

RFGrabber™
distributed WLAN analysis probe



Information in this document is subject to change without notice. No part of this manual may be reproduced or transmitted in any form, or by any means, electronic or mechanical, including photocopying, for any purpose, without the express written permission of WildPackets, Inc.

Copyright © 2001-2003, WildPackets, Inc. All rights reserved.

RFGripper Probe, version 1.0 user manual

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

(925) 937-3200

www.wildpackets.com

AiroPeek, AiroPeek NX, EtherPeek, EtherPeek NX, iNetTools, NAX, NetDoppler, NetSense, Network Calculator, PacketGrabber, PacketScrubber, ProConvert, ProtoSpecs, RFGripper, RMONGripper, WebStats, WildPackets and WildPackets Academy are trademarks of WildPackets, Inc. All other trademarks are the property of their respective holders.

RFGrabber Probe

RFGrabber Overview	1
How RFGrabber works	1
System requirements	2
RFGrabber as an analysis module	2
Assembling and Configuring the RFGrabber Probe	3
Hardware setup	3
Configuring the RFGrabber Probe	5
Adding a probe on a remote network	7
Using static IP addresses	8
Setting RFGrabber Probe properties	9
Name properties	9
Address properties	11
Filter properties	12
Using RFGrabber	13
Support for multiple probes.....	16
Troubleshooting.....	16
Products and Services	A-1

RFGrabber Probe

This document describes how to use AiroPeek with the separately purchased RFGrabber Probe to extend AiroPeek's monitoring and analysis capabilities.

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.

This chapter explains how to set up and configure the RFGrabber Probe hardware, and how to use the probe with AiroPeek.

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.

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.

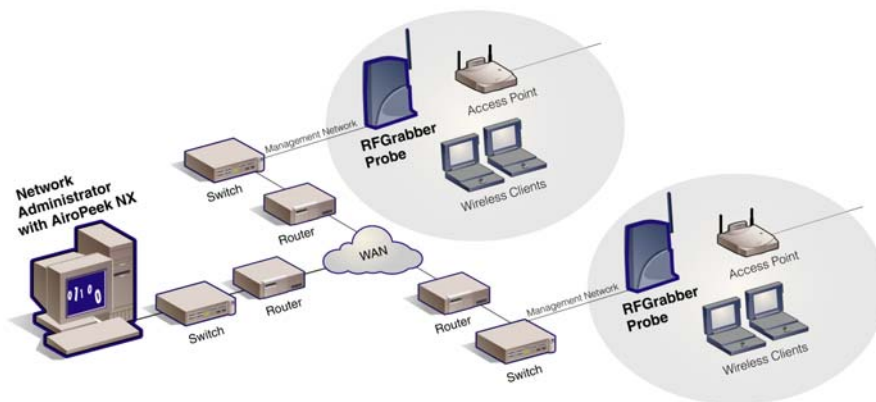


Figure 1 AiroPeek NX with two RFGripper Probes

System requirements

The RFGripper Probe requires either AiroPeek or AiroPeek NX, versions 2.0 in order to configure and use the device. In addition, the RFGripper Probe uses both Ethernet and IP to communicate. 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, at a minimum.

The RFGripper Probe is like a “listen-only” access point that connects to your existing Ethernet network and communicates with AiroPeek using IP. You can configure an individual probe, setting its 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.

RFGripper as an analysis module

AiroPeek uses the Analysis Modules architecture to interact with the RFGripper Probe. The *RFGripper* 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 RFGripper Probe. You can enable or disable the RFGripper 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 RFGripper, check or uncheck the left-most checkbox beside its name, in the column labeled **Enabled**. Click **OK** to exit the dialog, accepting your changes.

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 Ethernet broadcast 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

RFGrabber Probe

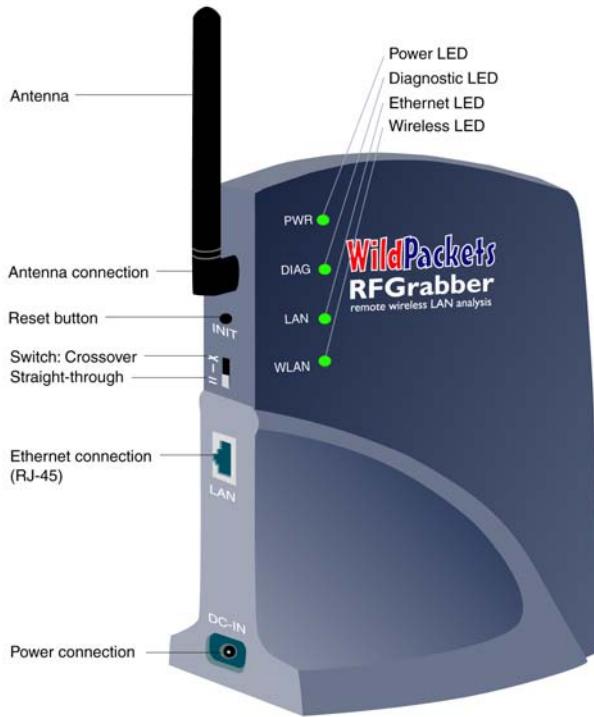


Figure 2 The RFGrabber Probe

1. Connect the antenna to the main unit by screwing it onto the gold connector.
2. To initially configure your RFGrabber Probe, it should be connected to the same local network as the computer on which AiroPeek is running.
3. Connect an Ethernet cable to the back of the RFGrabber Probe and to a hub or switch that connects to the computer on which AiroPeek is running.
4. 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.

-
5. 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.
 6. 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 Ethernet connection. Try moving the switch to the other setting.

Tip A straight-through connection is the standard way of connecting devices to an Ethernet. The crossover connection is used when connecting two Ethernet devices directly to one another, without benefit of any router, hub, or switch.

The probe is set by default to use DHCP to obtain an IP address when it is first powered on. If you do not have DHCP on your network, you may wish to configure the probe the first time you use it by connecting it directly to the machine running AiroPeek. Set the crossover switch to the crossover position. Remember to move the switch back to the straight-through position before connecting the configured RFGrabber Probe to the Ethernet network.

Configuring the RFGrabber Probe

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 configure your RFGrabber Probe 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. The **Adapter** view is open by default.

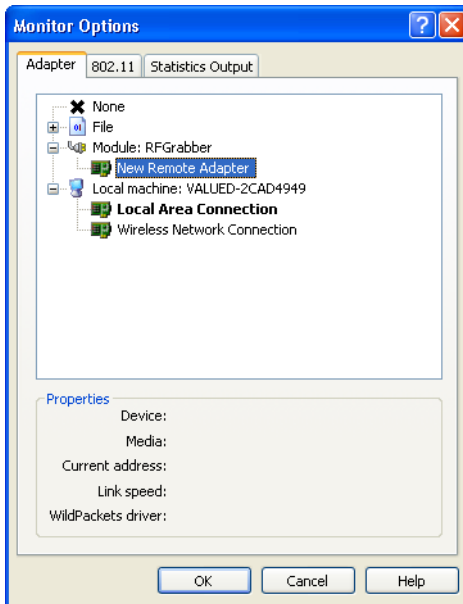


Figure 3 Adapter view of the Monitor Options dialog, showing RFGrabber Probe

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 4).

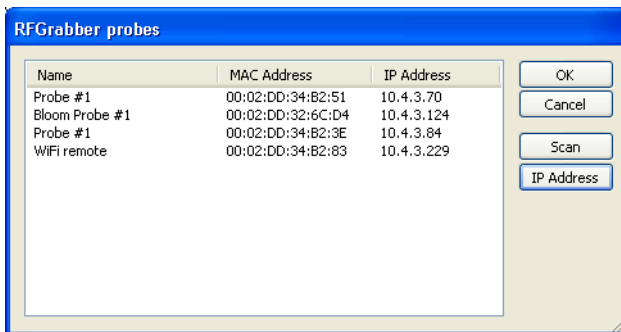


Figure 4 RFGrabber Probes dialog, showing available probes

-
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.

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 9.

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 16.

Adding a probe on a remote network

The automatic probe discovery protocol used by AiroPeek is based on Ethernet broadcast packets and 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 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*.

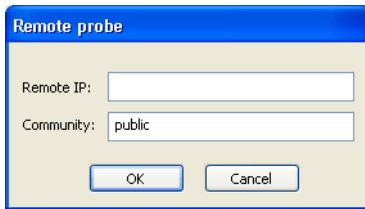


Figure 5 Remote Probe dialog

Using static IP addresses

The RFGGrabber Probe can use either a DHCP assigned IP address or a static IP address. By default, the RFGGrabber 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 relies on broadcast packets to discover a probe. This means 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.

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*. Enter a valid *IP address* in dotted decimal notation. You may also enter a *Subnet mask* and *Default gateway*, as appropriate.
5. 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**.

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

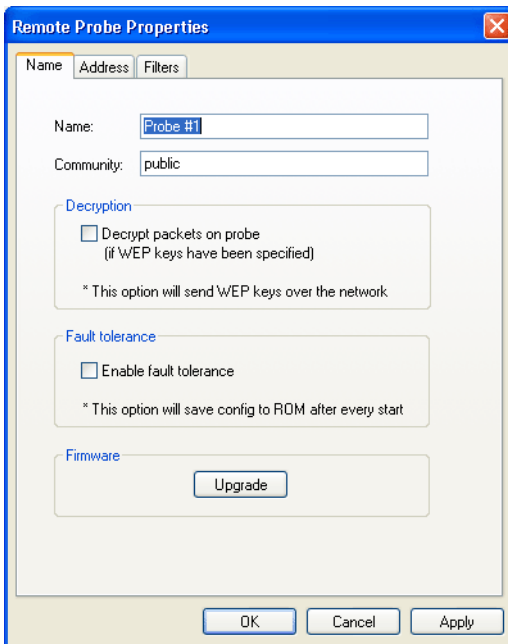


Figure 6 Remote Probe Properties dialog, Name view

In the **Name** view, 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.

RFGrabber 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.

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. 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 encryption on AiroPeek rather than on the probe.

The *Fault tolerance* section of the **Name** view lets you *Enable fault tolerance* 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.

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. 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 of the **Remote Probe Properties** dialog, 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.

Address properties

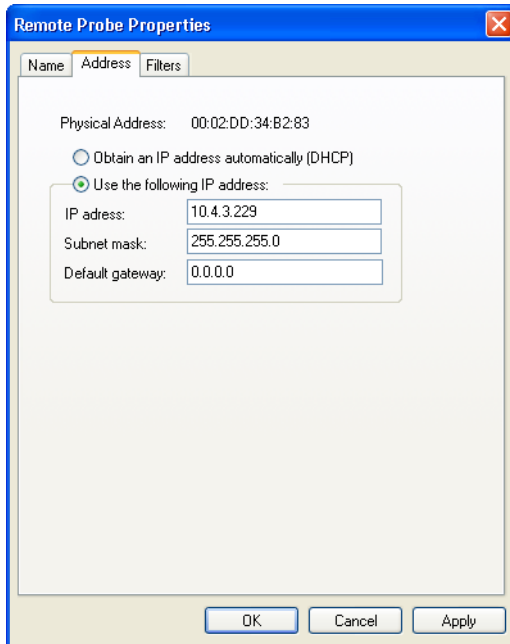


Figure 7 Remote Probe Properties dialog, Address view

The **Address** view 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 does not reflect any changes to probe address made from the local computer.

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 “Configuring the RFGripper Probe” on page 5.

Filter properties

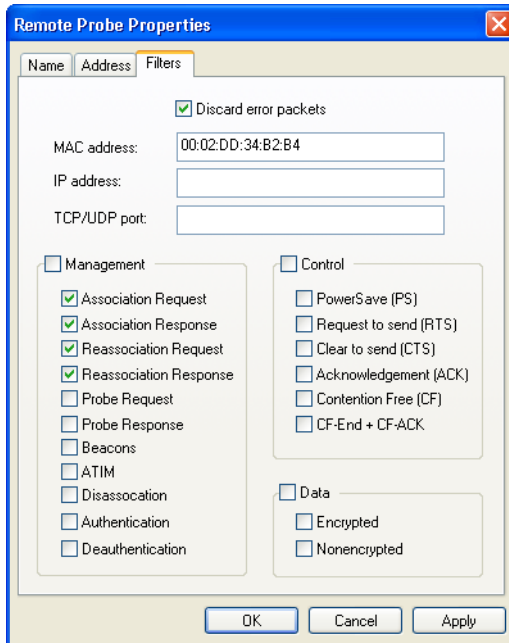


Figure 8 Remote Probe Properties dialog, Filters view

In the ***Filters*** view, you can set filters for the RFGripper 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 RFGripper Probe is that it can greatly reduce the number of packets that must be streamed back to AiroPeek.

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 packet 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 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). 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.

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.

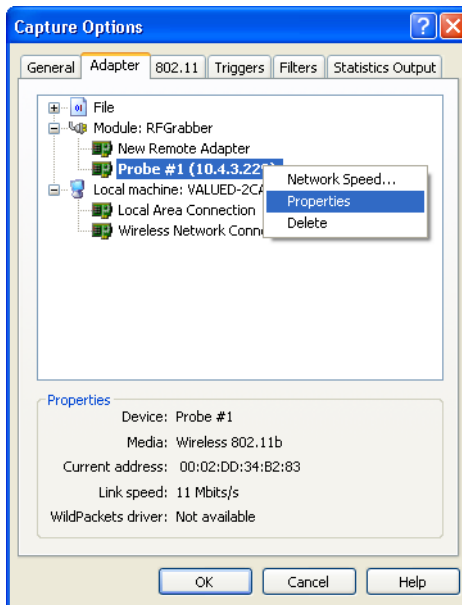


Figure 9 Adapter view of Capture Options dialog

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 RFGripper Probe. For a detailed discussion of how to use this view, see “Capture options: general” in the AiroPeek main manual.
3. Click on the **Adapter** tab to open the **Adapter** view. Expand the **Module: RFGripper** item to see a list of all available RFGripper 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 RFGripper 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 RFGripper 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” in the AiroPeek main manual.
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 RFGripper 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” in the AiroPeek main manual 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” in the AiroPeek main manual. For information on filters set on the RFGripper Probe, see “Filter properties” on page 12.
11. You can automatically output statistics from a Capture window that is using an RFGripper Probe as its adapter, just as you would from any other Capture window. Please see “Output from statistics” in the AiroPeek main manual.
12. You can save to a capture template (*.ctf) file the settings of any Capture window that is using an RFGripper 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 RFGripper 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 10).

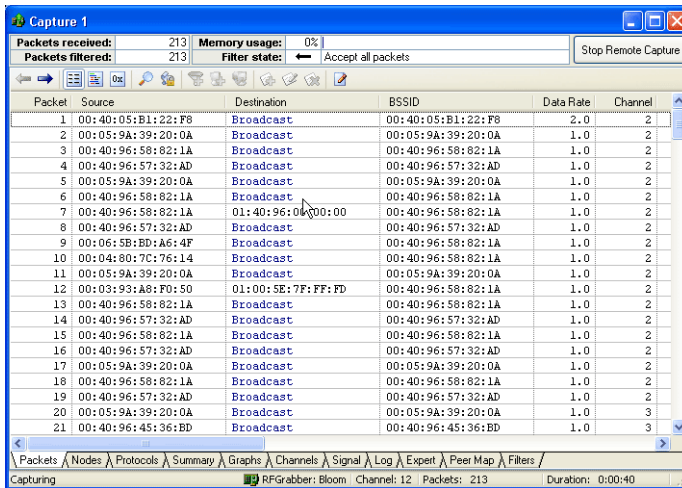


Figure 10 Remotely captured packets are streamed into the Capture window

Support for multiple probes

AiroPeek treats the RFGripper Probe like any other adapter. You can collect Monitor statistics and have multiple Capture windows using the same RFGripper 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 RFGripper Probes are connected over a separate management network, then there will be no impact on ordinary network traffic.

The number of RFGripper 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.

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 it 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 8.

How do I reset the RFGrabber Probe to its factory defaults?

To reset the RFGrabber Probe to its factory defaults:

1. Unplug the power cable.
2. Using a paper clip, hold down the reset button (marked INIT) on the back of the RFGrabber Probe.
3. Still holding down the reset button, plug in the power cable.
4. When the WLAN LED starts to blink (about 3 seconds), release the reset button.

All configuration options will be returned to their factory defaults.

What if I want to connect an RFGrabber Probe directly to my PC?

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.

Use the straight-through setting when the RFGrabber Probe is connected to an Ethernet network in the ordinary way.

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 1 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
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", "DIAG"
	Certifications	FCC Class B, CE Mark
	Operating Temp.	0° C to 50° C (32° F to 122° F)
	Storage Temp.	-25° C to 70° C (-13° F to 158° F)
	Operating Humidity	10% to 90% Non-Condensing
	Storage Humidity	10% to 90% Non-Condensing

Products and Services

WildPackets Products



WildPackets is committed to simplifying network troubleshooting, maintenance and analysis by providing excellent, robust, accessible network management tools, by lowering the price entry point and the level of technical sophistication required to use network management tools, and by providing unsurpassed Product Support and Professional Services. These analysis tools represent our core product line.

- 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
- NetSense™** - Post-capture expert network analysis
- PacketGrabber™** - Remote packet capture application
- PacketScrubber™** - Selective trace data removal tool
- ProConvert™** - Packet trace conversion tool
- RFGripper™** - Distributed WLAN analysis probe for AiroPeek NX
- RMONGripper™** - RMON capture module for EtherPeek NX
- WebStats™** - Real-time website analysis module for EtherPeek NX

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

WildPackets Professional Services

WildPackets offers a full spectrum of unique professional support services, available on-site, online or through remote dial-in service.

WildPackets Academy

WildPackets Academy provides the most effective and comprehensive network and protocol analysis training available, meeting the professional development and training requirements of corporate, educational, government, and private network managers. Our instructional methodology and course design centers around practical applications of protocol analysis techniques for Ethernet and 802.11 wireless LANs. Network Analysis courses include the following topics:

- Foundations of Network Protocol Analysis
- Network Troubleshooting Methods
- Emerging Ethernet Technologies: VoIP, Full Duplex, Gigabit, and Switching
- TCP/IP Protocol Analysis
- Advanced TCP/IP Protocol Analysis
- AppleTalk, AppleShare IP, and Mac OS/X Protocol Analysis Methods
- Wireless LAN Administration

Live Online Quick Start Program

WildPackets now offers one-hour online Quick Start Programs on using EtherPeek NX/EtherPeek and AiroPeek NX/AiroPeek, led by a WildPackets Academy Instructor. Please visit www.wildpackets.com for complete details and scheduling information.

Web-Delivered Training



Web delivery of courses is a time-efficient method for networking professionals to get the protocol analysis training they need while saving the expense of travel and out-of-office time. WildPackets Academy offers Web delivery of the “Foundations” and “AppleTalk” courses, delivered in five half-day segments. Students log in to the course through a PlaceWare conference and follow real-time presentation and live EtherPeek use with a WildPackets Academy instructor.

WildPackets Academy Testing Center

The WildPackets Academy Testing Center is designed for networking professionals to demonstrate proficiency in specific subject areas. The Pre-Test Study Guides, available at <http://www.wpatesting.com>, provide a detailed description of the test sections and the scope and depth of information presented in a test.

T.E.N. Video Workshop



The Technology, Engineering, and Networking Video Workshop is a 5-Session, 14-Module self-paced program including over 15 hours of lively lecture and animated graphics to explain difficult protocol analysis topics. Participants work through exercises and complete each Module by submitting answers to Challenge Questions to an NAX Mentor at WildPackets Academy. The Modules in the T.E.N. program are consistent with the material tested in the NAX certification program.

Network Consulting Services

WildPackets offers a full spectrum of unique professional support services, available on-site as well as through remote dial-in service, ready for integration with your network management strategy. Our professional consultants will provide protocol analysis expertise for your network troubleshooting, capacity planning, or baseline performance analysis needs. With our remote analysis services, we capture live traffic from your network and give you a general characterization of network performance and potential problems.

NAX Certification



A Network Analysis Expert certificate is confirmation by the network analysis experts at WildPackets Academy that an individual is fully qualified to perform Ethernet or 802.11 Wireless network protocol analysis. NAX Certification is completely vendor neutral and picks up where the retired CNX certification program left off in accrediting IT professionals with protocol analysis expertise. CNX-certified IT professionals can transition to the NAX certification program at no additional cost. Visit www.nax2000.com for complete details.

About WildPackets, Inc.

WildPackets, a privately-held corporation, was founded in 1990 with a mission to create software-based tools to simplify the complex tasks associated with maintaining, troubleshooting, and optimizing evolving computer networks. WildPackets' patented, core "Peek" technology is the development base for EtherPeek™, TokenPeek™, AiroPeek™, and the NX™ family of expert packet analyzers. All are recognized as the analysis tools of choice for small, medium, and large enterprise customers, allowing IT Professionals to easily maximize network productivity. Information on WildPackets, WildPackets Academy, Professional Services, products, and partners is available at www.wildpackets.com.

WildPackets, Inc.
1340 Treat Blvd., Suite 500
Walnut Creek, CA 94597
925-937-3200
www.wildpackets.com

