

AiroPeek NX and Wireless Security: *Identifying and Locating Rogue Access Points*

This tutorial will present a step-by-step method for identifying and locating rogue access points using WildPackets' 802.11 wireless LAN analyzers, AiroPeek NX.

A rogue access point is an access point that is not authorized in an 801.11 wireless environment. The presence of a rogue access point could be the innocent result of a group of users wanting to extend access to the wired Ethernet, or it could be an attempt on the part of an intruder to access network resources without authorization. In either case, it's important to identify the presence of an unauthorized access point on the network.

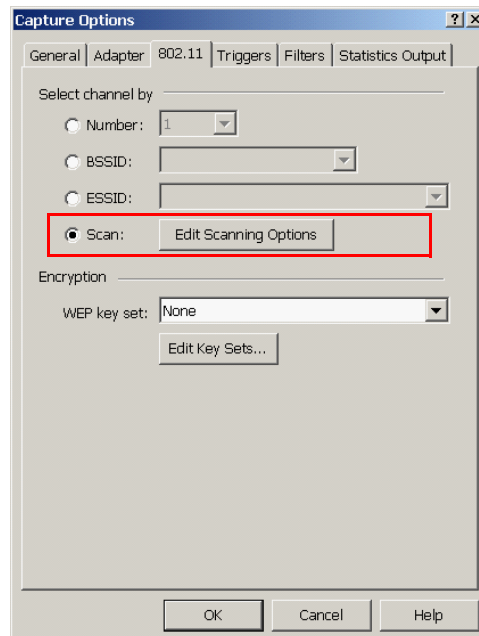
Identifying rogue access points

Scanning all the channels that your card can support will find all the APs (access points) that AiroPeek NX can hear.

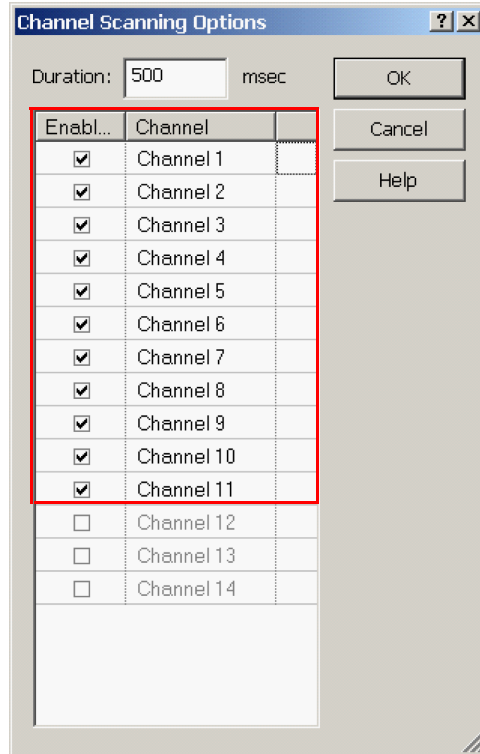
Step 1. Capture packets with channel scanning

Select **New...** from the **File** menu in AiroPeek.

This will open the **Capture Options** dialog. Click on the *802.11* tab.



Select the radio button next to *Scan*, and click on the *Edit Scanning Options* button. This opens the **Channel Scanning Options** window.



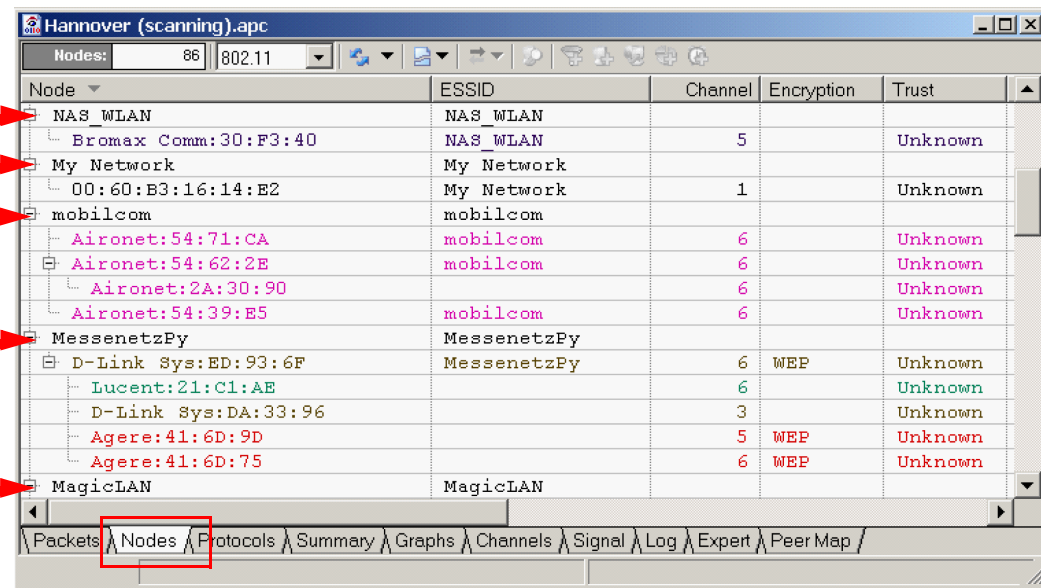
Tip Scan all channels, even if some channels are not legal in your country. A rogue AP might be on an illegal channel! Since AiroPeek NX does not transmit any data at all, you are not violating the law by capturing on illegal channels.

Step 2. Interpreting the Node Statistics

Start capturing packets by clicking OK at the bottom of the **Capture Options** dialog. Click the *Start Capture* button at the top of the Capture window. Packets will begin to be displayed in the **Packets** view of the Capture window.

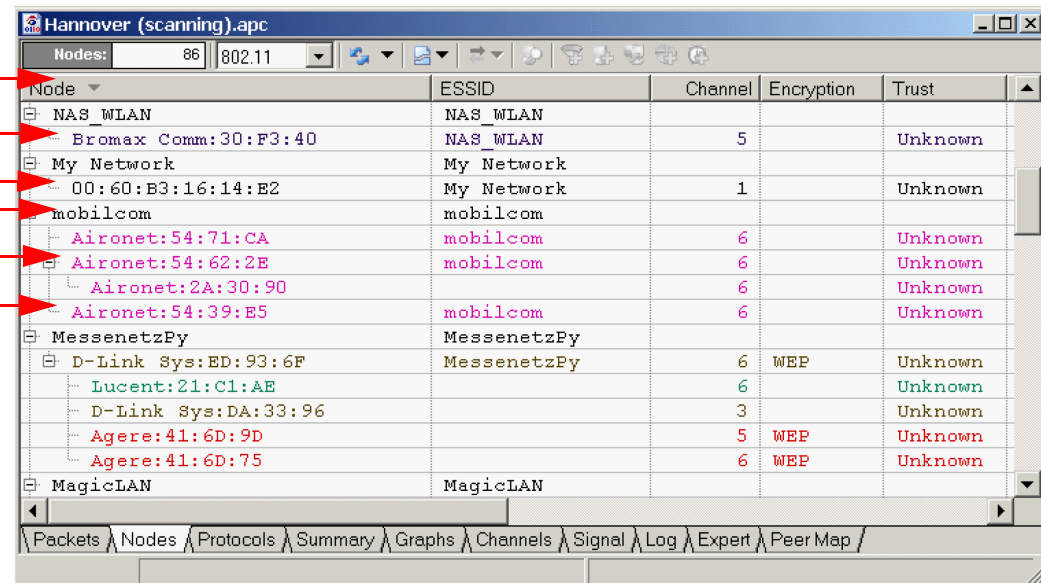
Open the **Nodes** view of the Capture window by clicking on the *Nodes* tab. There are three levels of nodes to observe here:

Level 1: ESSIDs



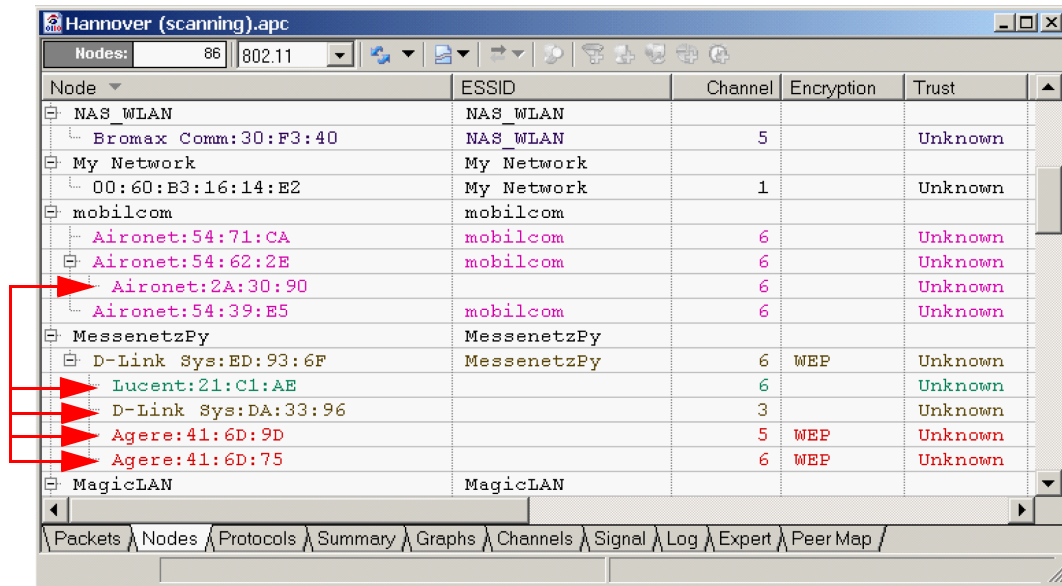
ESSIDs are Extended Service Set Identifiers, used to identify a group of access points (APs) belonging to the same Extended Service Set (ESS). An ESS is two or more access points connected to the same wired network or DS (distribution system).

Level 2: Individual Access Points



The individual access points mediate communications among the nodes and provide a connection to resources on the wired network. The BSSID (Basic Service Set Identifier) of such a group is typically the MAC address of the Ethernet card in the access point (AP) serving them.

Level 3: Wireless Stations

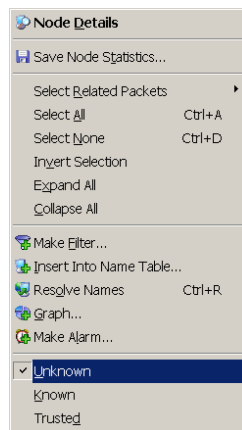


Each individual wireless station (STA) is ranged under the AP to which it most recently sent a packet.

Step 3. Set Trust Level in Node Statistics

You can assign a value of Trusted, Known, or Unknown to any node. Right-click on an Access Point or Station to set its trust level.

Note: The default value set for all nodes is Unknown. You must set which nodes are Trusted and Known.



Unknown

- You have not previously identified this node.
- This node might be a rogue.

Known

- This is a known node, but it is not trusted.
- Use this setting when a node is not a rogue, but it is not trusted either.

Trusted

- This node is not a rogue and is known to be safe.

For example, 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.

Step 4. Identify rogues in the Expert

Click on the *Expert* tab in the Capture window.

The screenshot shows the AiroPeek Expert window for a scan named 'Hannover (scanning).apc'. It displays 46 conversations analyzed and 2,484 problems detected. The main table lists problems between Net Node 1 (Client) and Net Node 2. Below this, a 'Problem Summary' table is shown with the following data:

Layer	Event	Count
Physical	Wireless Access Point - Rogue	54
Physical	Wireless Access Point - Too Many	12
Physical	Wireless Access Point - Weak Signal	26
Physical	Wireless Ad-hoc Detected	2

As noted above, the default value set for all nodes is Unknown. When AiroPeek sees an Unknown device, it treats the device as a rogue. Therefore, in the beginning you will see many “Rogue Stations” in the Expert. This is because you have not set which stations are Trusted and Known yet, not because these stations are rogues. After you have set the values for the Trusted and Known stations, the rogues will be clearly identified as Unknown in the *Trust* column of the **Nodes** view.

Locating rogue access points

As far as physically locating an intruder, it must be remembered that AiroPeek is a PROTOCOL analyzer, and not an RF test tool. Tools are available on the market that allow directional identification of RF signals. AiroPeek can quickly pinpoint the 802.11 channels that are in use in a particular environment. Knowing the channel usage in a particular location provides the information about the signal frequencies that are being used. By using a directional RF signal strength meter, it is possible to triangulate the location of an RF transmitter. Suffice it to say, a high-end directional RF signal strength meter (and hence, an expensive device) can pinpoint the location with great accuracy. More realistically, a lower-end tool will be able to provide the location of an intruder to within several meters.

In the same way that AiroPeek is most effective when used by an experienced, trained engineer, so too, an RF signal strength meter is simply a tool that is dependent on the user's expertise to provide accurate information. When one thinks about RF signal detection, it is easy to slip into pictures of clandestine operatives working for the intelligence agency; locating foreign intruders in sensitive networks. The realm of signal detection engineering and

methodology can seem somewhat “cloak-and-dagger” and the techniques, tools, and methodologies are, without a doubt, being used for national security.

The network manager of a commercial, corporate, or educational network should carefully weigh the need for RF-level network analysis, since this area of technology is significantly different from the LAN/WAN world of TCP/IP protocols with which we are all familiar.

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.

In addition to classroom-taught Network Analysis Courses, WildPackets Academy also offers:

- Web-Delivered Training
- On-site and Custom Courseware Delivery
- The (T.E.N.) Technology, Engineering, and Networking Video Workshop Series
- On-site and Remote Consulting Services
- Instruction and testing for the Network Analysis Expert (NAX™) Certification

For more information about consulting and educational services, including complete course catalog, pricing and scheduling, please visit www.wildpackets.com/academy. NAX examination and certification details are available at www.nax2000.com.

Live Online Quick Start Program

WildPackets 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.

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.

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

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

