260 MHz	**52**	200 mW
	5280 MHz	**56**	200 mW
	5300 MHz	**60**	200 mW
	5320 MHz	**64**	200 mW
U-NII high band (for outdoor use) (5725 MHz to 5825 MHz)			
	5745 MHz	**149**	800 mW
	5765 MHz	**153**	800 mW
	5785 MHz	**157**	800 mW
	5805 MHz	**161**	800 mW

Notice that the channel numbers for 802.11a WLANs appear in a gapped sequence, with 20 MHz separating the center frequency of one allocated channel from the next. This is a recognition of the fact that the spectrum spreading approaches used in all 802.11 WLAN standards actually take up far more spectrum than 5 MHz. In fact an active channel fills more than 16 MHz.

Note: 802.11a WLAN cards based on the Atheros chip set may support a proprietary mode called Turbo Mode (specific card vendors may use other names). Turbo Mode doubles the standard data rates and uses twice the RF spectrum specified for a normal channel in the 802.11a WLAN standard. For more information, please visit the support pages of our website, at: http://www.wildpackets.com/support.

Collision avoidance and media access

One of the most significant differences between Ethernet and 802.11 WLANs is the way in which they control access to the medium, determining who may talk and when. Ethernet uses CSMA/CD (carrier sense multiple access with collision detection). This is possible because an Ethernet device can send and listen to the wire at the same time, detecting the pattern that shows a collision is taking place. When a radio attempts to transmit and listen on the same channel at the same time, its own transmission drowns out all other signals. Collision detection is impossible.

The carrier sense capability of Ethernet and WLANs is also different. On an Ethernet segment, all stations are within range of one another at all times, by definition. When the medium seems clear, it is clear. Only a simultaneous start of transmissions results in a collision. As shown in Figure A.6, nodes on a WLAN cannot always tell by listening alone whether or not the medium is in fact clear.

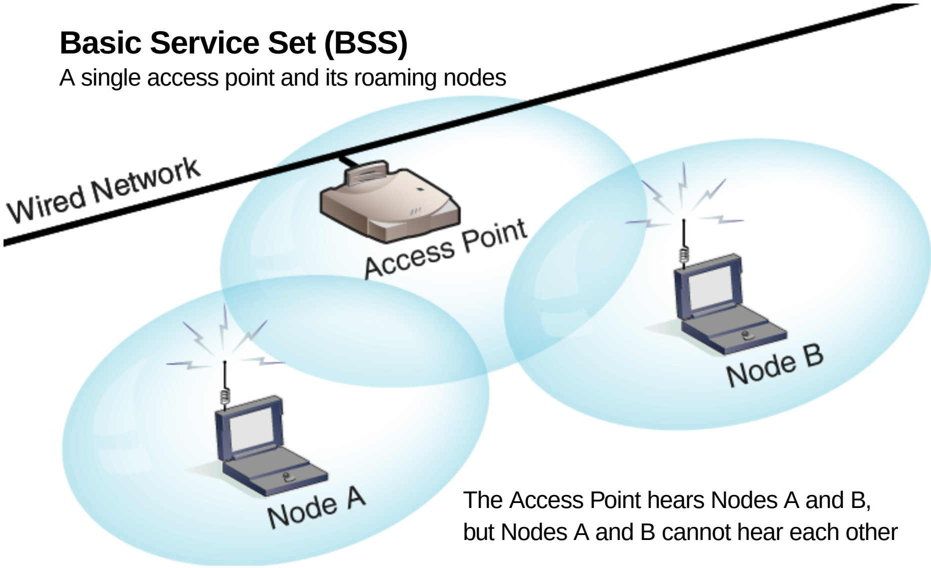

Basic Service Set (BSS)
A single access point and its roaming nodes
Wired Network
Access Point
Node B
Node A
The Access Point hears Nodes A and B,
but Nodes A and B cannot hear each other

Figure A.6 Basic Service Set (BSS), showing the hidden node problem.

In a wireless network, a device can be in range of two others, neither of which can hear the other, but both of which can hear the first device. The access point in Figure A.6 can hear both node A and node B, but neither A nor B can hear each other. This creates a situation in which the access point could be receiving a transmission from node B without node A sensing that node B is transmitting. Node A, sensing no activity on the channel, might then begin transmitting, jamming the access point's reception of node B's transmission already under way. This is known as the "hidden node" problem.

To solve the hidden node problem and overcome the impossibility of collision detection, 802.11 WLANs use CSMA/CA (carrier sense multiple access with collision avoidance). Under CSMA/CA, devices use a four-way handshake (Figure A.7) to gain access to the airwaves to ensure collision avoidance. To send a direct transmission to another node, the source node puts a short Request To Send (RTS) packet on the air, addressed to the intended destination. If that destination hears the transmission and is able to receive, it replies with a short Clear to Send (CTS) packet. The initiating node then sends the data, and the recipient acknowledges all transmitted packets by returning a short ACK (Acknowledgement) packet for every transmitted packet received.

The 802.11g WLAN standard uses this RTS/CTS method only when it detects nodes using 802.11b transmissions. Because the RTS/CTS in these mixed b/g networks must be sent in a form compatible with the older and slower 802.11b WLAN standards, this reduces the overall throughput of 802.11g WLANs, particularly near the top end of their performance, by something on the order or 20-50%.

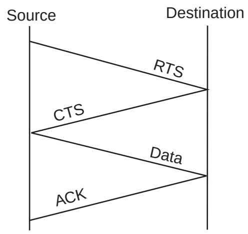


Figure A.7 A Four-Way Handshake ensures collision avoidance in 802.11 networks.

Timing is critical to mediating access to the airwaves in WLANs. To ensure synchronization, access points or their functional equivalents periodically send beacons and timing information.

Wireless LAN topologies

Wireless LANs behave slightly differently depending on their topology, or make-up of member nodes. The simplest arrangement is an *ad hoc* group of independent wireless nodes communicating on a peer-to-peer basis, as shown in Figure A.8. The standard refers to this topology as an Independent Basic Service Set (IBSS) and provides for some measure of coordination by electing one node from the group to act as the proxy for the missing access point or base station found in more complex topologies. Ad hoc networks allow for flexible and cost-effective arrangements in a variety of work environments, including hard-to-wire locations and temporary setups such as a group of laptops in a conference room.

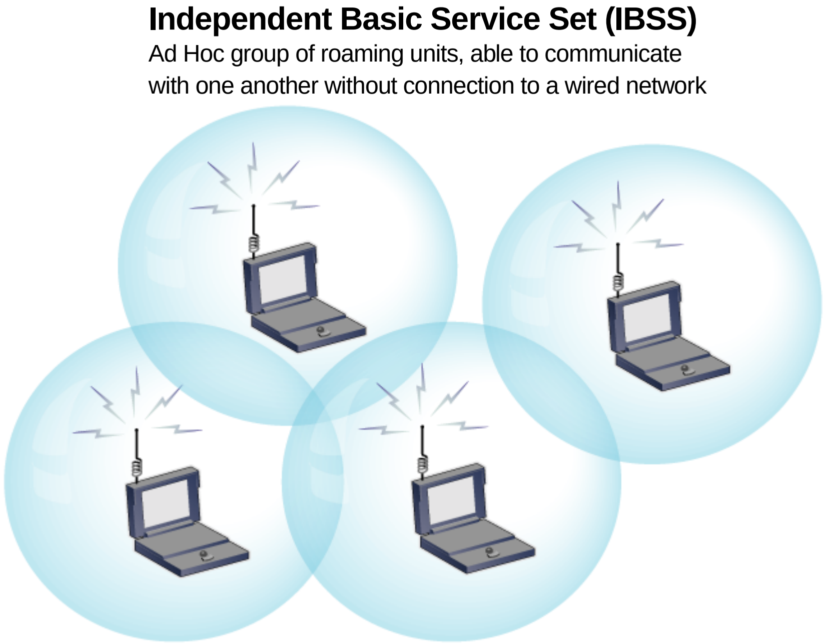

Independent Basic Service Set (IBSS)
Ad Hoc group of roaming units, able to communicate
with one another without connection to a wired network

Figure A.8 An IBSS or “Ad Hoc” Network.

The more complex topologies, referred to as *infrastructure* topologies, include at least one access point or base station. Access points provide synchronization and coordination, forwarding of broadcast packets and, perhaps most significantly, a bridge to the wired network.

The standard refers to a topology with a single access point as a Basic Service Set (BSS) as shown in Figure A.6. A single access point can manage and bridge wireless communications for all the devices within range and operating on the same channel.

To cover a larger area, multiple access points are deployed. This arrangement (shown in Figure A.9) is called an Extended Service Set (ESS). It is defined as two or more Basic Service Sets connecting to the same wired network. Each access point is assigned a different channel wherever possible to minimize interference. If a channel must be reused, it is best to assign the reused channel to the access points that are the least likely to interfere with one another.

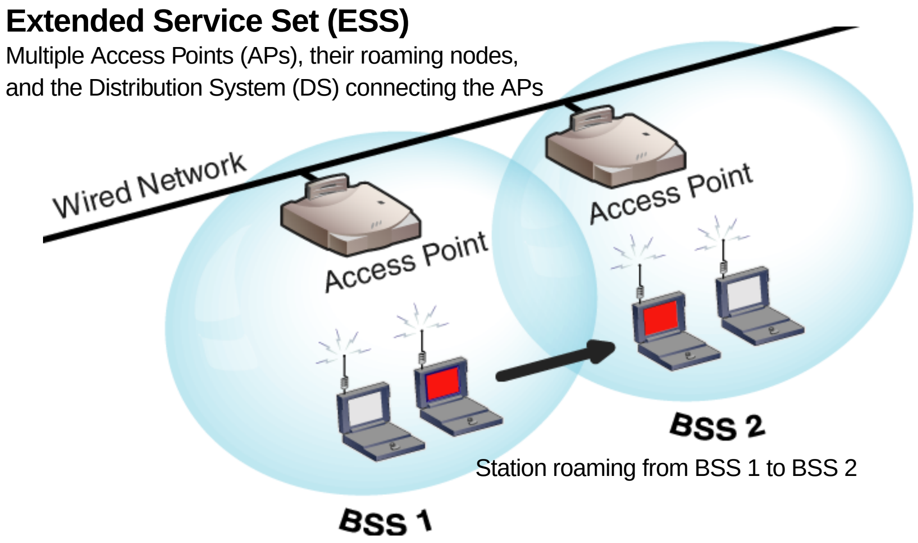

Extended Service Set (ESS)
Multiple Access Points (APs), their roaming nodes, and the Distribution System (DS) connecting the APs
Wired Network
Access Point
Access Point
BSS 2
Station roaming from BSS 1 to BSS 2
BSS 1

Figure A.9 Extended Service Set (ESS) supports roaming from one cell to another.

When users roam between cells or BSSs, their mobile device will find and attempt to connect with the access point with the clearest signal and the least amount of network traffic. This way, a roaming unit can transition seamlessly from one access point in the system to another, without losing network connectivity.

An ESS introduces the possibility of forwarding traffic from one radio cell (the range covered by a single access point) to another over the wired network. This combination of access points and the wired network connecting them is referred to as the Distribution System (DS). Messages sent from a wireless device in one BSS to a device in a different BSS by way of the wired network are said to be sent by way of the distribution system or DS.

Note: To meet the needs of mobile radio communications, 802.11 WLAN standards must be tolerant of connections being dropped and reestablished. The standards attempt to ensure minimum disruption to data delivery, and provide some features for caching and forwarding messages between BSSs. Particular implementations of some higher layer protocols such as TCP/IP may be less tolerant. For example, in a network where DHCP is used to assign IP addresses, a roaming node may lose its connection when it moves across cell boundaries and have to reestablish it when it enters the next BSS or cell. Software solutions are available to address this particular problem. In addition, IEEE may revise the standards in ways that mitigate this problem in future versions.

Whether they have one base station or many, most corporate WLANs will operate in infrastructure mode to access servers, printers, Internet connections and other resources already established on wired networks. Even users seeking an “all wireless” solution may find that an access point does a better job of mediating communications with an Internet connection, for example, and is worth the additional expense.

Authentication and privacy

Authentication restricts the ability to send and receive on the network. Privacy ensures that eavesdroppers cannot read network traffic.

Authentication can be open or based on knowledge of a shared token. In either case, authentication is the first step for a device attempting to connect to an 802.11 WLAN. The function is handled by an exchange of management packets. If authentication is open, then any standards-compliant device will be authenticated. If authentication is based on a shared token, then a device must prove it knows this shared token in order to be authenticated.

WEP (Wired Equivalent Privacy) is a data encryption technique supported as an option in the 802.11 WLAN protocols. The technique uses shared keys and a pseudo random number (PRN) as an initial vector (IV) to encrypt the data portion of network packets. The 802.11 WLAN network headers themselves are not encrypted.

The designers’ purpose in supporting this feature was to give a wireless network, with its inherent vulnerability to eavesdropping, a level of security similar to that enjoyed by a wired network operating without encryption. Eavesdropping on a wired network, they reasoned, requires a physical network tap or a suite of sophisticated radio listening devices. Eavesdropping on a radio network requires only a device capable of listening on the same channel or frequency. Since all 802.11 WLAN network adapters are capable of listening on any of the usable channels, eavesdropping is almost a certainty, given a large enough number of devices in circulation.

The original WEP specification called for 64 bit key length encryption. In part, this was an explicit effort to make commercial implementations of the protocol exportable from the U.S. in an era when only the very weakest encryption technologies were granted export licenses. The standard's support for such a weak encryption method also underlines the design function of encryption in this protocol. It is intended to stop casual eavesdropping, not to stop a concerted attack. Several vendors now support 64-bit, 128-bit, or larger key lengths. This significantly increases the barriers to attack, but even at 128-bit key lengths, WEP is still the door to an office, not a bank vault. Any of these levels of encryption serves the primary purpose of WEP quite well.

Because WEP encrypts all the data above the 802.11 WLAN layers, it can prevent AiroPeek from decoding higher level network protocols, and so prevent accurate troubleshooting of problems with TCP/IP, IPX, NetBEUI and so forth. To overcome this limitation, AiroPeek allows users to specify the WEP shared key set for their network. This allows AiroPeek to decode the network data contained in 802.11 WLAN packets in the same way that every other station on the user's network does.

Note: Although it is possible to implement WEP with open authentication, this is strongly discouraged as it leaves the door open for intruders to collect enough information to compromise the security of WEP.

Toward improved security

The authentication and encryption methods supported in the original 802.11 WLAN standards provide only a minimal level of security. IEEE is currently working on a new specification for authentication and privacy, 802.11i, which is expected to be finalized by the end of 2003. In the interim, the WiFi Alliance has published a set of guidelines for implementing enhanced security measures called WPA (WiFi Protected Access). The equipment vendor Cisco Systems also provides its own proprietary implementations of earlier drafts of the 802.11i standard in some of its products.

AiroPeek can decode the most commonly used forms of authentication from among these interim offerings. This allows you to identify the methods in use on your network. All of the new authentication methods are based on the Extensible Authentication Protocol (EAP). The methods decoded by AiroPeek are: EAPTLS (EAP using Transport Level Security), PEAP (Protected EAP), and Cisco's LEAP (Lightweight EAP). Note that while AiroPeek can decode these protocols, some implementations encrypt the authentication traffic in such a way as to make the packets unreadable by any outside observer, including AiroPeek.

The primary weakness of the original implementation of WEP was the small number of keys and their frequent reuse. Even larger key lengths cannot defend against attacks aimed at this weakness. To overcome this weakness, early drafts of 802.11i called for better key management. The WiFi Alliance offered an interim solution adopting TKIP (Temporal Key Integrity Protocol). Cisco deployed its proprietary CKIP (Cisco Key Integrity Protocol) in some of its products. AiroPeek can identify the method in use for either type of system. Both TKIP and CKIP improve the security of encryption methods by dramatically reducing the reuse of keys. Keys are generated dynamically and replaced very frequently. This eliminates the primary weakness of the original WEP implementations with their user-entered keys and infrequent re-keying.

Packet structure and packet types

Like the rest of the 802 family of LAN protocols, 802.11 WLAN sends all network traffic in packets. There are three basic types: data packets, network management packets and control packets. The first section describes the basic structure of 802.11 WLAN data packets and the information they provide for network analysis. The second section describes the management and control packets, their functions and the role they play in network analysis.

Packet structure

All the functionality of the protocol is reflected in the packet headers. RF technology and station mobility impose some complex requirements on 802.11 WLAN networks. This added complexity is reflected in the long physical layer convergence protocol (PLCP) headers as well as the data-rich MAC header.

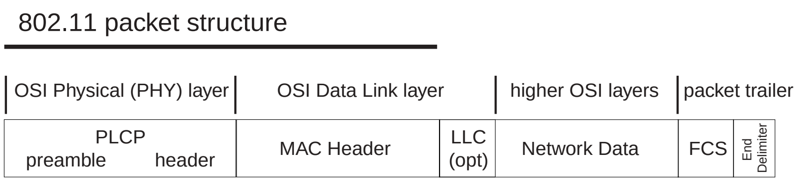
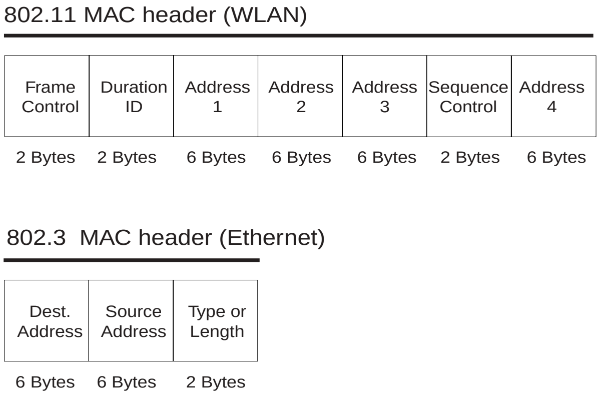


Figure A.10 802.11 WLAN data packet structure

Because 802.11 WLANs must be able to form and re-form their membership constantly, and because radio transmission conditions themselves can change, coordination becomes a large issue in WLANs. Management and control packets are dedicated to these coordination functions. In addition, the headers of ordinary data packets contain a great deal more information about network conditions and topology than, for example, the headers of Ethernet data packets would contain.



802.11 MAC header (WLAN)

Frame Control	Duration ID	Address 1	Address 2	Address 3	Sequence Control	Address 4
2 Bytes	2 Bytes	6 Bytes	6 Bytes	6 Bytes	2 Bytes	6 Bytes

802.3 MAC header (Ethernet)

Dest. Address	Source Address	Type or Length
6 Bytes	6 Bytes	2 Bytes

Figure A.11 Comparison of MAC headers: 802.11 WLAN to 802.3 Ethernet

A complete breakout of all the fields in the packet headers and the values they may take is found in the next section. For this overview, Table A.3 below presents a list of the types of information 802.11 WLAN data packet headers convey. The table also shows the types of information carried in management and control packets.

Table A.3 Protocol functions in 802.11 WLANs

Authentication / Privacy	
The first step for a device in joining a BSS or IBSS is authentication. This can be an open or a shared key system. If WEP encryption of packet data is enabled, shared key authentication should be used. Authentication is handled by a request/response exchange of management packets.	
authentication ID	This is the name under which the current station authenticated itself on joining the network.
WEP enabled	If this field is true, then the payload of the packet (but not the WLAN headers) will be encrypted using Wired Equivalent Privacy.
Network membership / Topology	

Table A.3 **Protocol functions in 802.11 WLANs (continued)**

The second step for a device joining a BSS or IBSS is to associate itself with the group, or with the access point. When roaming, a unit also needs to disassociate and reassociate. These functions are handled by an exchange of management packets. The current status is shown in packet headers.	
association	Packets can show the current association of the sender. Association and Reassociation are handled by request/ response management packets. Disassociation is a simple declaration from either an access point or a device.
IBSSID or ESSID	The ID of the group or its access point. A device can only be associated with one access point (shown by the ESSID) or IBSS at a time.
probe	Probes are supported by request/response management packets used by roaming devices in search of a particular BSS or access point. They support a roaming unit's ability to move between cells while remaining connected.
Network conditions / Transmission	
The 802.11 WLAN protocol supports rapid adjustment to changing conditions, always seeking the best throughput.	
channel	The channel or radio frequency used for the transmission
data rate	The data rate used to transmit the packet. 802.11 WLAN nodes can rapidly adjust their transmission data rate to match conditions.
fragmentation	802.11 WLANs impose their own fragmentation on packets, completely independent of any fragmentation imposed by higher level protocols such as TCP/IP. A series of short transmissions is less vulnerable to interference in noisy environments. This fragmentation is dynamically set by the protocol in an effort to reduce the number, or at least the cost, of retransmissions.
synchronization	Several kinds of synchronization are important in WLANs. Network management packets called "beacon" packets keep members of a BSS synchronized. In addition, devices report the state of their own internal synchronization. Finally, all transmissions contain a timestamp.

Table A.3 **Protocol functions in 802.11 WLANs (continued)**

power save	Laptops in particular need to conserve power. To facilitate this, the protocol uses a number of fields in data packets plus the PS-Poll (power save-poll) control packet to let devices remain connected to the network while in power save mode.
Transmission control	
While the protocol as a whole actually controls the transmission of data, certain header fields and control packets have this as their particular job:	
RTS, CTS, ACK	Request to send, clear to send, and acknowledgement, respectively, these control packets are used in the four way handshake in support of collision avoidance.
version	The version of the 802.11 protocol used in constructing the packet.
type and sub-type	The type of packet (data, management, or control), with a sub-type specifying its exact function.
duration	In support of synchronization and orderly access to the airwaves, packets contain a precise value for the time that should be allotted for the remainder of the transaction of which this packet is a part.
length	Packet length
retransmission	Retransmissions are common. It is important to declare which packets are retransmissions.
sequence	Sequence information in packets helps reduce retransmissions and other potential errors.
order	Some data, such as voice communications, must be handled in strict order at the receiving end.

Table A.3 **Protocol functions in 802.11 WLANs (continued)**

Routing	
Again, many fields are related to routing traffic, but the following are most directly related:	
addresses	There are four address fields in 802.11 WLAN data packets, instead of the two found in Ethernet or IP headers. This is to accommodate the possibility of forwarding to, from, or through the distribution system (DS). In addition to the normal Destination and Source addresses, these fields may show the Transmitter, the Receiver, or the BSSID. The type of address shown in each address field depends on whether (and how) the packet is routed by way of the DS. Control and management packets need only three address fields because they can never be routed both to and from (that is, through) the DS.
to/from DS	In an ESS, traffic can be routed from a device using one access point to a device using a different access point somewhere along the wired network. These fields describe routing through the distribution system (DS) and tell the receiving device how to interpret the address fields.
more data	Access points can cache data for other devices. This serves both roaming across BSS or cell boundaries and the power save features. When a device receives a message from an access point, it may be told the access point has more data waiting for it as well.

Management and control packets

Control packets are short transmissions which directly mediate or control communications. Control packets include the RTS, CTS and ACK packets used in the four way handshake (see Figure A.7), as well as power save polling packets and short packets to show (or show and acknowledge) the end of contention-free periods within a particular BSS or IBSS.

Management packets are used to support authentication, association, and synchronization. Their formats are similar to those of data packets, but with fewer fields in the MAC header. In addition, management packets may have data fields of fixed or variable length, as defined by their particular sub-type. The types of information included in management and control packets are shown in Table A.3, along with the related information found in data packet headers.

For a complete list of control and management packets and their functions, please see Appendix C, “802.11 WLAN Packet Types” on page A-41.

802.11 WLAN frames and packet headers

This section describes the various layers of 802.11 WLAN packet headers and the clues they contain to the protocols found in the network data which they frame. The typical 802.11 packet frames the network data inside a physical layer header, followed by a MAC layer header with a FCS trailer for error control. All versions of 802.11 support use of the 802.2 standard for Logical Link Control or LLC.

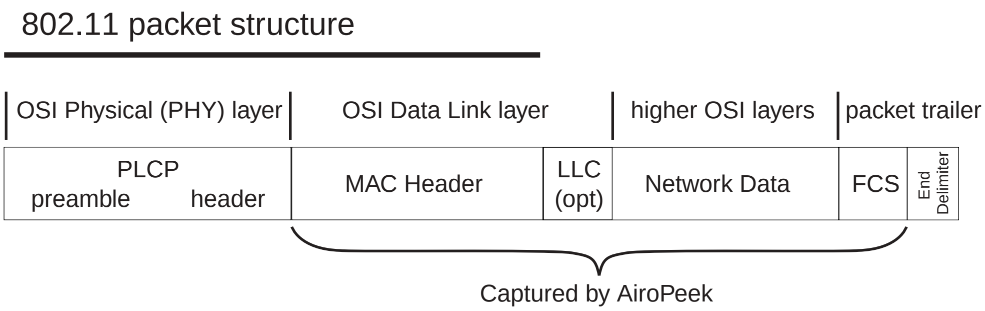


Figure A.12 802.11 packet structure

As Figure A.12 above shows, the hardware preamble, packet start delimiter and end delimiter bytes are not captured by AiroPeek. The PLCP header is used by network hardware to control the transmission and maintain the physical (in this case, radio wave) link between stations. Higher layers in the packet, beginning with the MAC header, are captured by AiroPeek and presented both as raw data and as decoded data.

PLCP

802.11 WLAN protocols permit negotiation of transmission rates for each session. They also permit changes in packet fragmentation to improve overall throughput under changing conditions. To support these functions, they use a physical layer header called the PLCP (Physical Layer Convergence Protocol), consisting of a PLCP preamble and the PLCP header.

The physical layers of the 802.11a WLAN and the 802.11b WLAN are different, and so the PLCP is distinct for each. Even so, they have important similarities. In both standards, the PLCP header is transmitted immediately after an initial synchronization or training sequence, and immediately before the MAC header. In both standards, the PLCP header contains information on the rate and length of the rest of the packet.

Whether the packet length is expressed in bytes or as a unit of time, receiving stations can use the PLCP header to determine how much time should be allowed for transmission of this packet. Even if a receiver does not support the data rate requested in the packet, it knows how long to wait before the channel will again be clear. PLCP header also contains error correction and information on the encoding scheme (related to data rate) used in the remainder of the packet.

The PLCP portion of the transmission is always sent at the lowest commonly supported data rate, to insure maximum reliability and compatibility with other stations.

802.11 MAC header

The particular format of the 802.11 MAC header depends on the type of packet: data packets, network management packets or control packets. The description which follows (based on Figure A.13) is for an 802.11 WLAN data packet. Management and control packets have only the first three of the four address fields. They may also contain information in the frame body in fields of fixed or variable length which are specific to that particular type and subtype of packet.

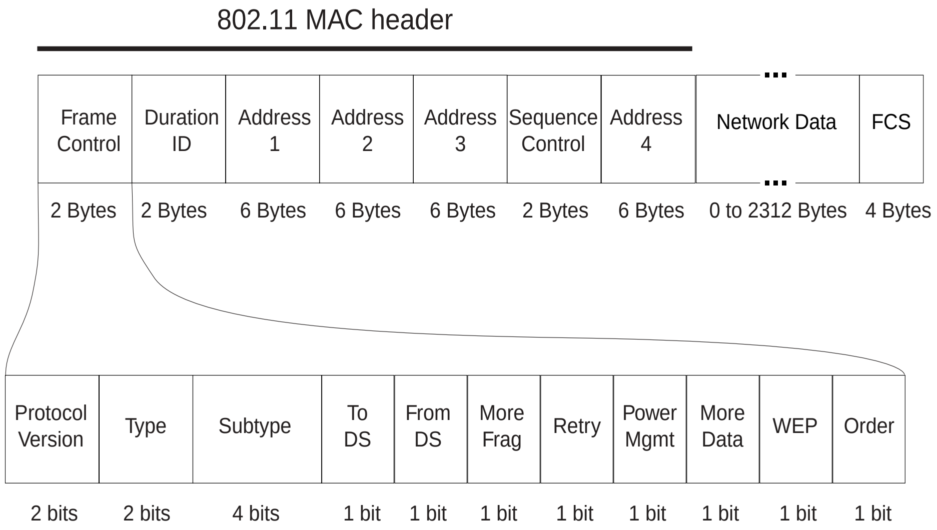


Figure A.13 802.11 MAC header

The Frame Control field is 2 bytes long. Its contents are broken out in detail at the bottom of Figure A.13 and are described below. The Duration ID field is 2 bytes long and contains the duration value for each of the fields. For control packets this field also carries the association identity (AID) of the transmitting station. There are four address fields rather than the expected two (as in Ethernet or IP) to accommodate the possibility of message relay. Which address appears in what field depends on whether the packet is being forwarded through the Distribution System (DS). The values of the To DS and From DS bits in the Frame Control field determine the content of the address fields, as shown in Table A.4. The Sequence Control field is 2 bytes and is used to filter out duplicate messages, such as a message sent again because an earlier one was not acknowledged.

Table A.4 **Address Fields in 802.11 MAC header**

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	Destination	Source	BSSID	N/A
0	1	Destination	BSSID	Source	N/A
1	0	BSSID	Source	Destination	N/A
1	1	Receiver	Transmitter	Destination	Source

The bit-wise breakdown of the Frame Control field is as follows: The first two bits are the Protocol Version and tell which version of 802.11 is to follow. The Type field (2 bits) and the Sub Type field (4 bits) work together to describe the type of frame and its function. The To DS and From DS fields are one bit each and are set to 1 for true and 0 for false, indicating whether the packet was sent to or from the Distribution System. For messages within a single BSS (Basic Service Set), both of these fields would be set to 0. The More Fragments bit would be set to 1 if there were more fragments of the current packet.

Note: The fragmentation noted in the MAC header is that imposed by the 802.11 node to accommodate changing transmission conditions. Large packets are more susceptible to corruption by radio interference than smaller ones, so a node may increase fragmentation to reduce retransmissions in conditions of heavy interference.

The Retry bit is set to 1 if the current packet is a retransmission of a previous attempt. The Power Management bit is set to 1 if the node will enter power save mode after the current transmission or 0 if the node will be active. The More Data bit is set to 1 if packets have been buffered and are waiting to be delivered to the destination node. The WEP (Wired Equivalent Privacy) bit is set to 1 if the content (payload) of the packet has been encrypted using the WEP algorithm. The Order bit is set to 1 if the packets must be strictly ordered, as with voice over IP, for example.

Note: The MAC (Media Access Control) address is the physical address of a particular Network Interface Card (NIC) or other physical layer network device. For more information on addressing, please see Appendix B, “Addresses and Names” on page A-33.

802.2 headers

Like all LAN protocols in the IEEE 802 family, 802.11 permits the use of the 802.2 protocol for Logical Link Control (LLC). The 802.2 header, usually called the LLC, contains information about the protocol type of the packet. These 802.2 headers are either 3 bytes or 8 bytes long. The first section of the LLC header is 3 bytes long and contains two LSAP values and one LSAP command. These LSAP values can either contain information about the protocol of the packet, or they can point to the optional 5 byte SNAP section that follows. If they point to the SNAP section of the header then the protocol is described by this 5 byte Protocol Discriminator or SNAP ID.

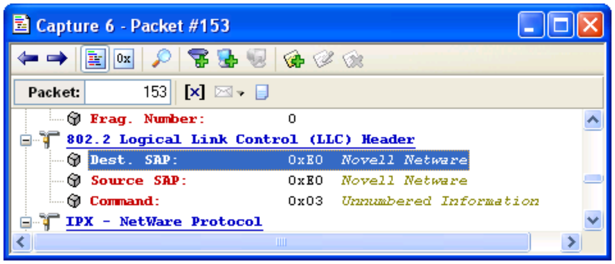
The LSAP Values and the SNAP IDs are described in the next two sections.

802.2 LSAP values

In AiroPeek, the 1-byte protocol type specifications found in the first 3 byte section of the 802.2 LLC header are referred to as 802.2 LSAP values.

The first three bytes of an 802.2 LLC header are as follows:

- The first byte is the Destination Service Access Point (DSAP), which designates a destination protocol.
- The second byte is the Source Service Access Point (SSAP), which designates a source protocol, most often set to the same value as the DSAP.
- The third byte is a control byte that indicates the data format in the packet. This byte is ignored by most protocols (except SNA).



Packet: 153

```
Frag. Number:                      0
802.2 Logical Link Control (LLC) Header
  Dest. SAP:                       0xE0  Novell Netware
  Source SAP:                      0xE0  Novell Netware
  Command:                         0x03  Unnumbered Information
IPX - NetWare Protocol
```

Figure A.14 802.2 LSAP values in the 802.2 LLC Header

The DSAP and SSAP fields are referred to *collectively* as the LSAP (Link layer Service Access Point).

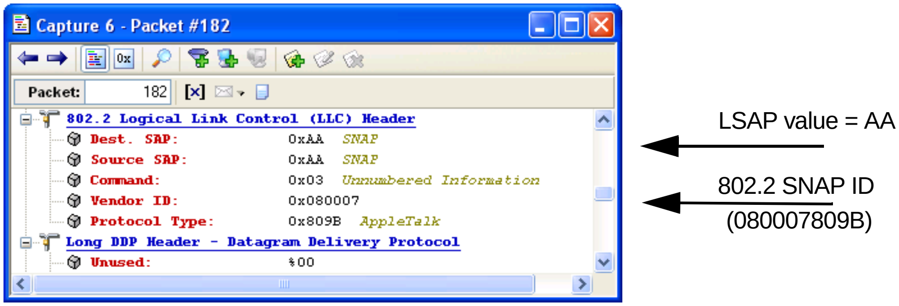
Note: The 1-byte hexadecimal number in these fields can be used to identify the specific 802.2 LSAP protocol in a filter. For example, XNS uses this LSAP value: 0x80.

802.2 SNAP IDs

When both the DSAP and SSAP are set to 0xAA, the type is interpreted as a protocol not defined by IEEE and the LSAP is referred to as SubNetwork Access Protocol (SNAP).

In SNAP, the 5 bytes that follow the DSAP, SSAP, and control byte are called the *Protocol Discriminator.*

In AiroPeek, protocol type specifications found in this optional 5-byte SNAP section of the 802.2 header are referred to as 802.2 SNAP IDs. The following figure shows an example of an 802.2 header with a SNAP ID.



```
802.2 Logical Link Control (LLC) Header
    Dest. SAP:              0xAA  SNAP
    Source SAP:             0xAA  SNAP
    Command:                0x03  Unnumbered Information
    Vendor ID:              0x080007
    Protocol Type:          0x809B  AppleTalk
Long DDP Header - Datagram Delivery Protocol
    Unused:                 %00
```

LSAP value = AA

802.2 SNAP ID
(080007809B)

Figure A.15 802.2 Header with SNAP ID

Error packets

AiroPeek recognizes only one error type, CRC, shown in the table below:

Table A.5 **Error Types**

Error Type	Description
CRC Error	At the end of the packet, four bytes are transmitted which force the checksum to a known constant. If the receiving end does not compute the same constant after receiving the four bytes, the packet must have been corrupted. A *CRC error* occurs when the CRC (Cyclic-Redundancy Check) fails. These bytes are referred to as a *Frame Check Sequence* or FCS.

The data in an error packet, including the source and destination physical addresses, should be viewed with caution since it may have little correspondence to what was originally transmitted. Packets flagged as errors are processed by **Network**, **Summary**, **Size**, and **History** statistics. In **Network Statistics**, error packets contribute only to overall packet and byte counts, not to broadcast or multicast counts. **Node**, **Protocol**, and **Conversation** statistics do not process error packets, nor do the standard Analysis Modules that ship with AiroPeek.

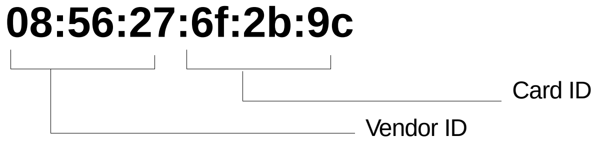
Addresses and Names

The basic concept of 802.11 WLAN networking, like that of Ethernet, is that packets are given destination addresses by senders, and those addresses are read and recognized by the appropriate receivers. Devices on the network check every packet, but fully process only those packets addressed either to themselves or to some group to which the device belongs.

AiroPeek recognizes three typologies of addresses: physical addresses, logical addresses, and symbolic names assigned to either of these.

Physical addresses

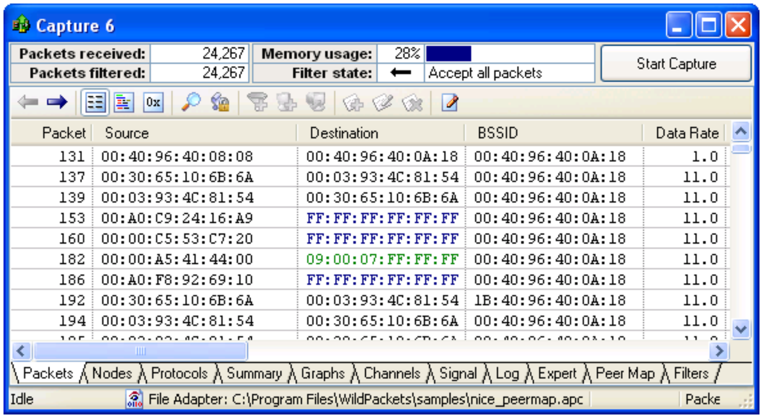
A physical address is the hardware-level address used by the 802.11 WLAN interface to communicate on the network. Every device must have a unique physical address. This is often referred to as its MAC (Media Access Control) address. An 802.11 WLAN physical address is six bytes long and consists of six hexadecimal numbers, usually separated by colon characters (:). For example:



Typically, a hardware manufacturer obtains a block of physical address numbers from the IEEE and assigns a unique physical address to each card it builds. The vendor block of addresses is designated by the first three bytes of the six byte physical 802.11 WLAN address. In this way, 802.11 WLAN physical addresses are generally distinct from each other, although some networks and protocols will override this built-in mechanism with one of their own.

Note: A list of vendor IDs is installed by default in the Names directory within the AiroPeek directory. This file is in a format that is ready to import into the AiroPeek Name Table. Please see “Importing vendor and protocol IDs” on page 139.

Figure B.1 shows captured packets that use physical addresses to represent the source and destination:



Packets received: 24,267
Packets filtered: 24,267
Memory usage: 28%
Filter state: ← Accept all packets

Packet	Source	Destination	BSSID	Data Rate
131	00:40:96:40:08:08	00:40:96:40:0A:18	00:40:96:40:0A:18	1.0
137	00:30:65:10:6B:6A	00:03:93:4C:81:54	00:40:96:40:0A:18	11.0
139	00:03:93:4C:81:54	00:30:65:10:6B:6A	00:40:96:40:0A:18	11.0
153	00:A0:C9:24:16:A9	FF:FF:FF:FF:FF:FF	00:40:96:40:0A:18	11.0
160	00:00:C5:53:C7:20	FF:FF:FF:FF:FF:FF	00:40:96:40:0A:18	11.0
182	00:00:A5:41:44:00	09:00:07:FF:FF:FF	00:40:96:40:0A:18	11.0
186	00:A0:F8:92:69:10	FF:FF:FF:FF:FF:FF	00:40:96:40:0A:18	11.0
192	00:30:65:10:6B:6A	00:03:93:4C:81:54	1B:40:96:40:0A:18	11.0
194	00:03:93:4C:81:54	00:30:65:10:6B:6A	00:40:96:40:0A:18	11.0

Idle
File Adapter: C:\Program Files\WildPackets\samples\nice_peermap.apc

Figure B.1 Physical addresses displayed in a Capture window

Logical addresses

A logical address is a network-layer address that is interpreted by a protocol handler. Logical addresses are used by networking software to allow packets to be independent of the physical connection of the network, that is, to work with different network topologies and types of media. Each type of protocol has a different kind of logical address, for example:

- an IP address consists of four decimal numbers separated by period (.) characters, for example:

  130.57.64.11

- an AppleTalk address consists of two decimal numbers separated by a period (.), for example:

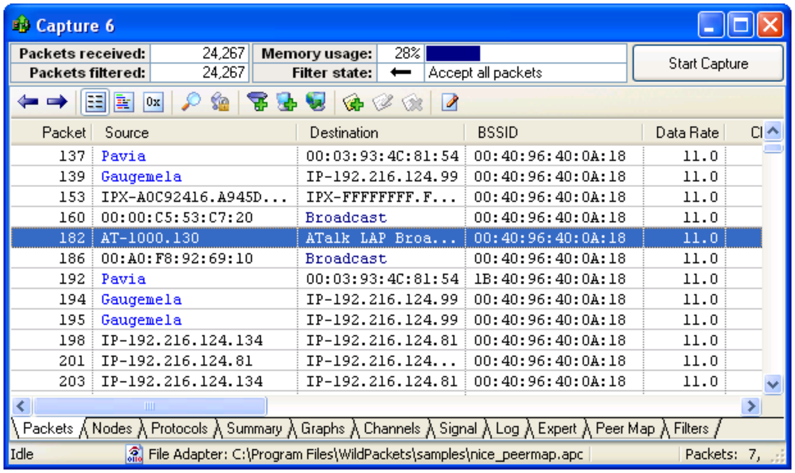
  2010.42

  368.12

Depending on the type of protocol in a packet (such as IP or AppleTalk), a packet may also specify source and destination logical address information, either as extensions to the physical addresses or as alternatives to them.

For example, in sending a packet to a different network, the higher-level, logical destination address might be for the computer on that network to which you are sending the packet, while the lower-level, physical address might be the physical address of an inter-network device, like a router, that bridges the two networks and is responsible for forwarding the packet to the ultimate destination.

The following figure shows captured packets identified by logical addresses under two protocols: AppleTalk (two decimal numbers, separated by a period) and IP (four decimal numbers from 0 to 255 separated by a period). It also shows symbolic names substituted for an IP address (*Gaugemela*) and an AppleTalk address (*Pavia*).


Capture 6
Start Capture
Packets ∖ Nodes ∖ Protocols ∖ Summary ∖ Graphs ∖ Channels ∖ Signal ∖ Log ∖ Expert ∖ Peer Map ∖ Filters

Packets received: 24,267
Packets filtered: 24,267
Memory usage: 28%
Filter state: Accept all packets

Packet	Source	Destination	BSSID	Data Rate	Cl
137	Pavia	00:03:93:4C:81:54	00:40:96:40:0A:18	11.0	
139	Gaugemela	IP-192.216.124.99	00:40:96:40:0A:18	11.0	
153	IPX-A0C92416.A945D...	IPX-FFFFFFFF.F...	00:40:96:40:0A:18	11.0	
160	00:00:C5:53:C7:20	Broadcast	00:40:96:40:0A:18	11.0	
182	AT-1000.130	ATalk LAP Broa...	00:40:96:40:0A:18	11.0	
186	00:A0:F8:92:69:10	Broadcast	00:40:96:40:0A:18	11.0	
192	Pavia	00:03:93:4C:81:54	1B:40:96:40:0A:18	11.0	
194	Gaugemela	IP-192.216.124.99	00:40:96:40:0A:18	11.0	
195	Gaugemela	IP-192.216.124.99	00:40:96:40:0A:18	11.0	
198	IP-192.216.124.134	IP-192.216.124.81	00:40:96:40:0A:18	11.0	
201	IP-192.216.124.81	IP-192.216.124...	00:40:96:40:0A:18	11.0	
203	IP-192.216.124.134	IP-192.216.124.81	00:40:96:40:0A:18	11.0	

Idle File Adapter: C:\Program Files\WildPackets\samples\nice_peermap.apc Packets: 7,

Figure B.2 Logical AppleTalk and IP addresses and symbolic names

Symbolic names

The strings of numbers typically used to designate physical and logical addresses are perfect for machines, but awkward for human beings to remember and use. Symbolic names stand in for either physical or logical addresses. The domain names of the Internet are an example of symbolic names. The relationship between the symbolic names and the logical addresses to which they refer is handled by DNS (Domain Name Services) in IP (Internet Protocol). AiroPeek takes advantage of these services to allow you to resolve IP names and addresses either passively in the background or actively for any highlighted packets.

In addition, AiroPeek allows you to identify devices by symbolic names of your own by creating a Name Table that associates the names you wish to use with their corresponding addresses.

To use symbolic names that are unique to your site, you must first create Name Table entries in AiroPeek and then instruct AiroPeek to use names instead of addresses when names are available.

To learn more about correlating names and addresses, see “Name table” on page 130.

Other classes of addresses

When one says “address,” one typically thinks of a particular workstation or device on the network, but there are other types of addresses equally important in networking. To send information to everyone, you need a *broadcast* address. To send it to some but not all, a *multicast* address is useful. If machines are to converse with more than one partner at a time, the protocol needs to define some way of distinguishing among services or among specific conversations. *Ports* and *Sockets* are used for these functions. Each of these is discussed in more detail below.

Broadcast and multicast addresses

It is often useful to send the same information to more than one device, or even to all devices on a network or group of networks. To facilitate this, the hardware and the protocol stacks designed to run on 802.x networks can tell devices to listen, not only for packets addressed to that particular device, but also for packets whose destination is a reserved broadcast or multicast address.

Broadcast packets are processed by every device on the originating network segment and on any other network segment to which the packet can be forwarded. Because broadcast packets work in this way, most routers are set up to refuse to forward broadcast packets. Without that provision, networks could easily be flooded by careless broadcasting.

An alternative to broadcasting is multicasting. Each protocol or network standard reserves certain addresses as multicast addresses. Devices may then choose to listen in for traffic addressed to one or more of these multicast addresses. They capture and process only the packets addressed to the particular multicast address(es) for which they are listening. This permits the creation of elective groups of devices, even across network boundaries, without adding anything to the packet processing load of machines not interested in the multicasts. Internet routers, for example, use multicast addresses to exchange routing information.

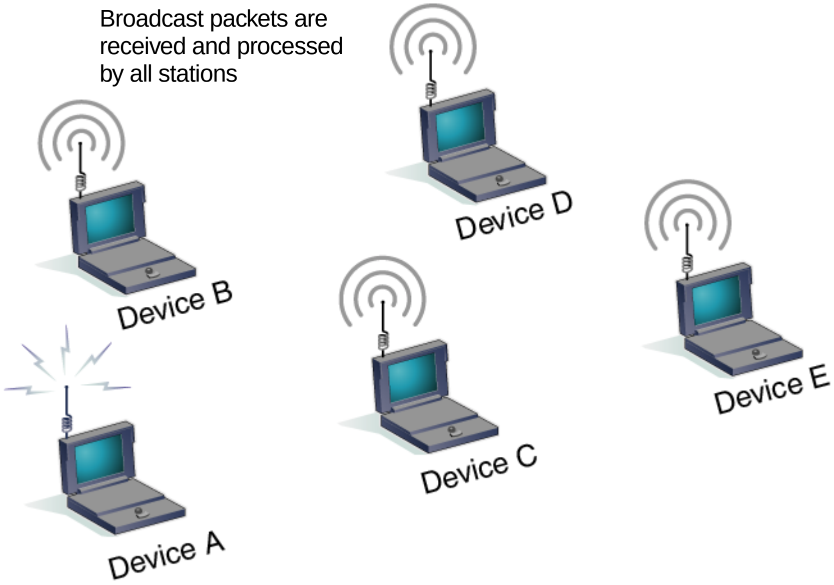

Broadcast packets are received and processed by all stations
Device B
Device D
Device E
Device C
Device A

Figure B.3 Broadcast packets are processed by all nodes on the network

Hardware Broadcast Address The following destination physical address is the 802.11 WLAN Broadcast address:
`FF:FF:FF:FF:FF:FF`

A packet with this destination address will be accepted by all devices on the network.

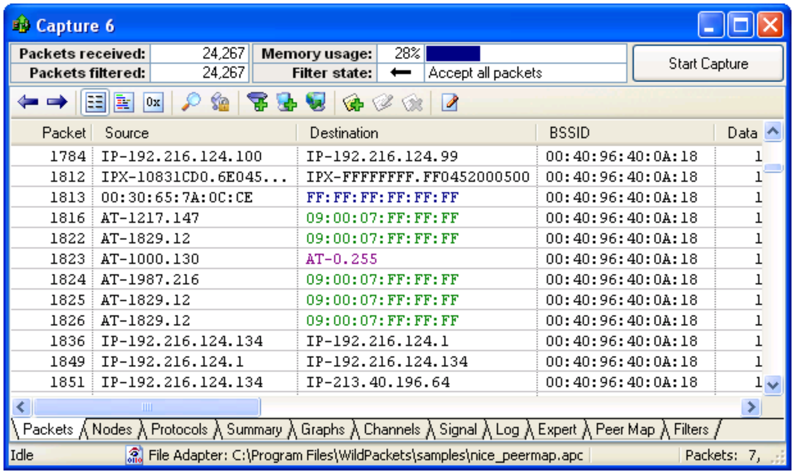
Some protocol types have logical Broadcast addresses. When an address space is subnetted, the last (highest number) address is typically reserved for broadcasts. For example:

IP Broadcast Addresses typically uses 255 as the host portion of the address; for example:
`130.57.255.255`

AppleTalk Broadcast Addresses use 255 as the node portion of the address:
`200.255`

While conceptually very powerful, broadcast packets can be very expensive in terms of network resources. Every single node on the network must spend the time and memory to receive and process a broadcast packet, even if the packet has no meaning or value for that node.

Multicast Address In 802.11 WLANs, as in Ethernet, odd-numbered addresses are reserved for multicasting. In IP, all of the Class D addresses have been reserved for multicasting purposes. That is, all the addresses between 224.0.0.0 and 239.255.255.255 are associated with some form of multicasting. Multicasting under AppleTalk is handled by an AppleTalk router which associates hardware multicast addresses with addresses in an AppleTalk *Zone*.



Packets received: 24,267
Packets filtered: 24,267
Memory usage: 28%
Filter state: ← Accept all packets

Packet	Source	Destination	BSSID	Data
1784	IP-192.216.124.100	IP-192.216.124.99	00:40:96:40:0A:18	1
1812	IPX-10831CD0.6E045...	IPX-FFFFFFFF.FF0452000500	00:40:96:40:0A:18	1
1813	00:30:65:7A:0C:CE	FF:FF:FF:FF:FF:FF	00:40:96:40:0A:18	1
1816	AT-1217.147	09:00:07:FF:FF:FF	00:40:96:40:0A:18	1
1822	AT-1829.12	09:00:07:FF:FF:FF	00:40:96:40:0A:18	1
1823	AT-1000.130	AT-0.255	00:40:96:40:0A:18	1
1824	AT-1987.216	09:00:07:FF:FF:FF	00:40:96:40:0A:18	1
1825	AT-1829.12	09:00:07:FF:FF:FF	00:40:96:40:0A:18	1
1826	AT-1829.12	09:00:07:FF:FF:FF	00:40:96:40:0A:18	1
1836	IP-192.216.124.134	IP-192.216.124.1	00:40:96:40:0A:18	1
1849	IP-192.216.124.1	IP-192.216.124.134	00:40:96:40:0A:18	1
1851	IP-192.216.124.134	IP-213.40.196.64	00:40:96:40:0A:18	1

Idle | File Adapter: C:\Program Files\WildPackets\samples\nice_peermap.apc | Packets: 7,

Figure B.4 AppleTalk broadcast and multicast packets

Ports and sockets

Network servers, and even workstations, need to be able to provide a variety of services to clients and peers on the network. To help manage these various functions, protocol designers created the idea of logical *ports* to which requests for particular services could be addressed.

Ports and *sockets* have slightly different meanings in some protocols. What is called a port in TCP/UDP is essentially the same as what is called a socket in IPX, for example.

AiroPeek treats the two as equivalent. ProtoSpecs uses port assignments and socket information to deduce the type of traffic contained in packets.

Station IDs in 802.11 WLANs

The roaming features of WLANs create extra demands for coordination and on-the-fly reconfiguration of network topologies. To accommodate this, the 802.11 WLAN standard refers to key pieces of the network by their station ID, based on the function that station is performing in the network. All of the addresses used in the 802.11 WLAN standard are the same hexadecimal format as typical MAC addresses (shown at the beginning of this appendix). The BSSID is typically the physical address of the access point providing coordination to a BSS. In an IBSS, the BSSID is derived from the MAC address of the station providing coordination. In AiroPeek, the ESSID is a 0 to 32 byte string identifying the ESS or extended service set, comprising multiple BSSs.

802.11 WLAN Packet Types

The table below lists the various packet types and subtypes specified in the 802.11 WLAN standard, and describes their usage briefly.

Table C.1 **WLAN packet types**

Packet Types				Usage
type		**subtype**		
00	mgmt	0000	Association Request	This packet is sent to an access point (in a BSS or ESS) or to any other peer (in an IBSS or ad hoc network). The sender must already be authenticated in order to gain a successful association.
00	mgmt	0001	Association Response	This packet is sent from an access point (in a BSS or ESS) or from any other peer (in an IBSS or ad hoc network) in response to an association request packet. If the request is successful, the response will include the Association ID of the requester.
00	mgmt	0010	Reassociation Request	Like an association request, but it includes information about the current association at the same time as it requests a new association (either with the original Station after some lapse of time, or with a new station upon moving from one BSS to another). This packet is sent to an access point (in a BSS or ESS) or to any other peer (in an IBSS or ad hoc network). The sender must already be authenticated in order to gain a successful association.
00	mgmt	0011	Reassociation Response	Like an association response, but in response to a reassociation request. This packet is sent from an access point (in a BSS or ESS) or from any other peer (in an IBSS or ad hoc network) in response to a reassociation request packet. If the request is successful, the response will include the Association ID of the requester.

Table C.1 **WLAN packet types**

Packet Types				Usage
type		subtype		
00	mgmt	0100	Probe Request	Probe request is used to actively seek any, or a particular, access point or BSS.
00	mgmt	0101	Probe Response	Probe response replies with station parameters and supported data rates.
00	mgmt	1000	Beacon	Beacon packets are sent by the access point in a BSS (or its equivalent in an IBSS) to announce the beginning of a Contention Free period (CF), during which the right to transmit is conferred by the access point by polling. Beacon management packets carry BSS timestamps to help synchronize member stations with the BSS, and other information to help them locate and choose the BSS with the best signal and availability.
00	mgmt	1001	ATIM	Announcement Traffic Indication Message. This packet serves much the same function in an IBSS that the Beacon packet does in an infrastructure (BSS or ESS) topology. The packet sets the synchronization of the group and announces that messages are waiting to be delivered. Stations in Power Save mode wake up periodically to listen for ATIM packets in ad hoc (IBSS) networks, just as they do for Beacon packets in infrastructure (BSS or ESS) networks.
00	mgmt	1010	Disassociation	This packet is an announcement breaking an existing association. It is a one-way communication (meaning it does not require or accept a reply), and must be accepted. It can be sent by any associated station or BSS and it takes effect immediately.
00	mgmt	1011	Authentication	Authentication packets are sent back and forth between the station requesting authentication and the station to which it is attempting to assert its authentic identity. The number of packets exchanged depends on the authentication method employed. Information relating to the particular scheme is carried in the body of the Authentication packet.

Table C.1 WLAN packet types

Packet Types				Usage
type		subtype		
00	mgmt	1100	Deauthentication	This packet is an announcement stating that the receiver is no longer authenticated. It is a one-way communication from the authenticating station (a BSS or functional equivalent), and must be accepted. It takes effect immediately.
01	ctrl	1010	PS-Poll	Power Save polling packet. Stations in power save mode awaken periodically to listen to selected Beacons. If they hear that data is waiting for them, they will awake more fully and send a PS-Poll packet to the access point (BSS) to request the transmission of this waiting data. In Control packets of the Power Save-Poll type, the Duration/ID field contains the association ID (AID) for the station sending the packet.
01	ctrl	1011	RTS	Request To Send. Coordinates access to airwaves.
01	ctrl	1100	CTS	Clear To Send. Response to a RTS, coordinates access to airwaves.
01	ctrl	1101	ACK	Acknowledges receipt of transmitted data.
01	ctrl	1110	CF End	Signals the end of Contention Free period.
01	ctrl	1111	CF End + CF ACK	Signals the end of the Contention Free period and Acknowledges the receipt of some packet in a single message.
10	data	any	any	Multiple subtypes exist for Data type packets, but all have the same basic format, as described above. (see Appendix A, “Packets and Protocols” on page A-3.) The different Data subtypes essentially just piggyback CF-Poll, CF-ACK, and CF-End messages onto the data message in a single transmission. This allows the BSS to gain higher throughputs possible using PCF (point coordinating function).

Product Support and Maintenance

Providing quality technical support to our customers is very important to us! Our online technical support form provides our customers with a standard format for reporting product issues and comments, while giving our staff the information required to deliver expeditious responses to specific issues and product feature requests.

AiroPeek is available with two levels of maintenance. Standard Maintenance is available for twelve or twenty-four months and can be purchased with your product on our Web site. Premium Maintenance is available for twelve months and can be purchased by contacting sales@WildPackets.com.

Standard Maintenance (available for 12 or 24 months)

- Priority technical support via telephone, electronic mail, fax
- Automatic notification of and on-line access to product updates and upgrades as available
- Password access to the maintenance area at www.WildPackets.com
- Free documentation updates
- Online technical reference materials
- Free utility software
- Qualification for pre-release product testing

Premium Maintenance

- Additional 12 months Standard Maintenance benefits
- One Remote Trace File Analysis (next business day response)
- 1 class seat in a WildPackets Academy 3-day class
- 1 companion seat at 50% discount in any WildPackets Academy 2-day class

Technical support

If you have a problem with AiroPeek, please fill out the web-based technical support form located at http://www.wildpackets.com/support/contact, or call (800) 466-2447.

Resources

WildPackets Academy

WildPackets Academy offers a structured educational curriculum centered on practical applications of protocol analysis techniques using EtherPeek and AiroPeek. Introductory courses in the basic concepts of protocol analysis provide the foundation for a full range of advanced offerings in specialized topics. See www.wildpackets.com/services for a full course catalog, current public course scheduling, web-delivered courses, and on-site course delivery information.

Network Analysis Courses

WP-100	Foundations of Network Protocol Analysis
WP-101	Network Troubleshooting Methods
WP-102	Emerging Ethernet Technologies: VoIP, Full Duplex, Gigabit, and Switching
WP-103	TCP/IP Protocol Analysis Methods
WP-104	Advanced TCP/IP Protocol Analysis
WP-105	AppleTalk, AppleShare IP, and Mac OS/X Network Analysis
WP-106	Wireless LAN Administration

Live Online QuickStart e-Seminars

QuickStart e-Seminars are hour-long programs focusing on detailed aspects of using EtherPeek and AiroPeek, led by a WildPackets Academy instructor. See our website at http://www.wildpackets.com for current scheduling information.

T.E.N. Video Workshop

The Technology, Engineering, and Networking Video Workshop is a 5-Session, 14-Module self-paced program covering the major components of protocol analysis. Participants complete each module by working though exercises and submitting answers to a professional instructor at WildPackets Academy. The modules in the T.E.N. program are consistent with the material tested in the NAX certification program. Visit our website at: http://www.wildpackets.com/services/video for more information.

NAX™ Certification

WildPackets Academy provides instruction and testing for the NAX (Network Analysis Expert) Certification. A Network Analysis Expert certificate is confirmation by WildPackets Academy that an individual is fully qualified to perform Ethernet or 802.11 Wireless network protocol analysis.The NAX certification program is completely vendor-neutral and is positioned as an industry-standard method for demonstrating protocol analysis expertise. For complete details, see http://www.nax2000.com.

Consulting Services

WildPackets offers a full spectrum of expert network analysis consulting services, available on-site, online or through remote dial-in service:

- On-Site Consulting
- Performance Baseline and Network Capacity Planning Report
- Infrastructure Design Analysis Services
- Remote Consulting Services

For complete details, see http://www.wildpackets.com/services/consulting.

White papers

WildPackets offers a number of white papers on network management topics, ranging from basic approaches to network monitoring, troubleshooting, and security to switched network management and remote analysis. To obtain copies of these white papers, please visit: http://www.wildpackets.com/support/resources.

Software License Agreement

SOFTWARE LICENSE AGREEMENT

PLEASE READ THIS LICENSE AGREEMENT CAREFULLY

You are purchasing a license to use WildPackets Software. The Software is owned by and remains the property of WildPackets, is protected by international copyrights, and is transferred to the original purchaser and any subsequent owner of the Software media for his/her use only according to the license terms set forth below. **Opening the packaging and/or using the Software indicates your acceptance of these terms.** If you do not agree to all of the terms and conditions herein, return the Software, manuals and any partial or whole copies you have made within thirty days of purchase to the party from whom you purchased it for a refund, subject to any restocking fee.

1. Grant of License:

WildPackets grants the original purchaser (Licensee) the limited rights to possess and use WildPackets Software (Software) and User Manual on the terms and conditions specifically set out in this License.

2. Term:

This License is effective as of the time Licensee receives the Software, and shall continue in Effect until Licensee ceases all use of the Software and returns or destroys all copies thereof, or until automatically terminated upon the failure of Licensee to comply with any of the terms of this License.

3. Your Agreement:

SINGLE USER LICENSE

• The Software is provided under a Single User License. This means that one specific individual is licensed to install and use the Software on his/her PC. That specific individual may also use the Software on his/her portable or home computer.

• If the Software is installed on a networked system, or on a computer connected to a file server or other system that physically allows shared access to the Software, Licensee agrees to prevent use of the Software by more than one user.

MULTIPLE USERS LICENSE

• If you want to install the Software on a network and provide access for more than one user, you can purchase additional single-user licenses. Each additional single-user license allows one other specific individual to install and use the Software. There is no limit to the number of additional single-user licenses that may be purchased.

• Additional single-user licenses are not concurrent-user licenses (that is, each additional single-user license is associated with a specific individual). There is no restriction on the number of additional single-user licensees who may access the Software at any given time. A group of 50 users who want access to a single copy of the Software must purchase 49 additional single-user licenses, for instance.

•One machine-readable copy of the Software may be made for BACK-UP PURPOSES ONLY, and the copy shall display all proprietary notices, and be labeled externally to show that the back-up copy is the property of WildPackets, and that its use is subject to this License. Documentation in whole or part may not be copied.

•Licensee may transfer its rights under this License, PROVIDED that the party to whom such rights are transferred agrees to the terms and conditions of this License, and written notice is provided to WildPackets. Upon such transfer, Licensee must transfer or destroy all copies of the Software.

•Licensee agrees and certifies that neither the Software nor any software product containing code generated by the Software: (a) is being or will be shipped, transferred or re-exported, directly or indirectly into any country prohibited by the United States Export Administration Act and the regulations thereunder, or (b) will be used for any purpose prohibited by same.

•Except as expressly provided in this License, Licensee may not use, copy, disseminate, modify, distribute, sub-license, sell, rent, lease, lend, give, or in any other way transfer, by any means or by any medium, including electronic, the Software. This license is for machine readable object code only, and Licensee will use its best efforts and take all reasonable steps to protect the Software from unauthorized use, copying or dissemination, and will maintain all proprietary notices intact.

4. LIMITED WARRANTY

WildPackets warrants the Software media to be free of defects in workmanship for a period of ninety days from purchase. During this period, WildPackets will replace at no cost any such media returned to WILDPACKETS, postage prepaid. This service is WildPackets' sole liability under this warranty. LICENSE FEES FOR THE SOFTWARE DO NOT INCLUDE ANY CONSIDERATION FOR ASSUMPTION OF RISK BY WILDPACKETS OR ITS LICENSOR, AND WILDPACKETS AND ITS LICENSOR DISCLAIM ANY AND ALL LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR OPERATION OR INABILITY TO USE THE SOFTWARE, OR ARISING FROM THE NEGLIGENCE OF WILDPACKETS AND ITS LICENSOR, OR THEIR EMPLOYEES, OFFICERS, DIRECTORS CONSULTANTS OR DEALERS, EVEN IF ANY OF THESE PARTIES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHERMORE, LICENSEE INDEMNIFIES AND AGREES TO HOLD WILDPACKETS AND ITS LICENSOR HARMLESS FROM SUCH CLAIMS. THE ENTIRE RISK AS TO THE RESULTS AND PERFORMANCE OF THE SOFTWARE IS ASSUMED BY THE LICENSEE. THE WARRANTIES EXPRESSED IN THIS LICENSE ARE THE ONLY WARRANTIES MADE BY WILDPACKETS AND ITS LICENSOR, AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND OF FITNESS FOR A PARTICULAR PURPOSE. THIS WARRANTY GIVES YOU SPECIFIED LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF WARRANTIES, SO THE ABOVE LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU.

5. General

This license is the complete and exclusive statement of the agreement of the parties. Should any provision of this License be held to be invalid by any court of competent jurisdiction, that provision will be enforced to the maximum extent permissible, and the remainder of the License shall nonetheless remain in full force and effect. This License shall be controlled by the laws of the State of California, and the United States of America.

6. United States Government Restricted Rights

Use of the Software by any department, agency or other entity of the United States Federal Government is limited as follows:

(1) The Software and User Manual are provided with RESTRICTED RIGHTS, and are trade secrets of WildPackets for all purposes of the Freedom of Information Act.

(2) Use, duplication or disclosure is subject to restrictions set forth in subparagraph (c)(I)(ii) of the Rights in Technical Data and Computer Software clause at 252.227-7013 or in subparagraphs (c)(1) and (2) of the Commercial Computer Software - Restricted Rights at 48 CFR 52.227-19, as applicable. Manufacturer: WildPackets, Inc., 1340 Treat Blvd., Suite 500, Walnut Creek, CA 94597.

Contacting WildPackets

During normal business hours, we are available by phone. You can also contact us by fax or email, and we will usually get back to you by the next business day.

Phone	(925) 937-3200
Domestic	(800) 466-2447
FAX	(925) 937-3211
Email	techsupport@wildpackets.com
	sales@wildpackets.com
Web	http://www.wildpackets.com

Our address:

WildPackets, Inc.
1340 Treat Blvd., Suite 500
Walnut Creek, CA 94597

Training and Certification:

WildPackets Academy
(800) 466-2447
http://www.wildpackets.com/services

Index