WildPackets

AiroPeek NX™

expert 802.11 wireless LAN network analyzer

Quick Tour

WildPackets, Inc.
1340 Treat Blvd, Suite 500
Walnut Creek, CA 94597
www.wildpackets.com

AiroPeek NX Quick Tour Contents

AiroPeek NX ™ Quick Tour

Welcome to AiroPeek NX, the real-time Expert network analyzer for 802.11 WLANs from WildPackets. AiroPeek NX combines AiroPeek's advanced set of troubleshooting and monitoring features with Expert problem detection heuristics and diagnostic capabilities. This Quick Tour will help you become familiar with some key program features.

AiroPeek NX works by capturing traffic from one or more wireless adapters, providing the tools to filter, analyze and interpret traffic patterns, data packet contents, statistics, and protocol types.

AiroPeek NX now supports distributed WLAN analysis with the separately purchased RFGrabber Probe. Please refer to the user manual and online help to find out how to extend monitoring and analysis capabilities to remote sections of your wireless network.

Note: AiroPeek NX works with all the latest revisions to the IEEE 802.11 WLAN standard, and automatically presents the correct options for 802.11a, b, or g. Any part of the documentation or program that refers to 802.11 without further qualification applies equally to networks of any of these standards.

Getting Started

When the **Monitor Statistics** item under the **Statistics** menu is enabled (as it is by default) and a supported adapter is chosen, AiroPeek NX calculates Monitor statistics based on all the traffic it sees on that adapter.

Monitoring the network

To begin collecting Monitor statistics, follow these steps:

1. Launch the program by choosing **WildPackets AiroPeek NX** from the **Start** menu.
2. Choose any supported 802.11 WLAN adapter from the list displayed in the ***Adapter*** view of the **Monitor Options** dialog. If you do not have a wireless adapter, you can choose *New File Adapter* and open any AiroPeek (*.apc) packet file, such as those in the Samples directory in the main program directory. AiroPeek NX will cycle through the packets in the chosen file, allowing you to simulate most aspects of “live” functionality.
3. To focus on a particular part of the radio spectrum, click the *802.11* tab to open the ***802.11*** view of the **Monitor Options** dialog.
4. Using the radio button in the ***802.11*** view of the **Monitor Options** dialog, you can tell the current adapter to *Select channel by* the specified channel *Number*, or by searching for a channel 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.

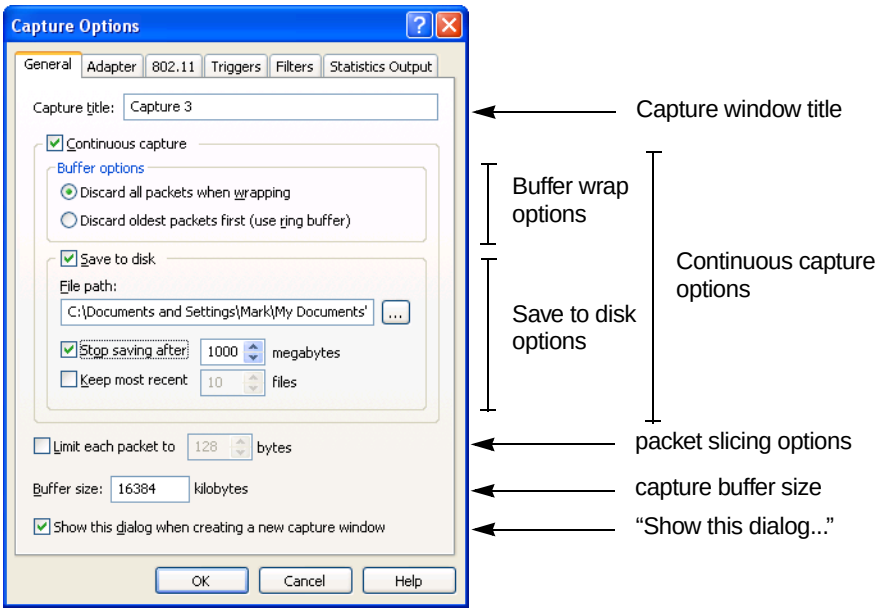
   You can also use the ***802.11*** view of the **Monitor Options** dialog to handle the automatic decryption of WEP encrypted packets on your network, by supplying AiroPeek NX with a valid WEP key set. For more on WEP, please see “WEP and AiroPeek NX” on page 3.
5. Under the **Monitor** menu, make sure the **Monitor Statistics** item has a check mark beside it, showing that it is enabled. If it does not, click the item to enable it.

6. Select from the **Monitor** menu to view statistics windows for **Nodes**, **Protocols**, **Size** (of packet), **Summary**, **History**, or **Channel**.

   AiroPeek NX will continue to collect Monitor statistics from the selected adapter until you quit the program or choose **Reset Statistics** from the **Monitor** menu.

Feature # 1: CAPTURING PACKETS FROM MULTIPLE ADAPTERS
Sampling network traffic in detail

To capture packets in AiroPeek NX, you create a Capture window, set its parameters, and click the **Start Capture** button. It's as simple as that.

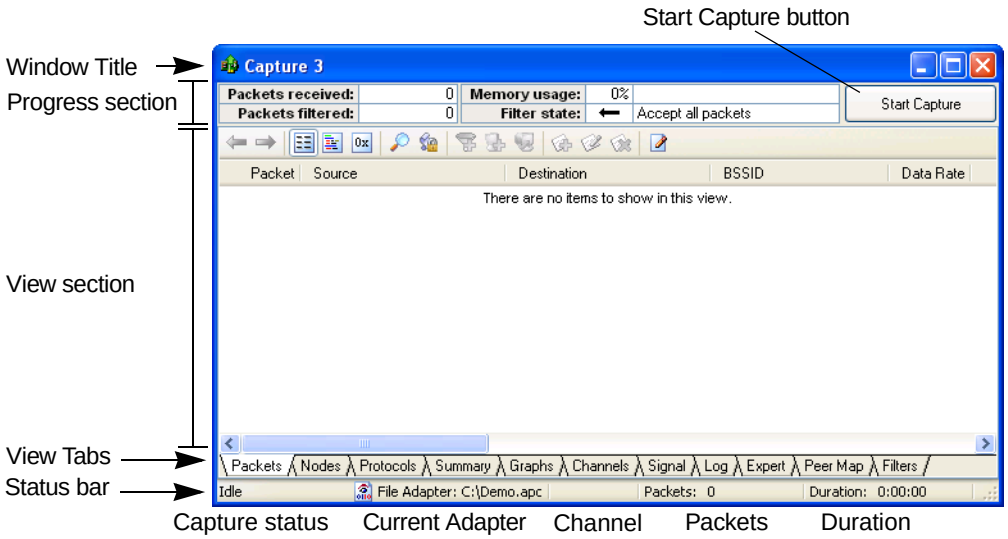


To create a new Capture window:

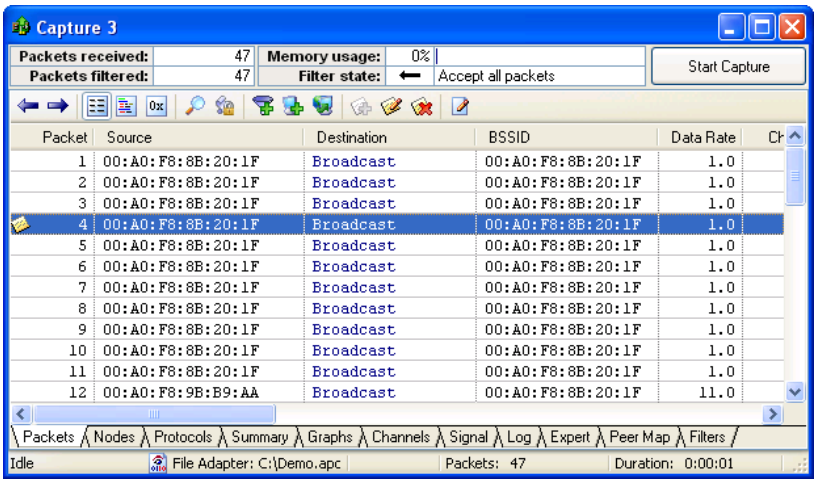
1. Choose **New…** from the **File** menu to open the **Capture Options** dialog.
2. The **Capture Options** dialog presents five views, allowing you to define a complete set of options for each Capture window. At a minimum, for each new Capture window, you must set, or accept the default values for:
   - the capture buffer (in the ***General*** view),
   - the adapter from which to capture (in the ***Adapter*** view), and
   - the channel selection (in the ***802.11*** view).

Note: 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.

3. When you have set the capture options, click **OK** to open the new Capture window.



4. Click **Start Capture**. You will see packets from your selected adapter processed and displayed in the new Capture window.



To add to or change the mix of columns, click in the column headings to open the **Packet List Options** dialog. To change column order, use drag and drop.

To open another Capture window, choose **New…** from the **File** menu again. You can open multiple Capture windows, each with its own buffer options, adapter, trigger settings, and options for filters and statistics output.

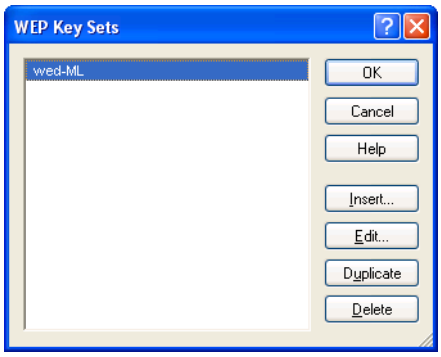
Feature # 2: WEP AND AIROPEEK NX

Configuring AiroPeek NX for wired equivalent privacy (WEP)

When provided with the appropriate key sets, AiroPeek NX can decrypt WEP (Wired Equivalent Privacy) encrypted traffic on your network on-the-fly, just like any other authorized user.

AiroPeek NX can store multiple sets of shared keys, each with its own short name. This prevents errors in entering long key strings when switching from one set to another.

Important! In order to see conversations displayed in the ***Expert*** view (Feature #3) and ***Peer Map*** view (Feature #4), traffic must be unencrypted.



Example: Enabling an existing WEP key set

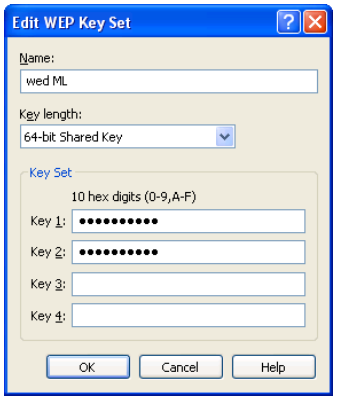
To enable AiroPeek NX to decode higher level protocols on networks where WEP is in use,

1. Select the adapter whose traffic you wish to decrypt in the ***Adapter*** view of either the **Capture Options** or the **Monitor Options** dialog.
2. Choose the *802.11* tab to bring up the ***802.11*** view.
3. In the *Encryption* section of the ***802.11*** view, use the drop-down list labeled *WEP key set* to choose the key set to use for this session of AiroPeek NX from the list of available key sets. 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 **Capture Options** or the **Monitor Options** dialog.

Example: Creating a new WEP key set

To create a new WEP key set,

1. Open the ***802.11*** view of the **Capture Options** or the **Monitor Options** dialog.
2. Click the **Edit Key Sets…** button to open the **WEP Key Sets** window.
3. Click the **Insert** button in the **WEP Key Sets** window to open the **Edit WEP Key Set** dialog.
4. 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 **Options** dialog, where you can enable each key set by name.
5. Choose a *Key Length* from the drop-down list. You can choose keys of *64-bit*, *128-bit*, *152-bit*, or *User defined length*.
6. Enter the keys in hexadecimal notation (*0-9, A-F*) in the numbered text entry boxes in the section labeled *Key Set*. Because WEP itself adds 24 bits to each key, the user-entered portion is 24 bits less than the total key length. Each hexadecimal digit represents 4 bits.
7. 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.



Feature # 3: EXPERT VIEW AND EXPERT PROBLEMFINDER

Expert analysis of peer-to-peer communications

The ***Expert*** view provides expert analysis of network 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's 113 separate network event diagnoses, including 27 exclusive to wireless networks, check for anomalies and sub-optimal performance at all layers of the network. The Expert ProblemFinder not only helps identify problems, but 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.

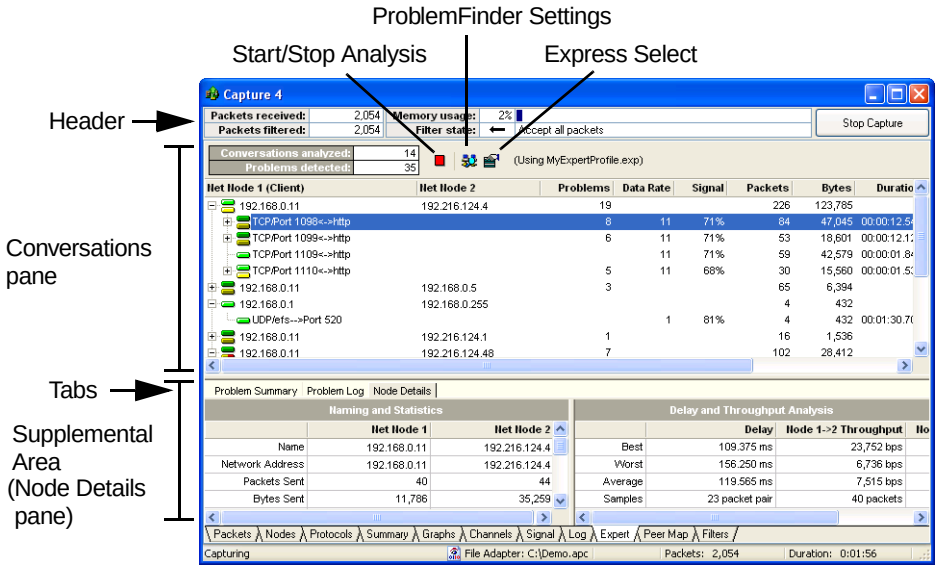
Using the Expert view

To see the ***Expert*** view in action:

1. Open a new Capture window and capture a sample of packets.
2. Click the *Expert* tab to open the ***Expert*** view.
3. Watch the ***Problems*** column for a conversation with some number of problems. Alternatively, you can watch the LED lights at the far left of the Conversations pane. The colors of the LEDs indicate the presence and severity of problems within a particular conversation.
4. Stop capture when you have a sample containing identified problems.
5. Scroll in the Conversations pane (the upper pane) of the ***Expert*** view and select a conversation or flow with one or more problems.
6. Expand the view of that flow by clicking on the + (plus) sign at the left margin.
7. Expand the descriptions of the individual problems encountered, by clicking on the + (plus) sign at the left margin.
8. Select an individual problem event.
9. Right-click on the problem event and choose **ProblemFinder Setting** from the context menu to open the **Expert ProblemFinder Settings** dialog with this particular class of event highlighted.
10. Notice that the **Expert ProblemFinder Settings** dialog tells you not only what sensitivity or setting value was used to flag this event as a problem, but it also provides a more

complete *Description* of the problem event and identifies *Possible Causes* and *Possible Remedies*.

11. Close the **Expert ProblemFinder Settings** dialog, but do not close the ***Expert*** view.



The ***Expert*** view makes it easy to get to the source of trouble. When the ***Expert*** view diagnoses a problem, you have a variety of ways to get to the packets involved. You can select all the packets in a conversation or an individual packet or group of packets with a particular problem. Where a diagnosis is based on a change or an unexpected response, you can select the pair of packets that allowed the diagnosis.

To review all the packets in a conversation diagnosed with one or more problems:

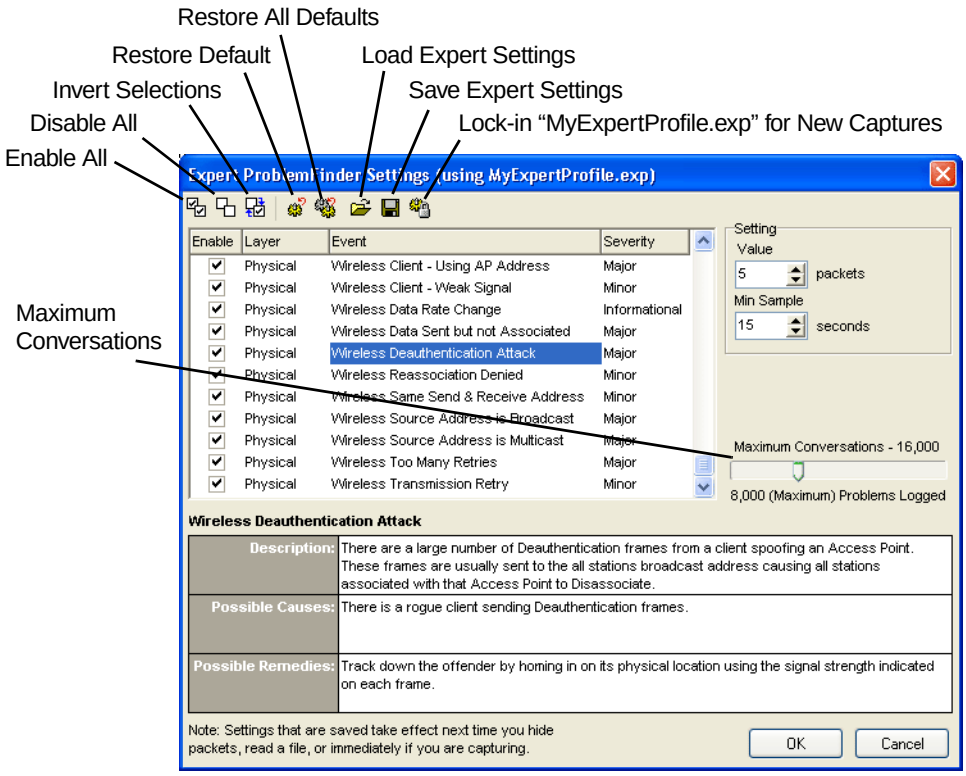
1. In the Conversations pane (the upper pane) of the ***Expert*** view, select a conversation with one or more problems.
2. Click the **Express Select** button in the ***Expert*** view header section.
3. In the **Selection Results** dialog which appears, choose **Hide Unselected**, and click **OK**.
4. In the resulting ***Packets*** view, scroll to the ***Expert*** column. Notice that individual packets have entries here, provided by the Expert Analysis function.
5. You can scroll through the ***Expert*** column entries to choose a packet to open (by double-clicking on its entry in the ***Packets*** view), or

To see the pair(s) of packets associated with a problem diagnosis:

1. In the supplemental information panes area at the bottom of the ***Expert*** view, click the *Problem Log* tab to open the *Problem Log*.
2. Click in the header of the ***Event*** column to sort by that column. You can sort the *Problem Log* by any of its columns. The ***Event*** column of the *Problem Log* shows the same information as is provided in the ***Expert*** column of the ***Packets*** view.
3. Each log entry is a single packet. Select one or more log entries containing a reference to a second packet, such as *(see packet 503)*. Problems related to transmission retries, response times, rate changes, and so forth may reference a second packet.
4. Right-click on the entry or entries and choose **Select Related Packets** > **Selected Entries + "See" or "From Pkt"** from the context menu.

5. From the **Selection Results** dialog which appears, you have a number of options for displaying decodes of the packets selected.

Expert ProblemFinder



The **Expert ProblemFinder Settings** window shows the *Description*, *Possible Causes*, and *Possible Remedies* for each problem it can diagnose. The window also contains a slider bar for setting the *Maximum Conversations.* This sets an upper limit on the system resources which can be used by the Expert Analysis functions.

Feature # 4: PEER MAP

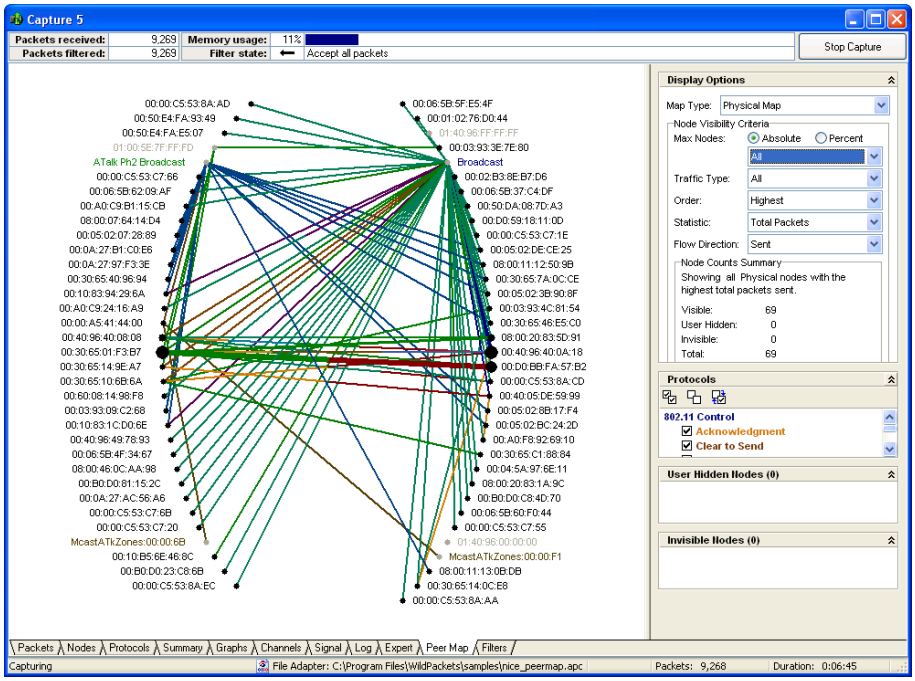
Visualizing traffic patterns

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 and line color to show the volume and protocol of traffic between nodes. The nodes themselves can be color-coded for protocol and size-coded for traffic volume and can show icons for node type, based on Name Table entries.

The Peer Map displays only the packets visible in the ***Packets*** view. Hiding and unhiding packets in the ***Packets*** view can be used to alter the Peer Map. In addition, 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 in 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, its

thickness the volume of traffic. When you drag nodes to new positions, the lines rubber-band.



To use the Peer Map:

1. Open a Capture window and capture some traffic.
2. Stop capture.
3. Click the *Peer Map* tab to open the ***Peer Map*** view.
4. In the *Display Options* section at the right of the ***Peer Map*** view, choose *IP Map* or *Physical Map* from the *Map Type* drop-down list.
5. If you selected *IP Map,* then only nodes engaged in IP traffic are displayed. If you have used a WEP key to unencrypt traffic, then nodes will be displayed only if you have selected *Physical Map*.
6. Change the *Traffic Type* setting, using the drop-down list, from the default *All* to *Unicast* or *Multicast*. Notice how the Peer Map changes to display only the nodes sending or receiving these types of traffic.
7. Restore the *Traffic Type* setting to *All*.

   Go to the *Protocols* section and deselect some of the protocols shown there. Notice that the lines indicating traffic between nodes disappear as their protocol is disabled in the *Protocols* settings.

Feature # 5: ALARMS

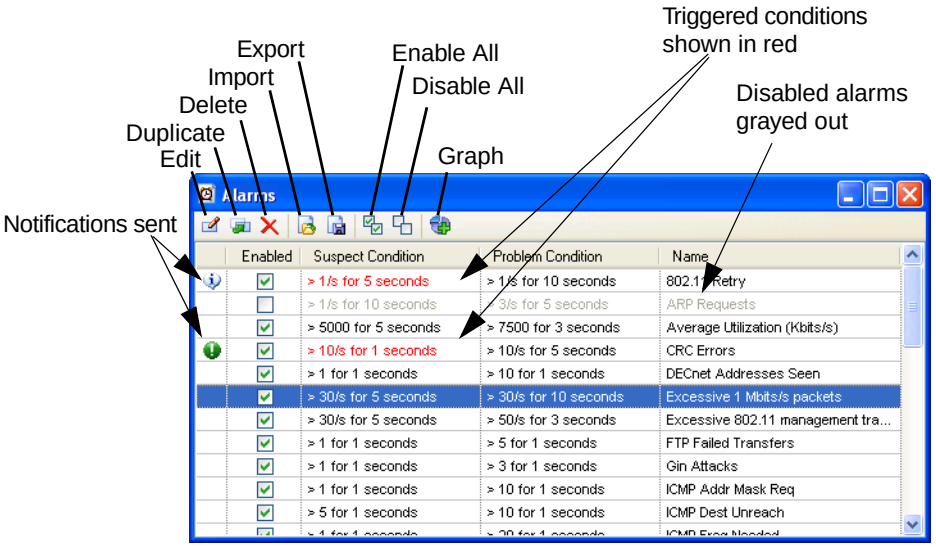
Monitoring for multiple possible problems simultaneously

Alarms query a specified Monitor statistics function approximately once per second, testing for user-defined alarm and alarm resolution conditions. On matching any of these tests, the alarm function sends a notification of a user-specified severity.

You can create an alarm for any individual statistics item in the **Node**, **Protocol**, or **Summary Statistics** windows. To create a new alarm, highlight the statistics item and click the **Make Alarm** button, or right click and choose **Make Alarm…** from the context menu. In the **Make Alarm** dialog, you can set the parameters defining two levels of alarm (*Suspect Condition* and *Problem Condition*) and define the *Resolve Condition* that signals a return to normal.

To review the installed Alarms:

1. Choose **Alarms** from the **View** menu to open the **Alarms** window.
2. Notice that any enabled alarm has a checkmark in the ***Enabled*** column.
3. Notice that any alarm which has been tripped is shown in red.
4. To edit any alarm, highlight it and click the **Edit** button at the top of the **Alarms** window to open the **Edit Alarm** dialog for that alarm.



Predefined alarms

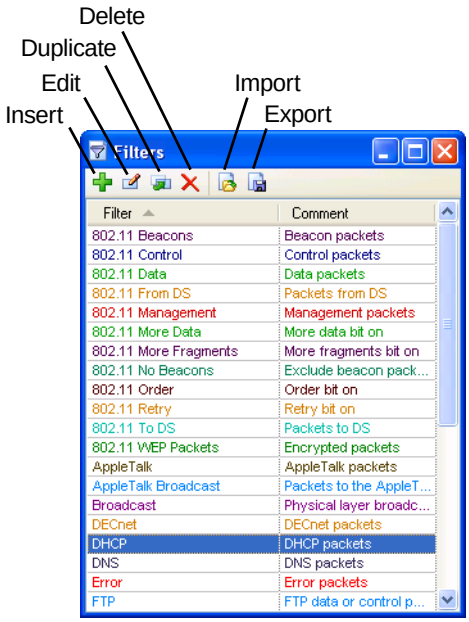
AiroPeek NX includes two sets of ready-made alarms for your convenience, located in the 1033\Alarms directory where you installed AiroPeek NX. The set of alarms loaded on installation is stored in a file called Default Alarms.alm. A second, larger set of alarms is included in a file called Additional 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.

Feature # 6: FILTERS

Pinpointing traffic of interest

Filters let you focus on specific traffic. If you want to check a problem between two particular devices, perhaps a computer and a printer, address filters can capture just the traffic between these two devices. If you are having a problem with a particular function on your network, a protocol filter can help you home in on traffic related to that particular function.

Filters do not apply to Monitor statistics, but can be used to restrict the flow of packets into a Capture window or to select packets already captured to a buffer or saved in a file. Because statistics in Capture windows are calculated on only those packets which are in the capture buffer for that window, the combination of filters and Capture window statistical views allows you to create precise pictures of particular conditions.



Example: Make Filter - an easy way to create a filter

A simple way to create a new filter is to use the **Make Filter** button or the **Make Filter** command in the (right click) context menu. Select a packet, an item in a statistics view, or even a line in a decoded packet and use this command to create a new filter matching most of the parameters of the packet, node, protocol, conversation, or packet data item selected.

Note: The **Make Filter** command makes the most precise filter that will capture packets matching the characteristics you highlighted. For example, if you highlight the top level of the IP protocol in the ***Protocols*** view, the new filter will capture all IP traffic. If you highlight a particular packet in the ***Packets*** view, the **Make Filter** command will produce a filter matching the address, protocol, and port (if any) of the packet.

To use the **Make Filter** command:

1. Select a packet or statistics item in any window. You can also choose any line item in a decoded packet (displayed in the Decode pane of a Capture window or Packet File window, or in the ***Decode*** view of the **Packet Decode** window).
2. Click the **Make Filter** button in the header section of the view or window, or right click and choose **Make Filter** from the context menu). The **Edit Filter** dialog opens with all the parameters set to match the type of traffic represented by the item that was selected when you clicked on **Make Filter**.
3. Change the name of the filter, make any additional modifications you wish, and click **OK**.

Feature # 7: SECURITY AUDIT TEMPLATE

Early warning for wireless networks

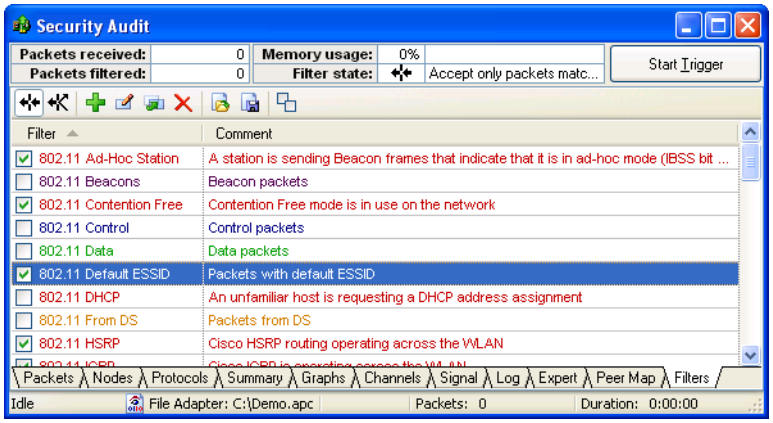
The AiroPeek NX Security Audit feature scans network traffic in the background, looking for protocols and station identifiers which could indicate a security breach. When it finds any of these, it captures the packet(s) that meet its criteria and sends a notification. It does this with a special set of filters and a capture template designed to use them.

In this section, we'll show you how to set up the Security Audit for the first time, and show you how easy it is to customize its features. The Security Audit Template is a great starting place for your own security scans.

The Security Audit requires a special set of filters. The first thing you must do is add these filters to the **Filters** window, so they will be available for the Security Audit Template.

1. On the **Start Page**, click on the link to the *Security Audit Template*.
2. This will open the the Security Audit Readme. Click on the link to the Security Audit Filters at the top of the Readme.
3. The Security Audit Filters.flt file will be automatically imported into the filters in AiroPeek NX.

   The Security Audit Template is a capture template. A capture template defines the set-up for a new Capture window, including its name, buffer size and usage, triggers, and filters. With capture templates, you can start a capture session with complex parameters in a matter of clicks.



To create a Capture window using the Security Audit Template:

1. Return to the Security Audit Readme and click on the link to the Security Audit Template.
2. This will automatically open a fully configured new Capture window called *Security Audit*.
3. It may be helpful to display the ***Filter*** column in the packet list, as this column shows the name of the filter which caused the template to trigger. Right-click in any column header in the ***Packets*** view to show the list of available columns. A check mark appears beside enabled columns. Click on **Filter** to add the ***Filter*** column to the ***Packets*** view.

4. Click the **Start Trigger** button in the new *Security Audit* Capture window to tell it to begin listening for any of the configured trigger events. Alternatively, you can choose **Start Trigger** from the **Capture** menu or type **Ctrl + Y** to start the trigger event watch.

Tip Once you have used a template, its name is added to a quick pick list immediately under the **New From Template** item in the **File** menu.

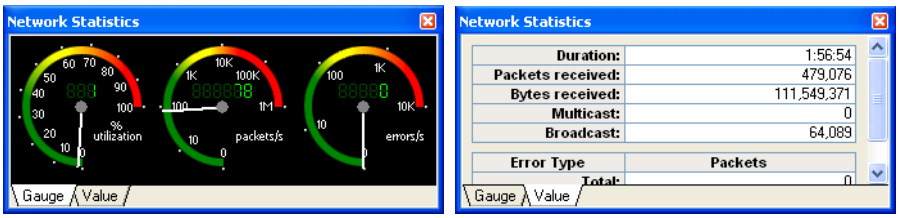
5. When AiroPeek NX encounters the first packet matching any of the enabled trigger event parameters, the trigger will be tripped. In this particular case, the start trigger is set to send a "Severe" notification when it is tripped. The Capture window is set to begin capturing any packets matching the separately enabled capture filters.

   You can examine and change any of the settings for the *Security Audit* Capture window, its trigger and/or filters. If you alter the template, then choose **Save Capture Template…** from the **File** menu and give the template a new name, you will have created your own custom security scanning template.

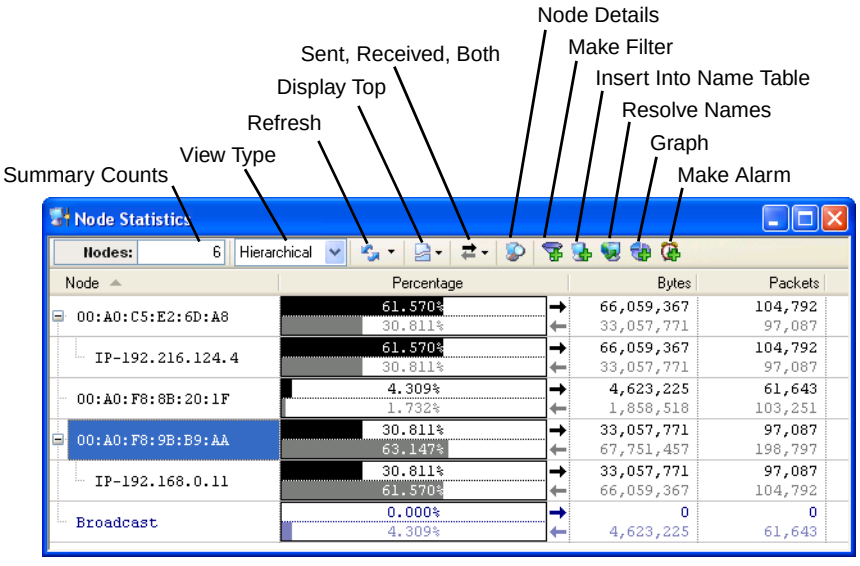
Feature # 8: MONITOR STATISTICS

Real-time statistics monitor traffic patterns

Monitor statistics provide insight into the overall flow of network traffic. They are like the view from a traffic helicopter and can indicate bottlenecks and anomalies. Use these windows to identify trends and current conditions that may signal unexpected network problems.



The Monitor statistics functions keep only the aggregate information needed to provide an updated tally of all the tracked parameters. Data collection for Monitor statistics is independent of any Capture windows, and cannot be altered by filters, triggers, or any other function.

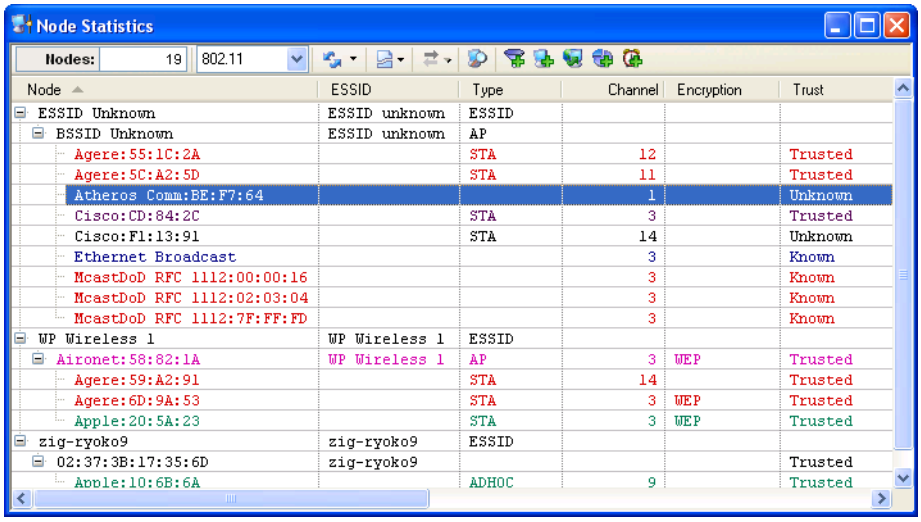


AiroPeek NX collects data on a wide variety of parameters, presented in statistics windows. You can open any or all of these Monitor statistics windows from the **Monitor** menu.

Example: SSID Tree view

AiroPeek NX can display all the wireless nodes seen on the selected adapter as an SSID (Service Set Identifier) tree in the ***802.11*** view of **Node Statistics**.

1. Select **Nodes** from the **Monitor** menu.
2. Choose *802.11* from the*View Type* drop-down list



3. To add to or change the mix of columns, click in the column headings to see a context menu with available column headings. To change column order, use drag and drop.

The SSID tree in the ***802.11*** view makes it easy to track activity on your 802.11 WLAN in a natural way, following the logical topology of your wireless network as it changes from moment to moment. By showing individual nodes under the BSSID of the group in which they most recently sent a packet, you see the topology the way the network sees it. When an access point is trying to serve too many stations, you see it at once. When a new ad hoc group is formed, you can see its members and identify the node acting as the base station for this temporary group.

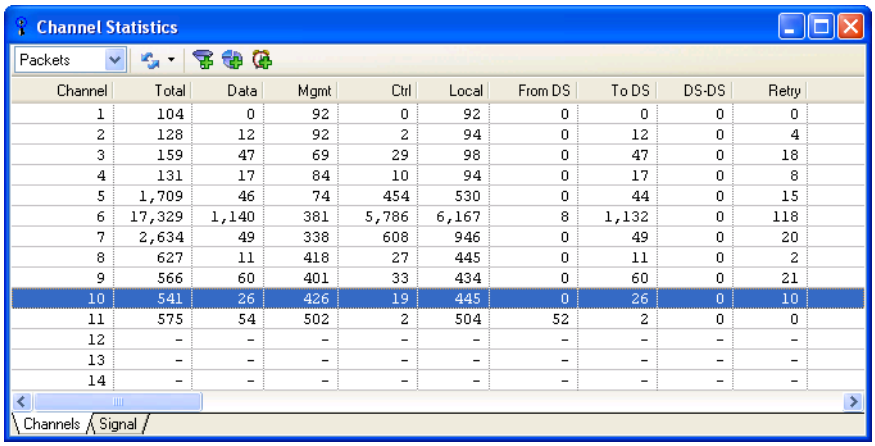
In AiroPeek NX, the ***802.11*** view also tracks the Trust value assigned to each node in the Name Table, by displaying this value in the ***Trust*** column. The default value for Trust is the lowest value: *Unknown*. This is assigned to any device added automatically to the Name Table, and is assumed for any address not found there. You can manually assign any of three Trust values to any node: *Unknown*, *Known* or *Trusted*. For example, 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.

With AiroPeek NX on your laptop, you can walk through your office and use the ***802.11*** view to create a complete snapshot of your wireless environment in a matter of minutes.

Example: Channel statistics

The ***Channels*** and ***Signal*** views of **Channel Statistics** (and the same views of Capture windows and Packet File windows) focus attention on the physical layers of 802.11 WLAN traffic.

1. Select **Channels** from the **Monitor** menu.

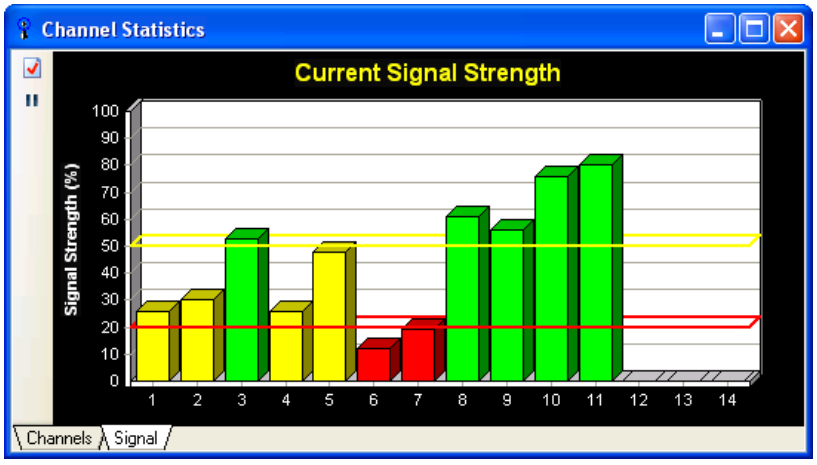


View Tabs

2. To add to or change the mix of columns, click in the column headings to open a context menu with available column headings. To change column order, use drag and drop.

   The ***Channels*** view displays a variety of information about the traffic on each channel on which the current adapter has been listening. You can show packets, bytes, or both (as appropriate) for a number of parameters, including: total traffic, data rates, WEP parameters, packet type (control, management, or data), DS forwarding status, error and retry status, and more. The ***Channels*** view lets you quickly compare the traffic patterns on multiple channels simultaneously, or focus on one channel in detail, quickly and easily.

3. Click on the *Signal* tab.

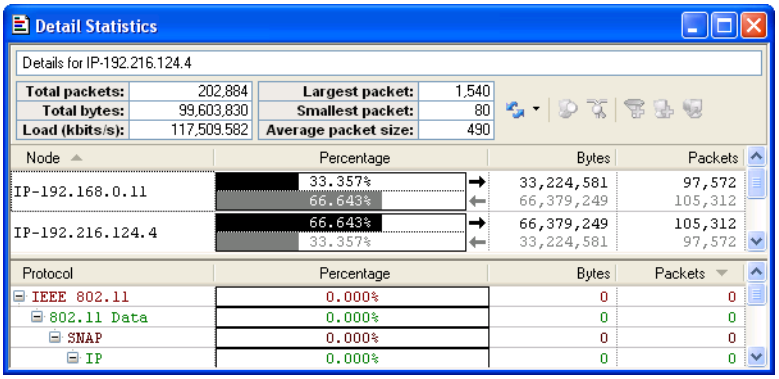


The ***Signal*** view shows the most recent signal, noise, or signal to noise comparison for all channels being scanned by the current adapter. You can choose which of these measures to show, and set the display units to RSSI (Receive Signal Strength Indicator) normalized to a percentage, or (if the selected adapter supports it) to decibel milliWatts (dBm). The ***Signal*** view shows the readings from the most recent packet captured on each channel. If

the current adapter is set to monitor only a single channel, the other channels will show no change. If the current adapter is set to scan across multiple channels, the ***Signal*** view will show the relevant reading from the most recent packet on each channel in the scan. For easy reading, the ***Signal*** view is color coded to show when signals fall above, below, or between a user-defined High and Low Threshold value. You can see at a glance when signals are falling out of range, on a single channel or on several at once.

Example: Focus on an individual device

1. Select **Nodes** from the **Monitor** menu.
2. Choose *Hierarchical* from the *View Type* drop-down list. Double-click on one of the Node addresses to get to a **Detail Statistics** window.

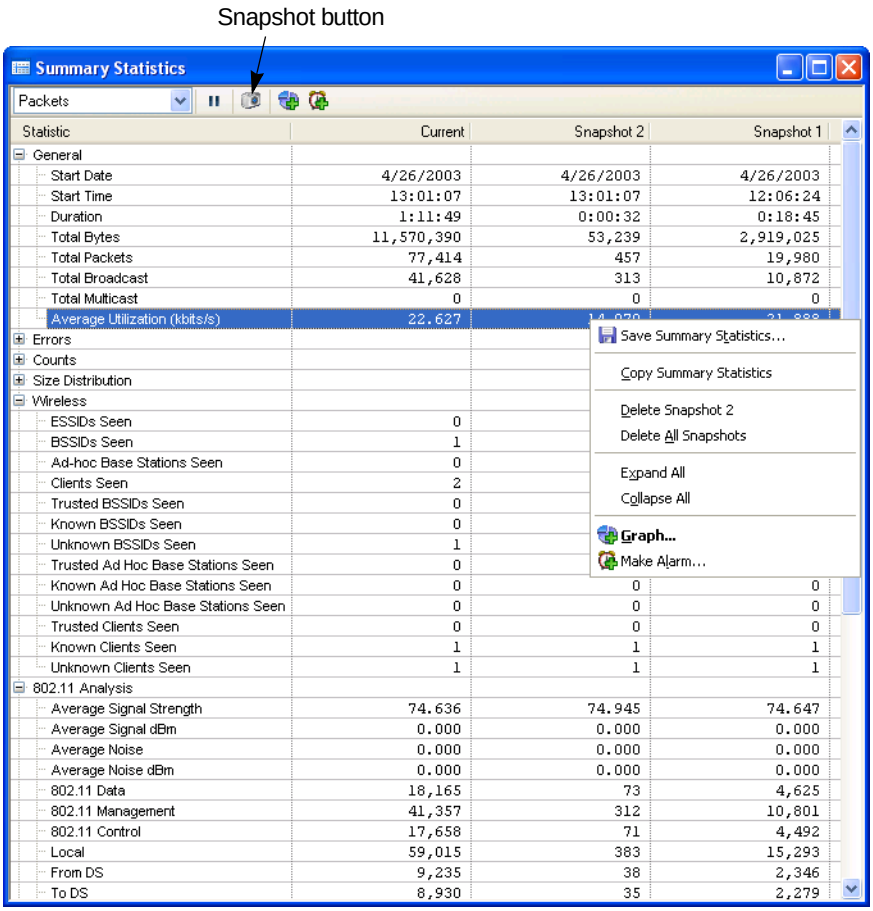


3. Click the ***Bytes*** column heading to sort the list in order of percentage of bytes. Click it again to reverse the sort order. The window will be redrawn with the largest contributors to bandwidth use at the top or bottom of the window, depending on the sort order you choose.
4. Use the *Display Top* 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*.
5. Use the drop-down list to choose to display only packets *Received*, only packets *Sent*, or both.
6. Double-click on any node to open a new window showing additional details.
7. A new window opens displaying the complete list of communication partners and protocols used by the selected node.

Example: Monitoring with Summary Statistics

The **Summary Statistics** feature allows you to monitor key network statistics in real time and save these statistics for later comparison by making a snapshot of current **Summary Statistics**. Use this feature to baseline “normal” network activity, save the data, and then compare these saved statistics with those observed during periods of erratic network behavior to help pinpoint the cause of the problem.

Of particular interest in 802.11 WLANs are the *Wireless* and *802.11 Analysis* sections of **Summary Statistics**. The *Wireless* section shows counts of *ESSIDs*, *BSSIDs*, *APs*, *Ad Hoc Base Stations*, and *Clients* seen. The *802.11 Analysis* section shows a summary of the main information provided in the ***Channels*** view, but reduces *Signal* and *Noise* measures to averages.



Summary statistics are also extremely valuable in comparing the performance of two different network segments 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” router snapshot and easily diagnose or eliminate the source of inconsistent or poor router performance.

To view **Summary Statistics**:

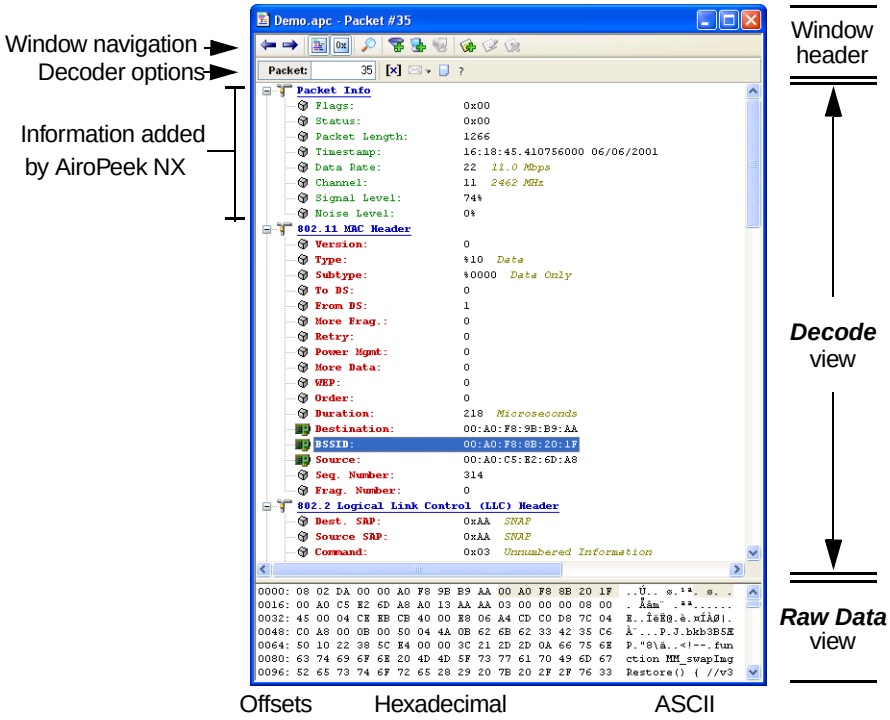
1. Choose **Summary** from the **Monitor** menu.
2. Click the **Snapshot** button. Data relating to your real-time network traffic will be displayed in a column identified with a date and start time.
3. Choose **Save Summary Statistics** from the **File** menu (or the context menu) to save the information to a text file.

   You can also periodically save **Summary Statistics** from Monitor statistics or from the ***Summary*** view of an open Capture window using the *CSV Row Report* in the ***Statistics Output*** views of (respectively) the **Monitor Options** or the **Capture Options** dialogs. Each time this report is saved, it adds a single row to the output text file. Each row contains the whole contents of the ***Current*** column as comma separated values (csv).

Feature # 9: VIEWING DECODED PACKETS

Getting to the source of problems at the detailed level

Sometimes network problems are revealed more quickly by looking at the detailed information contained in a packet. Protocol decoders and the **Packet Decode** window allow you to open packets and look inside, pinpoint sources of problems, track down faulty hardware, and learn about and examine protocol structure and compliance.



Example: Viewing packet contents

A **Packet Decode** window lays out the detailed structure and contents of a single packet. AiroPeek NX can decode thousands of types of protocols, and can display the individual elements of 802.11 WLAN packets. This example demonstrates how you can easily view the contents of individual packets to find and fix problems, as well as learn about network communications using packet decoders.

To view the detailed contents of a packet:

1. Open the Decode and/or Hex panes of the Capture window or Packet File window. Alternatively, you can double-click on a packet in the ***Packets*** view to open it in a separate **Packet Decode** window.
2. Notice the items in green at the top of the ***Decode*** view. This section includes information on the flags, size, status, packet length, timestamp, data rate, channel, signal level and noise level of the packet. If packet slicing was in effect when this packet was captured, the slice length will also be shown here.
3. Notice the body of the ***Decode*** view. The information is laid out in the same order as it appears in the packet itself. Each protocol is nested or framed within the higher level protocols. Each line shows the ASCII representation of the packet data for a particular field within the packet and the interpretation of that data, based on the protocol. A quick

glance at this section often reveals the source of trouble, particularly with incompatible implementations of a given protocol by stacks from different vendors.

4. Notice the ***Raw Data*** view at the bottom of the packet decode window. This view shows the raw hex contents of the packet on the left, with the offset of the first character in each line shown at the far left. In alignment with this, line for line, the ASCII version of the raw packet data is shown on the right.
5. When you highlight an item in one part of the window, the same bytes of the packet are highlighted in all the other views or panes as well. The highlight matches in the ***Decode*** and the ***Raw Data*** hex and ASCII views.
6. Click the **Decode Previous** or **Decode Next** buttons at the top of the window to step through the packets shown in the Packet List of the active Capture window or Packet File window.

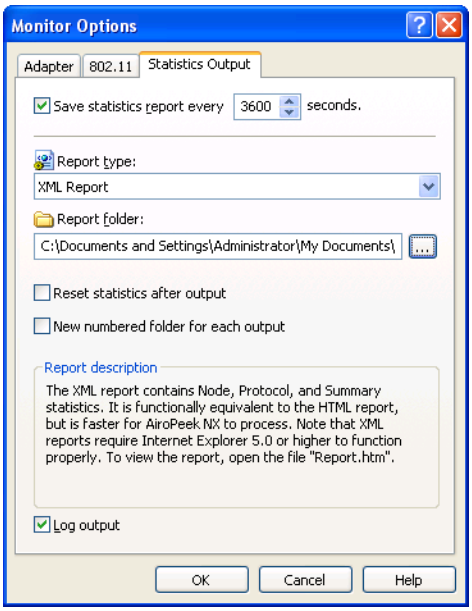
Feature # 10: PERIODICALLY SAVING STATISTICS

Building a history of your network's performance

AiroPeek NX can periodically save statistics from open Capture windows or open Monitor statistics windows as XML or HTML files, viewable with a web browser, or as either of two types of text files: comma separated values (*.csv) or tab-delimited (*.txt).

To periodically output current statistics:

1. Open the ***Statistics Output*** view appropriate to the source of the statistics you wish to periodically output. If you wish to output Monitor statistics, choose **Statistics Output…** from the **Monitor** menu to open the ***Statistics Output*** view of the **Monitor Options** dialog. If you wish to output statistics from a Capture window, open the **Capture Options** dialog for that window and click the *Statistics Output* tab to open the ***Statistics Output*** view. The two views are identical, and only the source of statistics is different.
2. Check the checkbox in the upper left to enable saving statistics
3. Set the frequency with which you want to update the statistics files, setting the interval in *seconds*.



4. Choose the type of statistics to be output and the file format to be used from the *Report type* drop-down list. A description of the selected report type is shown in the lower part of the ***Statistics Output*** view.
5. Choose the location to which these periodic reports should be saved, using the *Report folder* drop-down list.
6. Optionally, you can check *Reset statistics after output* to return statistics counts to zero after each report is written. This allows you to create a series of snapshots of network conditions.
7. 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.
8. You can also have a notice sent to the log file each time these statistics reports are updated, by checking the *Log output* checkbox.
9. Click **OK** to enable your choices.

You can also create a single instance of any of these same report types at any time for statistics in a Capture window or Packet File window, by using the **Save Report** item under the **File** menu.

There's more!

There are many more features to explore with AiroPeek NX, but not enough space here to document them all. We suggest you look at these additional features:

Name Table and name resolver options

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 NX. 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.

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

AiroPeek NX can scan all traffic, searching for logical and symbolic names in the contents of passing packets. You can control how and whether AiroPeek NX 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.

Analysis Modules

Analysis Modules are external modules that provide expert 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.

The Analysis Modules shipped with AiroPeek NX cover a wide range of the most common protocols and network applications. 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.

Triggers

Automate the start and stop of capture using triggers. Any filter can be specified as a trigger criterion. You can also set a trigger to start or stop packet capture based on time and date settings, so you can focus captures with pinpoint accuracy. Look for trigger options in the ***Triggers*** view of the **Capture Options** dialog.

ProtoSpecs™ and protocol definitions

WildPackets' ProtoSpecs technology offers a very fine level of protocol layer detail by identifying the top-level “parent” protocol and breaking-out each subprotocol layer in a hierarchical view. Look for ProtoSpecs in AiroPeek NX's Capture windows, **Filters** and **Protocol Statistics** windows. Display protocol information based on a total of the subprotocols under the parent protocol, or by each subprotocol broken-out by individual layers.

AiroPeek NX provides a definition of what a protocol abbreviation stands for and a concise description of how a protocol is used. This on-line help mechanism will assist you in determining the purpose of previously unseen packets on the network as well as help to increase your knowledge of LAN/WAN protocols. To view the definition for any particular protocol or subprotocol from any packet list view or **Protocol Statistics** window, click on your selection and then choose the **Protocol Info** command from the context menu.

Selecting, hiding and unhiding 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.

The **Select…** command from the **Edit** menu brings up the **Select** dialog that allows you to apply existing filters to 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.

Demonstration version of AiroPeek NX

The demonstration version of AiroPeek NX differs from the full-featured version in the following ways:

- Each Capture window is limited to 30 seconds of capture and no more than 250 packets.
- Only 5 Capture windows can be opened per launch.
- Only the first 250 packets of a saved file will be loaded into Packet File windows.
- Monitor statistics are captured for only 5 minutes.
- Printing and Saving are disabled.
- Does not open packet files created by other products.

- Send is limited to 100 packets.

System Requirements

The recommended configuration for systems running AiroPeek NX is:

- 600 MHz processor, 256 MB RAM
- Windows XP (Service Pack 1 or later) or Windows 2000 (Service Pack 3 or later)
- Supported wireless network adapter
- Microsoft Internet Explorer 5.5 or later required

Please see the Readme file for additional information about any special requirements for particular operating systems. Please see the installation instructions shipped with your software for additional information regarding network drivers, program file locations and uninstall instructions.

Additional product information

Please check our web site at www.wildpackets.com for product demos, literature, technical references, FAQs, system requirements and more.

AiroPeek NX™ - Expert 802.11 Wireless LAN network analyzer

AiroPeek™ - 802.11 Wireless LAN protocol analyzer

EtherPeek NX™ - Expert 10/100/1000 Ethernet network analyzer

EtherPeek™ - 10/100/1000 Ethernet protocol analyzer

EtherPeek™ for Macintosh - Ethernet packet analyzer

iNetTools™ - Menu-driven testing tools for Internet and IP-based networks

NetDoppler™ - Performance and application analysis tool

NetSense™ - Post-capture expert network analyzer

PacketGrabber™ - Remote packet capture application

PacketScrubber™ - Selective trace file data removal tool

ProConvert™ - Packet trace conversion tool

RFGrabber™ - Distributed WLAN analysis probe for AiroPeek NX

RMONGrabber™ - RMON capture module for EtherPeek NX

WebStats™ - Real-time website analysis module for EtherPeek NX

AiroPeek NX Product Maintenance

AiroPeek NX 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.

WildPackets Academy

WildPackets Academy offers a structured educational curriculum centered on practical applications of protocol analysis techniques. 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

About WildPackets, Inc.

Since 1990, WildPackets has built affordable and easy to use network analysis tools. Our customers rely on WildPackets tools to help them design, maintain, troubleshoot, and optimize their networks. For information about our company, its products and partners, please see our website at www.wildpackets.com. See the WildPackets Academy site, www.wildpackets.com/services, for information on courses and Professional Services offerings. WildPackets' Network Analysis Expert (NAX) Certification Program details can be found at www.nax2000.com.

20030514-E-APNX2.0_QT