OptiView™

Wireless Network Analyzer

Getting Started Guide

PN 2766304
October 2006

LIMITED WARRANTY AND LIMITATION OF LIABILITY

Each Fluke Networks product is warranted to be free from defects in material and workmanship under normal use and service. The warranty period for the mainframe is one year and begins on the date of purchase. Parts, accessories, product repairs and services are warranted for 90 days, unless otherwise stated. Ni-Cad, Ni-MH and Li-Ion batteries, cables or other peripherals are all considered parts or accessories. The warranty extends only to the original buyer or end user customer of a Fluke Networks authorized reseller, and does not apply to any product which, in Fluke Networks' opinion, has been misused, abused, altered, neglected, contaminated, or damaged by accident or abnormal conditions of operation or handling. Fluke Networks warrants that software will operate substantially in accordance with its functional specifications for 90 days and that it has been properly recorded on non-defective media. Fluke Networks does not warrant that software will be error free or operate without interruption.

Fluke Networks authorized resellers shall extend this warranty on new and unused products to end-user customers only but have no authority to extend a greater or different warranty on behalf of Fluke Networks. Warranty support is available only if product is purchased through a Fluke Networks authorized sales outlet or Buyer has paid the applicable international price. Fluke Networks reserves the right to invoice Buyer for importation costs of repair/replacement parts when product purchased in one country is submitted for repair in another country.

Fluke Networks warranty obligation is limited, at Fluke Networks option, to refund of the purchase price, free of charge repair, or replacement of a defective product which is returned to a Fluke Networks authorized service center within the warranty period.

To obtain warranty service, contact your nearest Fluke Networks authorized service center to obtain return authorization information, then send the product to that service center, with a description of the difficulty, postage and insurance prepaid (FOB destination). Fluke Networks assumes no risk for damage in transit. Following warranty repair, the product will be returned to Buyer, transportation prepaid (FOB destination). If Fluke Networks determines that failure was caused by neglect, misuse, contamination, alteration, accident or abnormal condition of operation or handling, or normal wear and tear of mechanical components, Fluke Networks will provide an estimate of repair costs and obtain authorization before commencing the work. Following repair, the product will be returned to the Buyer transportation prepaid and the Buyer will be billed for the repair and return transportation charges (FOB Shipping point).

THIS WARRANTY IS BUYER'S SOLE AND EXCLUSIVE REMEDY AND IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OR MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. FLUKE NETWORKS SHALL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES OR LOSSES, INCLUDING LOSS OF DATA, ARISING FROM ANY CAUSE OR THEORY.

Since some countries or states do not allow limitation of the term of an implied warranty, or exclusion or limitation of incidental or consequential damages, the limitations and exclusions of this warranty may not apply to every buyer. If any provision of this Warranty is held invalid or unenforceable by a court or other decision-maker of competent jurisdiction, such holding will not affect the validity or enforceability of any other provision.

4/04 Fluke Networks

PO Box 777

Everett, WA 98206-0777 U.S.A.

Table of Contents

Introduction

OptiView™Wireless Network Analyzer, hereafter referred to as the "analyzer", brings the ruggedness, portability, and ease-of use of OptiView Network Analyzer to wireless LANs. Whether you are designing your first wireless LAN deployment, detecting rogue access points, verifying a recent installation, monitoring or troubleshooting wireless connectivity problems, the OptiView Wireless Network Analyzer gives you the vision you need to manage your wireless network.

Note

The OptiView Wireless Network Analyzer is equipped with a wireless network access card that supports 802.11a/b/g specifications.

Before You Start

Safety Information

The OptiView Wireless Network Analyzer complies with:

- FCC part 64, class A
- FCC part 15, class A

Refer to the back of the Wireless LAN card for compliance symbols.

⚠Warnings

To avoid possible electric shock or personal injury, follow these guidelines:

- **Do not operate the product around explosive gas, vapor or dust.**
- **If this product is used in a manner not specified by the manufacturer, the protection provided by the product may be impaired.**

Contacting Fluke Networks Sales, Service, and Support Centers

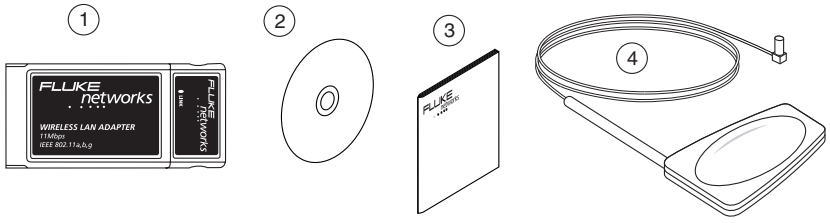
To order accessories or get the location of the nearest Fluke Networks distributor or service center, visit the Fluke Networks contact website at www.flukenetworks.com/contact. Send email to support@flukenetworks.com. For operator assistance in the USA, call 1-800-28-FLUKE (1-800-283-5853).

OptiView Wireless Network Analyzer Support

As a registered user, you are entitled to entry level product support, including three free telephone support incidents during the first 60 days of ownership, access to entry level online Knowledge Base library of product operation and Software information, and Web-based trouble ticketing. We will also be sending you Fluke Networks company and product information updates.

Please take the time to register your analyzer. A registration card is supplied in the shipping box. You can also register by going to www.flukenetworks.com.

OptiView Wireless Network Analyzer and Accessories



apo01f.eps

Item		Description
1	Wireless LAN Adapter	802.11a/b/g Wireless LAN PCMCIA card with antenna connection
2	CD-ROM	OptiView Wireless Network Analyzer CD-ROM. Contains installation software and documents.
3	OptiView Wireless Network Analyzer Getting Started Guide	Provides basic operating information, accessory part numbers, and specifications for the OptiView Wireless Network Analyzer.
4	Antenna	Triband flag directional antenna with Hirose connector.
	Registration Card	Fluke Networks can serve you best by registering online at www.flukenetworks.com. If you cannot register online, please fill out and return the supplied registration card.
	Warranty Card	Factory 1 year warranty.

Figure 1. The OptiView Wireless Network Analyzer and Supplied Accessories

Installing the OptiView Wireless Network Analyzer Software

If the OptiView Wireless Network Analyzer icon does not appear on your OptiView Series II or Series III Integrated Network Analyzer desktop, you will need to install the software. There are three steps involved in the installation:

- Move the self-extracting software file onto the analyzer's hard disk
- Install the software on the analyzer
- Install the Wireless LAN PCMCIA card

Note

The OptiView Wireless Network Analyzer software must be installed BEFORE installing the 802.11a/b/g Wireless LAN Card.

Moving the Software to Your OptiView Integrated Network Analyzer

There are three methods for moving the software file:

- Download the software file from the Fluke Networks Web Site directly to the analyzer
- Copy the file from the OptiView Wireless Network Analyzer CD to your analyzer using an external USB CD-ROM drive
- Copy the file from your OptiView Wireless Network Analyzer CD to your PC, and then transfer the file to the analyzer using one of the methods listed below:
  - Use a direct point-to-point connection
  - Transfer the software file to the analyzer using the analyzer's TFTP Server software
  - From the analyzer, use Microsoft Networking to map a drive on the PC, and copy the file to the analyzer (analyzer and PC must be in same subnet)

Once the software file is on your analyzer, you will need to install it as described in ***Installing the Software on the Analyzer***.

Downloading the Software File from the Fluke Networks Web Site Directly to the OptiView Integrated Network Analyzer

If your OptiView Integrated Network Analyzer is connected to a network that has Internet access, perform this procedure:

1. Connect the analyzer to the network and correctly configure the IP configuration. Refer to the analyzer documentation for help if needed.
2. Start your web browser and go to the www.flukenetworks.com web site.
3. Select the **Support and Downloads** tab and follow the instructions to select and download the correct version of Wireless Network Analyzer software.
4. You are now ready to ***Install the Software on the Analyzer***.

Copying the Software File from the OptiView Wireless Network Analyzer CD to the OptiView Integrated Network Analyzer using an external USB CD-ROM drive

Follow this procedure to move the file from a USB CD-ROM drive:

1. Connect the drive to the OptiView Integrated Network Analyzer's USB port.
2. Insert the OptiView Wireless Network Analyzer's CD into the CD-ROM drive.
3. Use the OptiView Integrated Network Analyzer's Windows Explorer to navigate to the CD and copy the file OPVWNA-V3.EXE (located in the ...\sw directory) from your PC to the analyzer (recommended directory is d:\temp).
4. You are now ready to ***Install the Software on the Analyzer***.

Transferring the Software from your PC to the OptiView Integrated Network Analyzer

These methods are described in the online Help. Online Help is available from the Startup menu of the OptiView Wireless Network Analyzer CD. Insert the CD in your PC and it will automatically load the Startup menu.

Installing the Software on the Analyzer

After the file OPVWNA-V3.EXE has been copied to the analyzer (preferably to the D: drive), perform the following steps to complete the installation:

Note

The Wireless Network Analyzer PCMCIA Card must NOT be installed in the analyzer during the software installation. After the software installation, the card can be inserted into the PCMCIA slot. Windows will then detect the card and add it as new hardware using the correct driver.

1. Use the Integrated Network Analyzer's Windows Explorer to navigate to the directory where the OPVWNA-V3.EXE file has been stored.
2. Double-click on the OPVWNA-V3.EXE file to run it.
3. Follow the InstallShield Wizard instructions to install the software. Reboot the analyzer as indicated in the InstallShield Wizard.

Note

If a previous version of the application is already installed, follow the InstallShield instructions to remove it. After rebooting the analyzer to finish the removal, start at step 1 to install the OPVWNA-V3.EXE file.

4. Once the analyzer reboots, stop the OptiView Integrated Network Analyzer application if it is running.
5. Follow the instructions in the next section ***Installing the Wireless LAN Card***.

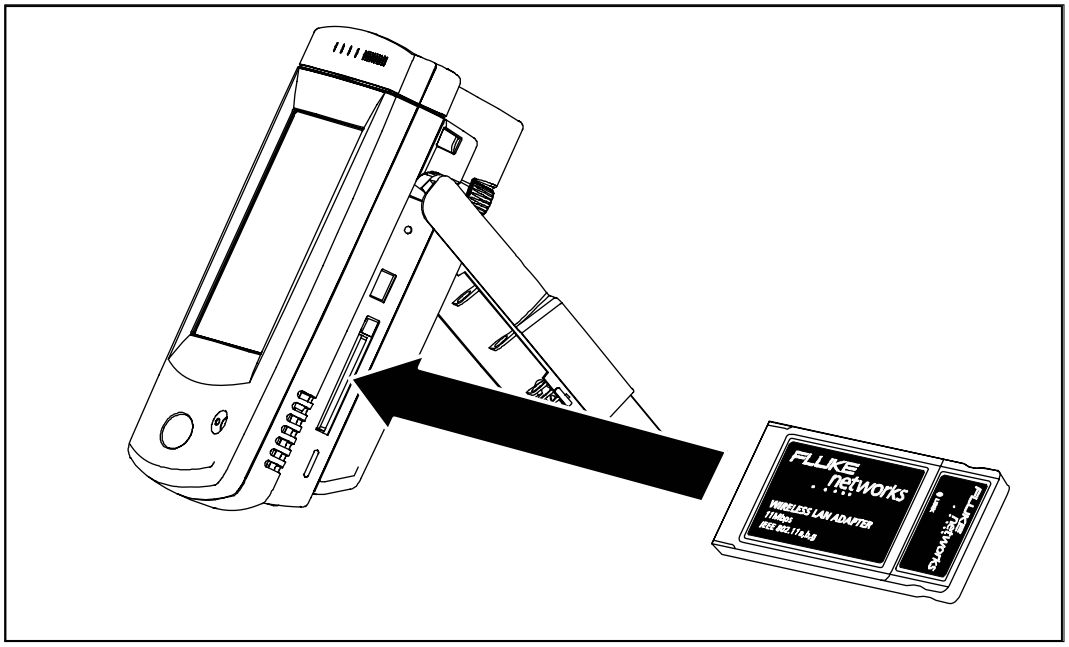
Installing the Wireless LAN Card

Notes

The OptiView Wireless Network Analyzer software must be installed BEFORE installing the 802.11a/b/g Wireless LAN Card.

You must use the Wireless LAN PCMCIA card that came with your Version 3 software; previous version LAN cards will not work with Version 3.

The WLAN PC Card is installed in the PC Card (PCMCIA) slot located on the right side of the OptiView Integrated Network Analyzer. When inserting the card, make sure it is properly aligned while sliding it into the card slot. It should slide in freely. Do not force it into the slot.



apo06f.eps

Figure 2. Wireless LAN Card Installation

Note

The LAN card may interfere with the operation of the Integrated Network Analyzer's bail. Refer to the section ***Installing a Replacement Bail on an OptiView Analyzer*** *for information on replacing the bail.*

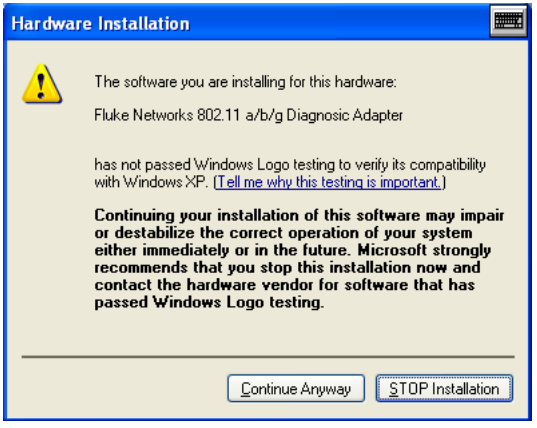
On Windows XP Service Pack 2, with the Windows Firewall turned **On**, you will be prompted with the following screen the first time the WLAN card is inserted:

apo30s.bmp

Figure 3. Forcing Windows to Look for the WLAN Card Driver Locally

Select **No, not this time**, and press **Next**.

You will also be prompted with the following message telling you that the driver has not passed Windows testing. Press **Continue Anyway** to complete the installation:



apo31s.bmp

Figure 4. Hardware Installation Message

Using the OptiView Wireless Networks Analyzer

Starting the OptiView Wireless Network Analyzer

On the Windows desktop, select the OptiView Wireless Network Analyzer (OPVWNA-V3) icon to launch the software.

Note

*The Windows Firewall should be turned **off** to enable discovery. If the firewall is **on**, you will be prompted with the following screen after launching the software:*

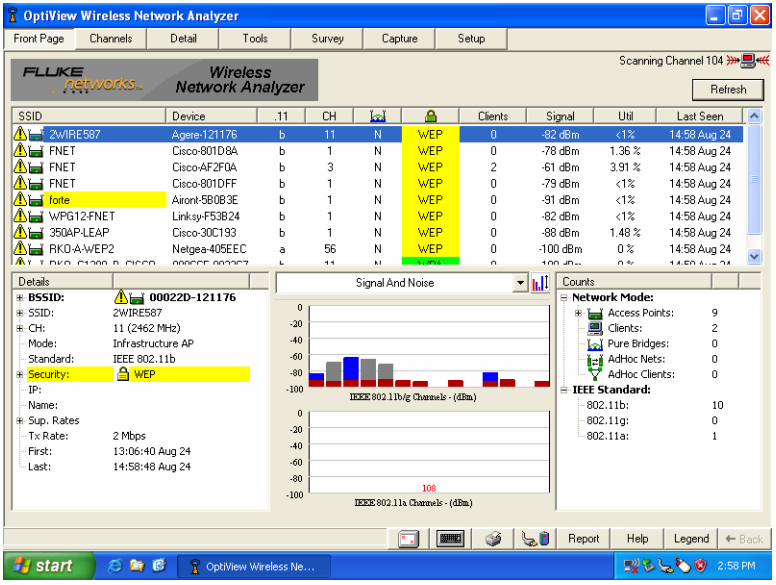
apo32s.bmp

Figure 5. Allowing Discovery Through the Windows XP Firewall

*Select **Unblock** to allow discovery by the OptiView Wireless Network Analyzer on the wireless network. If you select **Keep Blocking**, no discovery will take place.*

*The firewall security settings are configured in the **Windows Security Center** screen. Select the*  *icon on the taskbar to open the **Windows Security Center** screen. At the bottom of this screen, select **Windows Firewall**. The **Exceptions** tab allows you to enable/disable the OptiView Wireless Network Analyzer program block. Enable the checkbox next to the **OptiView WNA** entry to unblock the firewall.*

Upon a successful launch of the software, the OptiView Wireless Network Analyzer Front Page will appear as shown below. Monitoring of your WLAN is automatically started. Devices present on your wireless network are discovered and displayed.



apo33s.bmp

Figure 6. OptiView Wireless Network Analyzer Front Page

1. The top of the screen gives immediate visibility into the security level and potential security vulnerabilities. You can use the pull-down menu above the device list to filter the list by device type or network configuration.

Notes

IP and Name information can be discovered if the analyzer has been configured to autolink using a default SSID. See the ***Initial Setup*** *section later in this guide for more details.*

The color coding and icon legend for the ***Front Page*** *screen and throughout the user interface can be viewed by pressing the* ***Legend*** *button located at the bottom of the screen.*

2. Highlight an entry in the device list and key configuration parameters are displayed in the lower left section.
3. The overall network health is displayed in the lower center section. The application continuously monitors 802.11a/b/g channels and reports key statistics important for maintaining your network (e.g. signal strength, retry rates, signal-to-noise, etc.). Use the pull-down menu to display the parameters of choice.
4. The overall network summary is displayed in the lower right. It provides statistics on network device types, authorization levels, and security.

5. Use the row of tabs at the top of the **Front Page** to gain access to detailed information about your wireless LAN environment, troubleshooting tools, and tests that are available in the product. The online Help provides information about each feature.
6. Reports are available from most of the screens to aid in documenting your network.

Initial Setup

While the analyzer provides information about your wireless network as soon as it is invoked, you can improve the quality and detail of the information presented by configuring the following parameters:

- **Authorization** – the analyzer automatically tags any newly discovered device as Unauthorized. You can specify devices as **Authorized** or **Neighbor**. This allows you to easily identify rogue Access Points or unwanted clients. Previously configured authorization lists may be imported for use by the analyzer.
- **Default SSID** – as part of the ongoing discovery process, the analyzer will periodically establish link to an AP that is configured with the same SSID as the default SSID and perform active discovery. During active discovery, IP addresses and DNS names are discovered.
- **Wireless Security** – you will need to configure security settings for any device that has its security settings configured and to which you want to establish link. Whether a device's security has been configured and the type of security is indicated in the security column on the **Front Page**.
- **Radio and Global Settings** – you may need to change the Country settings, which determine the wireless channels that the analyzer will use, and to calibrate the Signal Strength settings of the radio card. You can also make other configuration changes that affect how the analyzer works and presents data.
- **Import Device Names** – you can import a file of device names that can be used to seed the analyzer's database with recognizable device names.

Authorization

The icons shown to the left of the SSID list are designed to provide immediate visibility into potential use of your network by unauthorized devices. Device authorization is configured in the Setup | Authorization screen.

 indicates the device is set to **Authorized**

 indicates the device has been set to **Neighbor**

 indicates the device has been set to **Unauthorized**

The **Setup | Authorization** screen allows you to configure the application to aid in the detection of rogue Access Points or Clients. All discovered devices are initially classified as **Unauthorized** ⚠ (rogue). You can change the classification to **Authorized** ✓ or **Neighbor** ✓.

Neighbor ✓ is a device that you frequently see but is not authorized on your network. A discovered device owned by an adjacent company is typically classified as a Neighbor device. This allows you to avoid concern about it being a rogue device while still monitoring it for changing signal strength or channel usage that may impact your network performance.

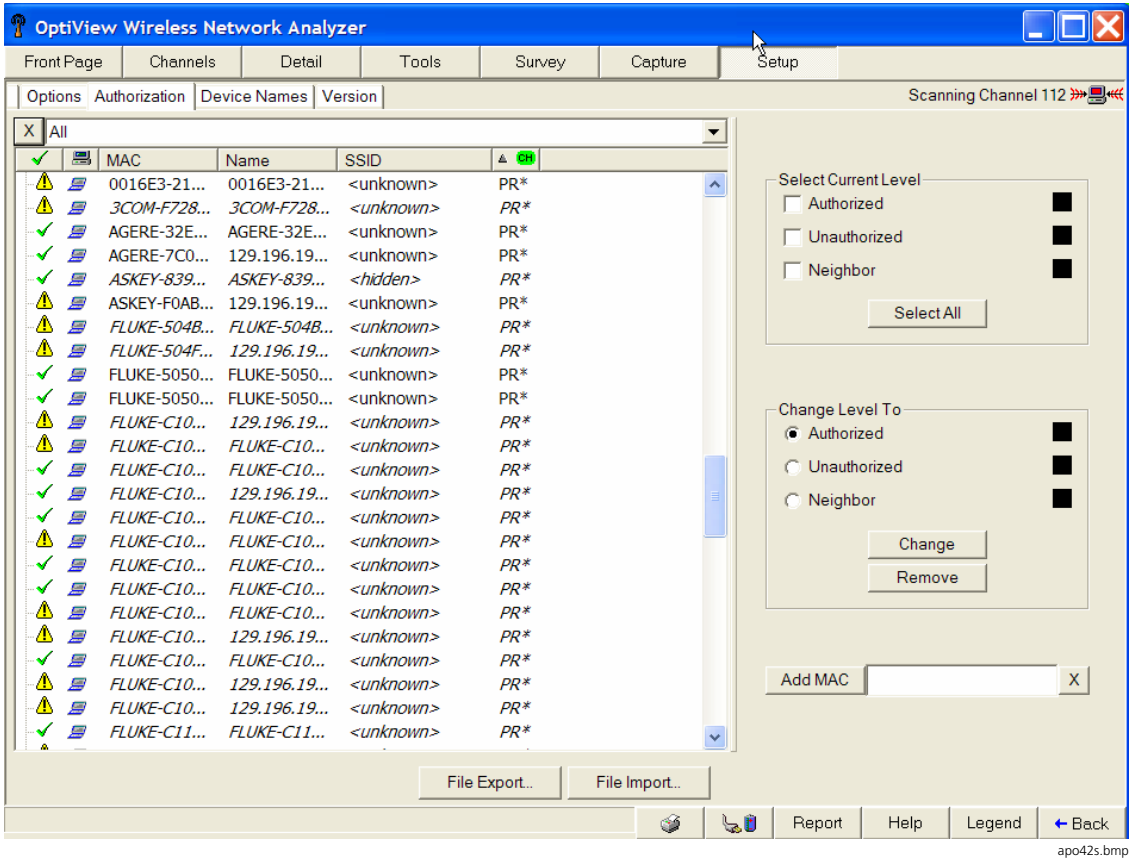


Figure 7. Authorization Screen

The Authorization screen shows a table of all the discovered devices and their authorization level.

To change the authorization assignment of a single device or multiple devices:

1. Select the device(s) to change. You can individually select a device by clicking on the entry in the table. Select additional devices by holding down the **Ctrl** key and clicking on each device. Select a block of devices by selecting the first device and then hold down the **Shift** key and click on the last device in the block. All devices in between will be selected.

   You can use the **Select Current Level** field to select a category of devices. Use the radio button to select one or more categories and then press the **Select All** button. The selected categories of devices will be highlighted. You can then deselect individual devices by using the **Ctrl** key while clicking on each device.

2. After selecting the devices to be changed, click on the appropriate radio button in the **Change Level To** field. Select the **Change** button to apply the change. You can use the **Remove** button to undo the changes.

3. You can also import a list of devices with their authorization level already defined. From the **Setup** tab, press the **Import** button and follow the instructions on the screen.

4. You can export the authorization list from the analyzer or you can use Microsoft WordPad to create a list of devices and their authorization levels and then import it into the instrument. The file must have a .acl extension and be saved with no formatting.

   An example of the file format is:

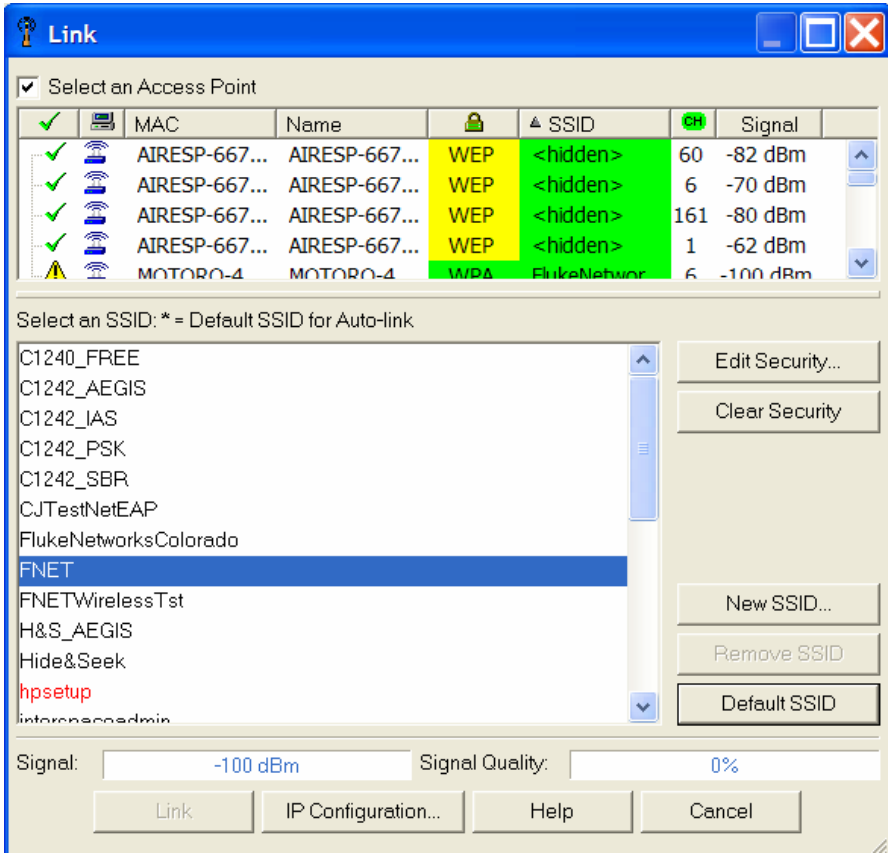
```
// FLUKE Networks Wireless Network Analyzer access control list

0001F4EC856F authorized
00022D2D8513 authorized
00022D32EA56 neighbor
00022D7C009D authorized
00022D80AE7B authorized
00022D86EEEC unauthorized
00045AC91363 neighbor
00062549D761 unauthorized
```

Default SSID

In order for the analyzer to discover complete details about your wireless network and its devices, you must configure security settings and designate a default SSID. As part of its active discovery mode, the instrument will link to

an AP using the configured default SSID and perform active network discovery. During active discovery, IP addresses and DNS names are identified.

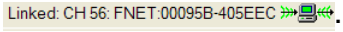


apo43s.bmp

Figure 8. Define Default SSID

To configure the Default SSID:

1. Select **Tools | Link.**
2. Highlight an SSID in the **Select an SSID** window.
3. Press the **Edit Security** button. Use the radio buttons on the **Security Settings** screen to select **Legacy WEP** or **WPA/802.1X** authentication.
4. Configure the security settings to match the security settings of the SSID. Press **OK** when finished to save the configuration.

5. Press the **Default SSID** button.
6. The default SSID is designated with an ***** next to the name.
7. Press the **Link** button to test the configuration settings. The analyzer will attempt to establish link with an AP that has the selected SSID. If successful the status indicator in the upper right corner will show 

.
8. The analyzer will stay linked until you exit the screen.

Note

You can set the security settings for multiple SSIDs, save the configurations and alternately select one as the default SSID so that you can test different networks. In some cases, you can save multiple security keys or ID's for a single SSID and alternately designate which key or ID that you want to use.

Wireless Security

You will need to configure security for any device that has its security settings configured and to which you want to establish link. Whether a device's security has been configured and the type of security is indicated in the security column of the **Front Page**.

Configure security as follows:

1. Select the **Tools** | **Link** tab and then press the **Link** button. The **Link** screen as shown in Figure 8 is displayed.
2. Highlight an SSID in the **Select an SSID** list and press the **Edit Security** button.

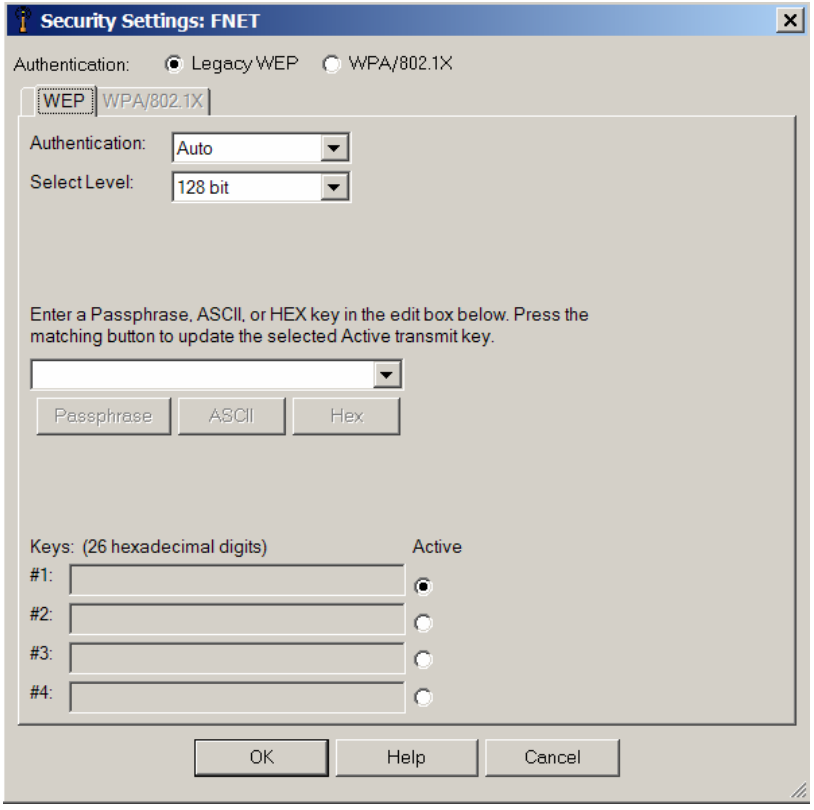


Figure 9. Configure Security Settings

3. Use the radio buttons in the **Authentication** field to select either **Legacy WEP** or **WPA/802.1X** security.
4. Configure the security keys to match the security settings of the SSID and will allow the analyzer to connect to an AP configured with the selected SSID.
5. Press **OK** when done.
6. After you have configured security for an SSID, you can verify that it works by pressing the **Link** button (while the SSID is highlighted) located at the bottom of the **Link** screen. The analyzer will link to an AP configured with the SSID. The analyzer will remain linked until you change screens. You can also select a specific AP in the **Select an Access Point** list and link directly to it.
7. For more information on Wireless Security, refer to the online Help.

Radio and Global Settings

Use this screen to change the radio card parameters and other settings that affect the performance of the analyzer and how data is presented. This screen is accessed by selecting Setup | Options.

Radio Settings

- **Mode** – Use the pull-down menu to select the type of wireless traffic that you want to view, **802.11a**, **802.11b/g**, or **Mixed**. **Mixed** includes all three channels.
- **Tx Rate** – Use the pull-down menu to select the transmission rate that the analyzer will use when linking with the wireless network.
- **Country** – Use the pull-down menu to select the country of operation. This determines the valid channels that the analyzer uses. Channels that are valid for a country are displayed in red throughout all screens.

Caution

Based on the country selection, only those channels that are allowed for the selected country are displayed as valid channels. IT IS YOUR RESPONSIBILTY TO USE ONLY VALID CHANNELS.

- **Signal Strength dBm Adjustments** - Use this to normalize the signal strength readings. This is useful when trying to compare the results from the analyzer with the results from another device.

Global Settings

- **Enable Active Channel** and **Active SSID Scan** – Active scanning allows for a richer discovery through analyzer initiated queries to devices. Clear this setting to disable the wireless card from transmitting and the analyzer from actively querying devices. The analyzer will use only passive discovery when this setting is disabled. Refer to the next section ***Wireless Discovery States*** for more information on Active Scanning.
- **Enable Vendor Prefix for MAC** - When this is selected, the vendor prefix (if known) is displayed along with the last 3 bytes of the MAC address. When this is not selected, the entire MAC address is displayed as a hexadecimal value.
- **Show Signal Strength in dBm** - When this is selected, signal strength is displayed in dBm units. When this is not selected, the signal strength is displayed as a percentage.

- **Enable Control Frame Packet Parsing** – Turns on and off the display of control frames in the Top Talkers and Packet Stats screens.
- **Enable Sounds for Wireless Discovery Events** – When enabled, SSIDs that become inactive for a specified time (see next item), are discovered for the first time, or are re-discovered from an inactive state will cause a beep to occur.
- **Remove Devices not seen for <time>** - This is the length of time that a device can be inactive before the device will be removed from the list of discovered devices. Current inactive devices are shown in red in the Link SSID and Authorization screens.
- **Language** – Use the pull-down menu to select the language for on-line help.

Import Device Names

Refer to the online help for more information on importing lists of device names into the analyzer.

Wireless Discovery States

Active Channel Scan is the default state for the **Front Page**, **Channels** and **Survey** screens.

In **Active Channel Scan** mode, the wireless radio card steps (sweeps) through all channels (250 msec each channel) and then performs an active scan (sends out a probe request from for Access Points to respond) at the end of sweep. To disable the active phase option while scanning, navigate to the **Setup** | **Options** screen and disable **Enable Active Channel Scan**.

Linked mode is the active state for **Tools** screens. When you leave any of the Tools screens, link with the SSID will be disabled. On the **Front Page** screen, link will periodically be re-established for about 15 seconds with the default and configured SSID, and then resume Active Channel Scan. To enable active discovery of WLAN devices, select the default SSID for autolink from the list and then select the **Default SSID** button. The configured default SSID will be indicated by an ***** next to the SSID name. Green text indicates the SSID is the active default SSID. You may also select a default SSID from the **Detail** | **Authorization** screen. Highlight an SSID and select the **Default SSID** button.

Monitor mode is the active state for all **Detail** screens except the **Top Talkers** screen. In monitor mode, the WLAN card is parked on a particular channel, and all packets received on that channel are processed for passive discovery of Access Points and Clients.

Installing a Replacement Bail on an OptiView Analyzer

With the bail nearly closed on the analyzer, grip one side of the bail where it pivots on the analyzer and gently pull out. It should pop out with little effort. Do the same for the opposite side. See Figure 10 below.

Caution

The bail must be nearly shut before removing or installing, or damage may occur to the analyzer case.

With the new analyzer bail placed in the nearly shut position, install it one side at a time by placing the pivot arm in the pivot hole on the analyzer and gently pushing until it pops into the hole and pivots freely. Do the same for the other side.

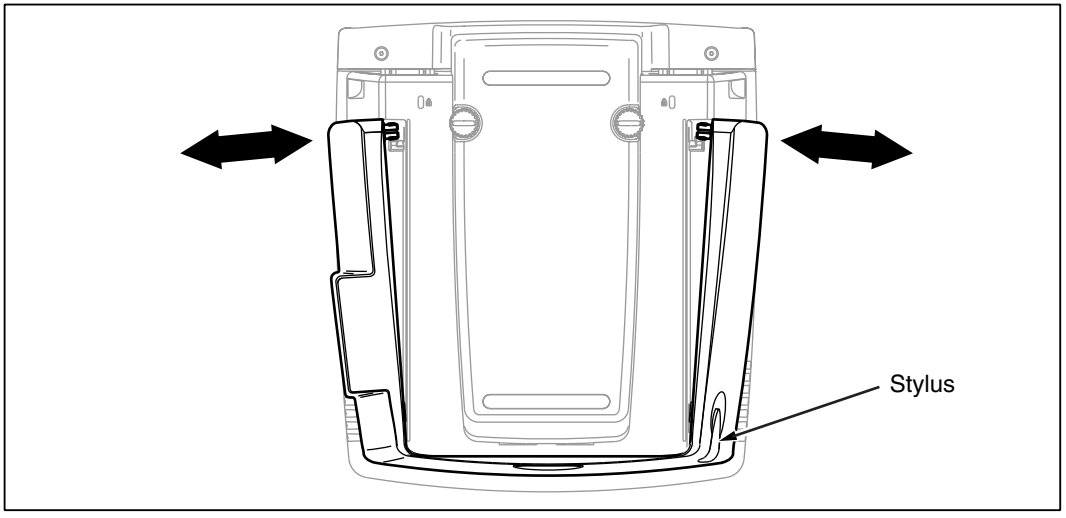


Figure 10. OptiView Wireless Network Analyzer Bail Removal

Troubleshooting Your Analyzer

Resetting and Powering the Analyzer Completely Off

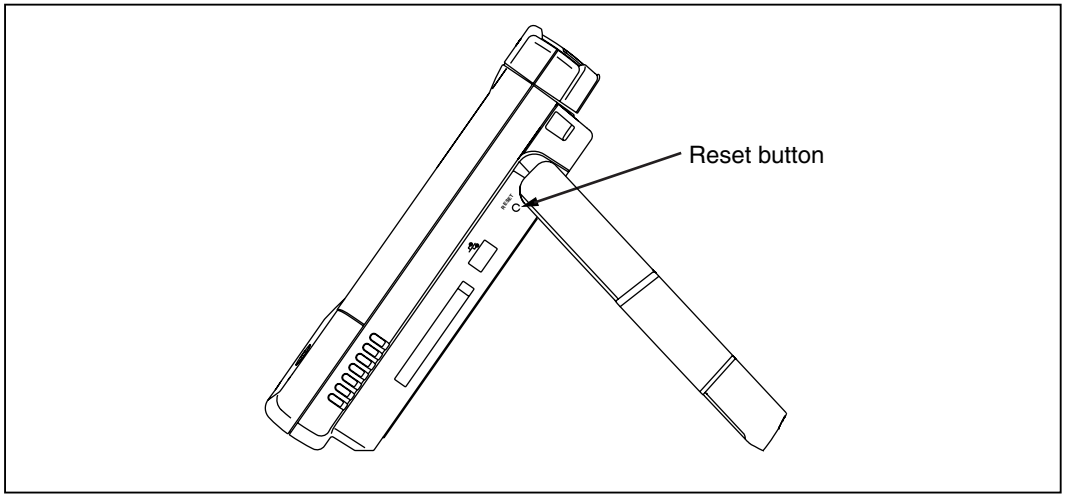
If you suspect the Windows environment has locked up, you may have to reset the OptiView Integrated Network Analyzer. This is done by pressing the **Reset** button. If you are not sure if the Windows environment or the analyzer (hardware) has locked up, you may have to completely power down the analyzer by forcing the power off as described below.

Resetting the Analyzer

The **Reset** button resets the Windows portion of the analyzer without shutting down the data acquisition board. The **Reset** button should only be used if the Windows environment has stopped responding.

Forcing Power Off

Power can be forced off by pressing and holding the **On/Off** button for approximately 7 seconds.



apo05f.eps

Figure 11. Reset Button Location

Before Calling Technical Support

Before calling technical support, you can perform these basic analyzer troubleshooting steps to pinpoint many problems:

Do you suspect Windows has locked up?

If yes, press the **Reset** button.

Do you suspect the analyzer has locked up?

If yes, completely power-down the analyzer. See **Forcing Power Off** on page 21.

Does the analyzer power-up?

Connect the AC adapter/charger to determine if the internal battery (or internal and external batteries) is the culprit. The analyzer will not power-up if the batteries are completely discharged.

If the analyzer only powers up with the AC adapter connected, the internal battery may be completely discharged.

The external battery has a charge indicator on the underside of the battery pack. The external battery will need to be removed from the analyzer to view the charge indicator. Press the charge indicator button to determine if the external battery is charged.

Does the Windows wireless setup not support your network's security settings?

If your analyzer is running Windows XP Service Pack 1, and the Windows security settings do not support your wireless network, you may have to go to http://support.microsoft.com/default.aspx?scid=kb;en-us;826942 and download the wireless patches. These patches are included in Service Pack 2.

Known Issues/Limitations

1. When doing a capture within a WPA environment, the analyzer can decrypt Broadcast frames (UI will ask you to link). Frames not destined for the analyzer can not be decrypted.
2. If you are analyzing multiple Access Points with different security configuration (WEP keys, WPA certificate, WPA passphrase, User ID and password), IP address, Name and Packet Stats will not be discovered for those devices with a different WEP key than the one currently set in the OptiView Wireless Network Analyzer **Setup** | **Configuration** screen.
3. In the **Capture** screen, the **Source/Destination MAC** filter supports Access Point, and Access Point to client filtering. It does not support client-to-client filtering. Entering two client MAC addresses will yield unexpected results.

4. Decoder issue: Shows incorrect **Source/Destination MAC** addresses if the option "Configuration, Display, Display Network Address" is not checked.

Using the Online Help System

The help system is an integral part of the OptiView Wireless Network Analyzer. While using the analyzer user interface, help can be accessed by selecting the **Help** button located on the bottom-right of the user interface screen.

When the Help is launched, the current screen topic is displayed. You can also select a topic from the **Contents** tab (left pane), choose an **Index** entry, or perform a full text **Search** on any help topic or term.

The **Hide** button collapses the left pane of the help screen giving you more room to view Help topics. The **Hide** button is replaced by the Show button. The **Show** button expands the left pane of the Help screen.

You can also press the **Back** and **Forward** buttons to move through the sequence of previous viewed topics.

The **Print** button allows you to either print the selected topic or print the selected heading and all subtopics.

WLAN Card Specifications

- Frequency Range:
  - USA: 2.412 - 2.462GHz, 5.15 - 5.35GHz, 5.725 - 5.825GHz, 2.400 - 2.483GHz
  - Europe: 2.412 - 2.472GHz, 5.15 - 5.35GHz, 5.47 - 5.725GHz, 2.400 - 2.483GHz
  - Japan: 2.421 - 2.484GHz, 5.15 - 5.25GHz, 2.400 - 2.483GHz, 4.90 - 5.091GHz, 5.15 - 5.25GHz
  - China: 2.412 - 2.484GHz, 5.725 - 5.85GHz, 2.400 - 2.483GHz
- Modulation Technique:
  - 802.11b/g: DSSS (DBPSK, DQPSK, CCK), OFDM for data rate > 20 Mbps
  - 802.11a: OFDM (BPSK,QPSK, 16-QAM, 64-QAM)
- Host Interface: Cardbus form factor with 32-bit interface
- Channels Support:
  - 802.11b/g
    US/Canada: 11 (1 - 11)
    Europe: 13 (1 - 13)
    France: 4 (10 - 13)
    Japan: 14 (1 - 14)
    China: 13 (1 - 13)
  - 802.11a
    US/Canada: 12 non-overlapping channels (5.15 - 5.35GHz, 5.725 - 5.825GHz)
    Europe: 19 non-overlapping channel (5.15 - 5.35GHz, 5.47 - 5.725GHz)
    Japan: 4 non-overlapping channels (5.15 - 5.25GHz)
    China : 5.725 - 5.85 GHz
- Operating Voltage: 3.3V +/- 5%

- Power Consumption:

	802.11a	**802.11b**	**802.11g**
Continuous Tx:	490-510mA @18dBm	570-590mA @18dBm	610-640mA @18dBm
Continuous Rx:	340-350mA	360-380mA	420-440mA
FTP Tx :	420-440mA	510-530mA	530-545mA
FTP Rx :	400-420mA	470-485mA	490-510mA
Standby mode:	360-380mA	440-450mA	450-470mA
Power saving mode:	50mA	50mA	50mA
RF Kill :	40mA	40mA	40mA

- Output Power:

  - 802.11b/g 18 dBm peak power
  - 802.11a
    US : 5.150 - 5.250: 15 dBm, 5.250 - 5.350: 18 dBm, 5.470 - 5.725: not allowed,
    5.725 - 5.825: 17 dBm
    Europe : 5.150 - 5.250 and 5.250 - 5.350: 18 dBm, 5.470 - 5.725: 17 dBm,
    5.725 - 5.825: Not allowed.
    Japan : 5.150 - 5.250: 18 dBm, 5.250 - 5.350: not allowed,
    5.470 - 5.725: not allowed, 5.725 - 5.825: not allowed

- Operating Distance:

  - 802.11a
    Outdoor: 40m@72Mbps,85m@54Mbps,250m@48Mbps,310m@36Mbps
    Indoor:20m@72Mbps,25m@54Mbps,35m@48Mbps,40m@36Mbps
  - 802.11b
    Outdoor:300m@11Mbps,465m@5.5Mbps,500m@2Mbps,515m@1Mbps
    Indoor: 60m@11Mbps,70m@5.5Mbps,83m@2Mbps,85m@1Mbps
  - 802.11g
    Outdoor: 82m@54Mbps,100m@48Mbps,300m@36Mbps
    Indoor:20m@54Mbps,25m@48Mbps,35m@36Mbps

- Operating System: Windows® 98SE, ME, 2000, XP
- Dimension: 119mm (L) * 54mm (W) * 9.4mm (H)

- Security:

  - 64-bit, 128-bit, 152-bit WEP Encryption
  - 802.1X Authentication
  - AES-CCM & TKIP Encryption

- Operating Mode: Infrastructure & Ad-hoc mode
- Transfer Data Rate:
  - 802.11b/g: 11, 5.5, 2, 1 Mbps, auto-fallback, up to 54 Mbps
  - 802.11g (Super mode): up to 108 Mbps
  - 802.11a (Normal mode): 54, 48, 36, 24, 18, 12, 9, 6Mbps, auto-fallback
  - 802.11a (Turbo mode): 108,96,72,48,36,24,18,12 Mbps, auto-fallback
- Operating Temperature: 0 – 70 degrees Celsius
- Storage Temperature: -20 – 80 degrees Celsius
- Wi-Fi Alliance: WECA Compliant
- WHQL: Microsoft® 2000, XP Compliant
- FAA: S/W audio On/Off support
- EMC Certificate:
  - FCC part 15 (USA)
  - Pre IC RSS210 certified
  - Telec (Japan)
  - ETSI, EN301893, EN60950 (Europe)
- Media Access Protocol : CSMA/CA with ACK architecture 32-bit MAC
- Embedded Antenna : Embedded Dual Band Antenna
- External Antenna:

  - VSWR 2.0
  - Antenna Gain:

    2.4GHz - 2.485GHz: 2dBi

    4.9GHz - 5.875GHz: 3.5dBi

  - Cable Length: 120cm