Tequipment.NET USA
205 Westwood Ave
Long Branch, NJ 07740
1-877-742-TEST (8378)
Fax: (732) 222-7088
salesteam@Tequipment.NET

1 Introduction

Your Fluke Networks EtherScope(tm) Network Assistant instrument is a Wireless LAN (WLAN) troubleshooting and maintenance tool that provides an efficient, task focused user interface that includes an effective set of automated tests and tools in a small and affordable product.

The instrument is designed to automatically provide quick visibility into the state of your wireless network. A series of automated tests is started by plugging in the radio card and turning on the power. It is an easy task to "drill down" from the main **Test Results** screen to get more detailed information about the status of your network. Some information about your network is discovered without any instrument configuration, however, to use all of the features of the instrument it is necessary to configure it. Refer to the topic Configure the Network Assistant for more information.

As the automated tests are running, the Test Results screen provides information about the status of each test. A synopsis of the highlighted test is provided in the left preview pane. The right pane displays the name of each test and reports its status. The icons that appear to the right of each test give you a visual indication of the progress and status of each test:

- Running
- Not running
- Completed and passed ✓
- Completed and failed 🚫

Highlight a test and tap the **Details** button to get more information about a particular test.

2 Navigating the User Interface

The EtherScope user interface is designed to provide as much relevant information as possible on each screen. Information is provided in a hierarchical format, where general information is shown at the top level screen and an increasing amount of detailed information is shown at the lower level(s). On most screens, a summary view of a selected test is shown on the left side Preview pane and detailed information is provided in the right pane.

Here are some tips for navigating the user interface:

- Use the stylus to make a selection on the screen. Tap a hyperlink or a button to make a selection.

- All blue text represents a hyperlink to a separate, related screen within the user interface.

- The Title bar is the banner at the top of the screen.

- The Status bar is at the very bottom of the screen.

- The Task bar is above the Status bar at the bottom of the screen.

- Tap the EtherScope icon , located on the left side of the Title bar, for a drop-down list of tests. Select a test to go directly to that screen. You can also select a test from the **Test Results** screen. Tap the entry in the list to highlight the test and the preview panel shows summary results. Tap the **Details** button to go to the test screen.

© 2004 - 2008 Fluke Corporation

- Select one of the Operations buttons (e.g. **Details**, **Report**) located on the Task bar at the bottom of the screen to perform tasks specific to a test. Operations buttons are disabled when they are not applicable to a test.

- Tap **Connection** on the **Test Results** screen and select the **Details** button to navigate to the Instrument Settings screen, or tap the EtherScope icon ▣ in the top left corner and select **Instrument Settings**.

- Tap a column heading to sort data by that value.

- Tap the ⊞ icon in a list to expand and view more tests or details. Tap the ⊟ icon to collapse the expanded list.

- Tap the **Keyboard** icon ⌨ , located on the Status bar at the bottom of the screen, to bring up the keyboard and tap the icon again to put it away. The keyboard allows both text and numeric entry.

- Tap the **Scan** button on the Task bar for a shortcut to the **Wireless Instrument Settings - Wireless Security** screen.

- Tap the Report button on the Task bar to generate and save a report of a test. Reports are stored on compact flash and can be viewed on your EtherScope Network Assistant or on a PC.

- Tap the **Refresh** button on the Task bar to update the results (in between regular updates) shown on the screen.

- Tap the **Back** icon ↩ on the Task bar to return to the previous screen.

- Tap the **Home** icon ⌂ on the Task bar to return to the **Test Results** screen.

- Tap the **Tools** icon ⚒ on the Task bar for a drop-down list of network troubleshooting tools. Some tools are device specific and not available on the **Tools** menu but instead are available on the Preview pane of the Device Details screen.

- To assist in finding a specific device in a list (e.g. on the **Device Discovery** screen, use the **Find** button located on the Title bar at the top of the screen. Enter a partial or full name or address in the entry box and select **Find** to initiate the search.

- Tap the ? icon for screen level help.

- To switch between **LAN** and **WLAN** tests, tap the WLAN Tests or LAN Tests button on the Task bar. The appropriate option must be installed in order to switch between the tests. You can check the installed options on the Instrument Settings - Options screen. Any data that has been collected will be lost when you switch.

3 Configure the Network Assistant

As soon as it is powered up (and a wireless card has been properly installed), your Network Assistant will begin to discover wireless networks and devices. However, in order for the instrument to discover complete details about your wireless network and devices, to enable the security features of the instrument, and to use many of the Network Tools, you will need to set configuration and security options. Instrument Settings explains how to configure the instrument. You should also read the topic Wireless Linking to understand how the instrument links to the network and the configuration issues with respect to establishing link.

You can modify the instrument's display, set the date and time, select the language for the online help, recalibrate the display, and modify the settings for battery management from the Desktop Settings screen.

4 Using the Wireless Network Assistant

As the automated tests are running, the instrument provides information on the **Test Results** screen about the status of each test and indicates the success or failure of a particular test. A synopsis of the highlighted test is provided in the Preview pane. The right pane displays the name of each test and reports its status. The icons that appear to the right of each test give you a visual indication of the progress and status of each test:

- Running

- Not running

- Completed and passed ✓

- Completed and failed 🚫

Using the stylus, tap any test to display a synopsis of the test results in the left panel (Preview pane) of the screen. Tap the **Details** button to view more information about a selected test. All blue text represents a hyperlink to a separate, related screen within the UI.

You can switch to **LAN** tests by tapping the LAN Tests button on the Task bar. The **LAN Option** must be installed in order to switch between the tests. You can check the installed options on the Instrument Settings - Options screen. Any data that has been collected will be lost when you switch.

Note: If you have a LAN/WLAN unit, the radio card should not be removed while the instrument is powered on (even when the instrument is in LAN mode).

Your Network Assistant instrument provides a set of tools commonly used in the network maintenance and troubleshooting process. Tap the **Tools** icon located in the lower right of a screen for a list of tools available with the product. When troubleshooting a specific device, a relevant set of these tools is available directly on the **Device Detail** screen. On most screens a **Report** button is available that will generate a report based on the information that has been discovered. Tapping the **Home** icon will return you to the main **Test Results** screen.

The EtherScope user interface is designed to provide as much relevant information as possible on each screen. Information is provided in a hierarchical format, where general information is shown at the top level and an increasing amount of detailed information is shown at the lower level(s). On most screens, a summary view of a selected item is shown on in the left side preview panel and detailed information is provided in the right pane.

Refer to the topic Navigating the User Interface for information on how to use the instrument's UI.

5 Wireless Linking

Your EtherScope Network Assistant's wireless card operates in three basic modes:

All channel scan mode - the application passively scans all wireless channels while sampling frames on each channel for about 250 milliseconds

Single channel scan mode - the instrument passively monitors a single wireless channel while gathering information on all traffic on the channel

Link mode – the instrument establishes link to the wireless network, permitting active discovery of devices and diagnostic tests such as Ping to function

Note: The button on the left side of the Task bar indicates the operating mode of the instrument. It reads **Scan** and displays the channel being scanned in either of the scan modes or it reads **Link** and indicates the channel that the instrument is attempting to link with.

In most environments there will be multiple wireless networks. A number of the instrument's features require linking to one of the available networks. This wireless network is referred to as the Default SSID and it should be the network that is of primary interest to you. You can configure the Default SSID on the Wireless Instrument Settings - Wireless Security screen. While configuring the Default SSID is not a requirement in order to use the instrument, it does allow a more complete discovery including DNS names and IP addresses of the wireless devices. In addition, many of the Network Tools require that the instrument establish link and the IP address of the target device be identified.

It is advisable to configure wireless security for all of the discovered SSIDs for the most effective use of your EtherScope Network Assistant.

When the instrument is first powered on and is on the **Test Results** screen, it performs a complete channel sweep in All Channel Scan mode, then attempts to link to the configured Default SSID network. Once link is established, it will perform active discovery of the default network for a period of 30 seconds. After active discovery, it returns to all channel scan mode.

The active discovery of devices is an important feature to gather accurate information, so the instrument attempts to re-link to the default SSID and do another 30 second active discovery every 10 minutes. Again this automatic linking and discovery occurs only when the **Test Results** screen is displayed. If the instrument is not on the **Test Results** screen when the 10 minutes have expired, the instrument will reset the timer and try to link 10 minutes later.

Note: If you move off the **Test Results** screen while the instrument is linked, then the instrument will disconnect and resume scan mode.

In addition to the regular link and discovery feature, some user-initiated operations will cause the instrument to attempt to link. The instrument must successfully link to a network in order to use the following Network Tools:

- **Ping**
- **Trace Route**
- **Web Browser**
- **Telnet**
- **SSH Telnet**
- **FTP**
- **TFTP**
- **Wireless Throughput**

These tools require a target device (the device you wish to test). If a device is currently selected in a device list when a network tool is selected, then the device becomes the target for the tool. When a target has been selected, the instrument will use the SSID that the device is associated with to establish link. If the instrument has not yet resolved the device's SSID (e.g. the device has a hidden or non-broadcasted SSID), the instrument will use the configured Default SSID.

If a device is not selected when a tool is started, the instrument first prompts the user for the target device's IP address. Once it has a target IP address, the instrument attempts to find a previously discovered device with the same IP address. If a match is found, the instrument will use that device as the target and attempt to link using the same protocol as above. If an IP address match is not found, the instrument uses the Default SSID when linking.

A link to an SSID can be initiated in either roaming mode (using the AP with the strongest signal) or directly to one specific AP (non-roaming mode). If a link is initiated when the target device is AP, the instrument will always link directly to that specific AP. The link is always initiated in roaming mode if the Default SSID is utilized. Otherwise, the user will be prompted to select the link mode to use (roaming or specify the AP to use).

A test link can be initiated when configuring an SSID from the **Wireless Instrument Settings - Wireless Security** screen to verify that the configuration options are valid. In this situation, the link is always initiated in roaming mode and link will be established using the AP with strongest signal.

If a link is already established when a second link-based tool is selected, the existing link will be used. In this manner, you could start a **Wireless Throughput** test, then initiate the **Ping** tool without re-linking.

6 Instrument Settings

When the wireless EtherScope application is first started, it begins scanning the wireless spectrum and reports on wireless devices and networks that it finds. After making one complete channel scan of the wireless spectrum it will try to establish link with an AP that is using the (user) configured default SSID. If link is established, the application obtains (either through DHCP or statically configured) an IP address and then performs active discovery of the network for approximately 30 seconds.

Note: Transmit must be enabled on the **Radio** settings (enabled by default).

After active discovery times out, the application unlinks and resumes a continuous scan of the wireless spectrum. After ten minutes have elapsed (and subsequently every ten minutes thereafter when the instrument is on the **Test Results** screen), link will be re-established and active discovery will commence for approximately 30 seconds.

The **Instrument Settings** screens allow you to configure the instrument for your network environment and to set the appropriate security measures for access to the instrument itself. You can access **Instrument Settings** by tapping the EtherScope Application icon located in the Title bar at the top of the display. Also, when the **Connection** test is highlighted on the **Test Results** screen, tap the **Details** button to display the **Instrument Settings** screen.

The **TCP/IP** screen is the default. Tap one of the hyperlinks found in the preview panel to view or change the instrument settings.

TCP/IP - Configure the TCP/IP settings of the instrument for proper operation while it is linked to the default AP.

Wireless Security - In order for the instrument to establish link during wired discovery you must configure security settings for at least one of the discovered SSIDs. As part of it's wired discovery mode, the instrument will link to an AP using the configured default SSID and perform additional discovery of wireless devices from the wired side of the network. If you do not set up a default SSID, then IP addresses and DNS names may not be discovered. Without an IP address identified for a device, many of the Network Tools are unavailable.

Radio - Configure the instrument's radio card for proper operation in the wireless environment.

Instrument Security - Configure the security settings that control access to the instrument and the instrument's access to the network.

General - Restore default settings and set other preferences.

© 2004 - 2008 Fluke Corporation

Authorization - Designate which wireless devices are authorized on the network.

Problem Thresholds - Enable or disable the problems that get reported and designate the level at which certain measured statistics will generate an entry in the Problem Log.

Options - Enter the registration key code for the instrument and view which options are enabled.

Version - View the hardware and software version information for the instrument and the wireless radio card.

When finished with the configuration task, tap the Apply button. Tap the Home home_button icon to return to the Test Results screen or tap the EtherScope application icon ▣ , where you can select other tests.

6.1 TCP/IP Settings

If DHCP is available on your network, the **Instrument Settings - TCP/IP** screen will display the address that the instrument was able to obtain. To use a static IP address or to change the subnet mask, tap the **Automatically configure TCP/IP settings** checkbox to disable auto-configuration of the IP address. Select the field that you wish to change, select the Keyboard icon ⌨ (or use the pull-down list) and enter an **IP address** or **Subnet mask** as appropriate. You can use the pull-down list or keyboard to change the **Default router, Primary DNS**, or **Secondary DNS**. Tap the **IP** icon next to an address field to edit the address shown in the field.

Note: The IP icon will be disabled for the IP Address field when auto configuration is selected.

Note: When assigning a static IP address, the address can be for an alternate network but must be in the same broadcast domain.

Note: If DHCP fails to deliver an IP address, the instrument will determine the network on which it resides and pick an unused address.

Once data has been entered, tap the **Apply** button to save the changes. You will see the **Applying IP Settings** dialog box, which indicates the status of the address changes as they are made. Close this box when the **Done** box is checked. If you do not select the **Apply** button before you exit the **Instrument Settings - TCP/IP** screen then all changes will be lost.

6.2 Wireless Security

As soon as it is powered up, your Network Assistant will begin to discover wireless networks and devices, however, in order for the instrument to discover complete details about your wireless network and its devices, you must configure security settings for at least one of the discovered SSIDs. As part of its active discovery mode, the instrument will link to a device using the configured default SSID and perform active network discovery. If you do not set up a default SSID, then IP addresses and DNS names may not be discovered.

You can access the **Wireless Security** screen from the Wireless Instrument Settings screen. On the **Wireless Security** screen, use the pull-down menu in the **SSID** field to select an SSID that you want to use. Select the **Default** box if you wish to make this the default SSID. The instrument will link to an AP in the default SSID during active discovery. The default SSID will be designated by the ✳ icon in the pull-down list.

Note: If the **Wireless Security Setting** is enabled on the Instrument Security screen, then the Wireless Security screen will be inoperable until the appropriate password is entered on the Instrument Security screen.

Note: The **Enable Transmit** checkbox must be enabled on the Wireless Instrument Setting - Radio screen in order for the instrument to establish link with an AP.

Select the appropriate security type (EAP, PEAP, WEP, WPA, etc) and configure the security keys that will allow the instrument to connect to an AP in the selected SSID. Tap the **Apply** button when you are done to save your changes. You can set the security settings for multiple SSIDs and 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.

After you have configured security for the SSID (and applied your changes), you can verify that it works by tapping the **Link...** button. The instrument will link to an AP configured with the SSID. Tap **OK** in the **WLAN Link** popup to unlink the instrument.

Note: Some network tools require that a default SSID be configured.

Note: The application contains MatrixSSL(tm) security software licensed from PeerSec Networks Inc.

6.3 Connection Log

The **Connection Log** screen shows the sequence of events related to the last time that the instrument connected to the network as part of its active discovery process. The sequence starts at time 0.00 seconds and each event is time-stamped relative to the first event. The first part of each event indicates the type of action or event, followed by information about the response to the event. The log is reset each time the instrument links to the network or when tests are restarted. You can use the Report button on the task bar to save the log to the CompactFlash.

6.4 Radio

You can use the **Radio** screen to configure the radio card that is plugged into Slot 1 of the instrument. You can reach the **Radio** screen from the Wireless Instrument Settings screen.

Note: The radio card should not be removed while the instrument is powered on.

These are the available settings:

Country Setting - This setting dictates which channels are legal. Use the pull-down menu to select the appropriate country. The **Global** selection configures all channels. Illegal channels are highlighted in red on the **Channels** screen and devices discovered on illegal channels will generate an error in the **Problem Log**.

Active Bands - Select the radio button for the frequency bands that you want the instrument to use and test:

- 802.11 a/b/g
- 802.11 a only
- 802.11 b/g only

Note: The instrument detects APs that are beaconing 802.11n but can not transmit or receive at that bandwidth.

Transmit Settings - If transmit is enabled, then the instrument will link to an AP (as specified on the Wireless Security screen) and conduct active discovery of the wireless network. If it is not enabled (the **Enable Transmit** checkbox is cleared), then only passive discovery of the wireless network occurs and it is unlikely that IP addresses and DNS names will be discovered. Devices not broadcasting their SSID (designated as **Hidden**) will not have their SSID identified. If this setting is disabled, the Status column entry for the **Connection** test on the **Test Results** screen will read **WLAN Transmit is disabled**. Use the pull-down menu to select the transmit rate, either **Auto** or a specific rate. **Auto** will cause the instrument to use the highest available value.

Signal Units - Select between **dBm** and **Percent** to set how the signal strength statistic is shown for a device. This setting affects the display in multiple tests.

Signal Strength dBm Corrections (only active when the **dBm** radio button is selected) **-** Use this to normalize the signal strength readings. This is useful when trying to compare the results from the Network Assistant with the results from another device.

6.5 Instrument Security

You can use the **Instrument Security** screen enable/disable **Password Control**, **Wireless Security**, and **Wireless Throughput**.

Password Control

Setting and Changing a Password
You can enable password protection that requires a password in order to view or edit SNMP Community strings, edit Wireless Security settings, or to run Throughput or Traffic Generation tests. To establish a password, tap **Create password...** and enter a password in the **New password** field. Re-enter the password in the **Confirm password** field and tap **OK**. To change an existing password, enter the password and tap **Change password...** . Enter a new password and then re-enter it to confirm. Cycle power to the instrument to enable the password setting.

Note: If you forget the password, you will need to contact your authorized service center or Fluke Networks product support for assistance.

Clearing a Password
To clear a password, you must enter the existing password. Tap the **Change Password** button. Leave the **New Password** and **Confirm Password** fields blank and tap **OK**. Tap **OK** a second time on the warning popup. Cycle power to the instrument to make the change take effect.

Wireless Security Settings
Use the checkbox to enable password control of the Instrument Security - Wireless Security settings. If this checkbox is enabled, the password must be entered before the Wireless Security settings can be viewed or changed.

Wireless Throughput
Tap the **Enable Throughput** checkbox to enable the Wireless Throughput test. Use the **Password required** checkbox to enable password control of the test. If this checkbox is enabled, the instrument password must be entered before the **Wireless Throughput** test can be run.

6.6 General

On the **Instrument Settings - General** screen you can:

- **Wireless Factory Defaults** - This will clear any user-defined configurations/authorization and clear the discovery database. Any collected data will be lost. All values will be reset to the factory settings. You will see a warning popup before the instrument is reset.
- **Show vendor prefix with MAC address** - You can control how a device's MAC address is shown: either in raw hexadecimal format (e.g. 00c017c0000c) or with a vendor prefix (e.g. FLUKE-c0000c).
- **MAC Address** - Change the instrument's MAC address. Enter the MAC address and tap **Save MAC Address**.
- **Restore factory MAC** - Change the instrument's MAC address to the original factory setting.

6.7 Authorization

The **Authorization** screen allows you to configure the instrument to aid in the detection of rogue Access Points or clients. All discovered devices are initially classified as **Unauthorized** (⚠). You can reclassify devices as **Authorized** (✓) or Neighbor (✓). A neighbor is a device that you frequently see but is not authorized on your network. The **Authorization** screen is accessible from the Wireless Instrument Settings screen.

Note: You can easily change the authorization level of a single device by highlighting a device on the Device Discovery screen and using the pull-down authorization menu.

The table shows all of the wireless devices discovered by the instrument, listed by MAC address. Each device's current authorization level is indicated by the icon to the left of the MAC address. By default, all devices are initially classified as **Unauthorized**. The type of device is indicated by the icon (AP , Bridge , or Client) in the first column. If a device is not in the list, you can enter the device's MAC address in the **New MAC Address** field and then tap the **Add MAC** button to add it to the list.

If you want to change the authorization level for one or more devices (but not all), tap each MAC address in the table that you wish to change. Each tapped table entry will be highlighted. (Tap an entry again to de-select it.) Use the **Change Level To** pane to select the authorization level that you want and then tap the **Change** button. The authorization icon next to the highlighted devices will change to reflect your choice.

Note: The authorization level changes are not permanent until you select the **Apply** button. If you exit the **Authorization** screen without applying your changes, the authorization levels will remain unchanged.

If you want to change the authorization level for a whole category of devices, select one or more categories in the **Select Current Level** pane and then tap the **Select All** button. The entries in the table for the selected categories will be highlighted. You can then select the authorization level in the **Change Level To** pane and tap the **Change** button to effect the change. Tap the **Apply** button to make the changes permanent. For example, if you want to change the status of all of the **Unauthorized** devices to **Authorized**, select the **Unauthorized** category in the **Select Current Level** pane, tap **Select All**, then select the **Authorized** category in the **Change Level To** pane, and tap the **Change** button. The unauthorized icon (⚠) next to each device will change to the authorized icon (✓). Tap the **Apply** button to make the changes permanent.

After you have changed the authorization level for a device, the authorization icon for the device shown in the device list of other measurements will reflect the change.

After you have discovered and designated the authorization level, you can save (export) to the CompactFlash a list of devices and their authorization levels. The exported file has a .acl extension. You can also import a list of devices. Use the **Import...** and **Export...** buttons to accomplish this. You can view the files exported to the CompactFlash by using a text editor like Microsoft Wordpad. You can also use 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:

```
// EtherScope Wireless access control list

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

6.8 Group Names

The **Instrument Settings - Group Names** screen allows you to assign the same alias name to one or more devices. The Group Name will show up in the **Name** field of a device. This is useful if you have a device with multiple BSSIDs (it may be beaconing on two bandwidths, or assigned to two or more VLANs). The Network Assistant identifies two different devices. Assigning the two BSSIDs the same group name allows you to sort the device list on the **Name** field and the "two" devices will be grouped together.

Tap the **New Group** button and enter a name in the **New Group** popup. Tap the **OK** button and the new name will be displayed in the **Group Name** field. You can then highlight a device in the list and use the **Add to Group** button. You can also use the **New MAC/BSSID** button to add a new device to the list and then add it to the Group.

You can create multiple **New Groups** or use the pull-down menu in the **Group Name** field to select a previously created name. Tap the **Apply** button when done; the EtherScope application will restart.

6.9 Wireless Problems

You can customize the application to control which problems are entered in the **Problem Log**. For certain conditions detected by the instrument, you can set the threshold level at which the instrument will report the problem in the **Problem Log** (and become visible to the user). The **AP supported rate** thresholds are the minimum rates that an AP must advertise (beacon). If an AP does not support the threshold rate, an error is generated.

You can also enable or disable whether problems get entered in the **Problem Log** at all. Use the checkbox next to each problem to specify whether it is reported (enable the checkbox to enable reporting). Tap the **Apply** button when done to make changes take effect. If you exit without applying your changes, the values will revert to the previously stored values.

6.10 Options

The **Options** screen allows you to enter a Key Code that enables different applications for your EtherScope Network Analyzer. **Options** is available from Instrument Settings.

The available options are:

- **LAN Option (ES_LAN_OPT)** - enables you to monitor and test IEEE 802.3 Ethernet 10/100/1000 networks
- **WLAN Option (ES_WLAN_OPT)** - enables you to monitor and test IEEE 802.11 a/b/g wireless networks
- **Internet Throughput/Traffic Generation (ES_ITO_OPT)** - enables you to test network throughput and generate test traffic on your IEEE 802.3 network
- **Fiber Option (ES_FIBER_OPT)** - enables the 1000BASE-X gigabit fiber interface

Your instrument will come from the factory configured with the appropriate key code to enable the options that you ordered. If you add an option, then it is necessary to enter the key code in the **Set Key Code** field to enable it.

6.11 Version

Tap the **Version** hyperlink (found on the **Instrument Settings** screen) to view the current software and hardware versions and information on the Fiber Module installed on your instrument.

7 Status LEDs

There are 5 Status LEDs above the instrument display and one LED above the power button. From top to bottom, the 5 Status LEDs indicate:

Link

- **Green** - 802.11b
- **Amber** - 802.11a or 802.11g

Utilization (% bandwidth used)

- **Green** - 1% to 30%
- **Amber** - 31% to 60%
- **Red** - 61% to 100%

Collision

- **Amber** - Any packet received with retry bit set. The retry bit is set by the transmitting station to indicate the packet was transmitted previously but no ACK was received, so the packet is being retransmitted.

Error

- **Red** - Any packet received with a "hardware" error. Hardware errors include any CRC or phy error preventing receipt of a packet. It does not include logical errors such as decryption errors, key mismatches, or MIC integrity check errors.

Transmit

- **Green** - packet transmitted

Power Status - the LED above the power button indicates the following:

- **Green Blinking** - (on EtherScope Series II instruments) indicates that the unit is powered off but AC

power is applied and the battery is being charged.
- **Green** - the instrument is in full power mode, by either battery or AC power.
- **Amber** - the instrument is in Suspend mode

8 Desktop Settings

To configure the instrument's desktop settings, tap the **Desktop** icon, located on the left side of the status bar, and select **Settings**. The **Settings** tab includes several tools, including **Appearance**, **Date/Time**, **Language**, **Light & Power**, **Recalibrate**, and **Sound**. Tap on any of these tools to change the settings.

The windows color scheme, style, and frame type can be configured using the **Appearance** tool. The default color scheme is **EtherScope**.

The current date and time, along with their respective formats, can be set with the **Date/Time** tool. Power management can be configured using the **Light & Power** tool. Refer to the Battery Management topic for more information. Select Language to set the language for the user interface and online help. Use the **Recalibrate** tool to recalibrate the instrument's touch screen. The volume can be set using the **Sound** tool.

8.1 Language Support

Your EtherScope Network Assistant has a localized User Interface and screen level help for the following languages:

- **English**
- **French**
- **German**
- **Japanese**
- **Portuguese**
- **Simplified Chinese**
- **Spanish**
- **Russian**

You can verify whether Language Support has been loaded on your instrument by looking at the Version screen. If the Language Support field has an (**Extended**) notation as part of the version, then a translated User Interface and online help are available.

If Language Support has not been loaded on the instrument, you can get the files from the Fluke Networks web site (www.flukenetworks.com). Select **Support | Software Downloads** and then select **EtherScope Network Assistant**. Follow the instructions on the web site in order to download the executable to your PC. The ESUpdate.exe file will appear on your desktop. Run the ESUpdate file and follow the directions to transfer the translated files (EtherScope Language Support) to a CompactFlash. You can also choose to transfer updated EtherScope firmware but it is not necessary if your EtherScope instrument is already current. You must have a CompactFlash with the translation files on it in order to install and use the localized files.

Once you have the CompactFlash with the translated files on it, follow these steps to change your screen level help to the desired language:

1. Insert the CompactFlash in **Slot 2** of your EtherScope Network analyzer and power cycle the unit.

2. Tap the Desktop icon, located on the left side of the status bar, and select **Settings**.

3. Select the Language icon.

4. You will see a popup advising you that there is a newer file available. Select **Yes** to copy the language file to the instrument. After the file is copied, the list of available languages is shown in the **Language** dialog window.

5. Select the language which you wish to use to view the user interface and help.

6. Select **OK** to close the dialog.

7. You must power cycle the instrument in order for the changes to take effect.

Note: You can remove the CompactFlash after you have completed the language selection procedure.

8.2 Touch Screen Recalibration

The product uses a touch screen that has been calibrated at the factory. In the unlikely event that the touches on the screen seem off target, use the **Recalibrate** utility to remedy it. Select the **Desktop** icon, located on the left side of the status bar, tap **Settings** and then tap the **Recalibrate** icon. Follow the screen prompts to recalibrate the touch screen.

8.3 Battery Management

The EtherScope Network Assistant can be powered either by connecting the external power cord, or via the removable, rechargeable lithium-ion battery. Once fully charged, the battery is capable of powering the instrument for approximately 4 hours (3.5 in wireless mode) of full operation. When fully discharged, the battery takes approximately 4.5 hours to reach full charge when the instrument is powered off. When the instrument is powered on, it takes approximately 7 hours to fully charge the battery.

The instrument provides several methods for extending battery life between charges:

- Turn the instrument off when not in use by holding down the green power button until the power button LED turns completely off (about 2 seconds). The instrument will then go into a software power down sequence that takes several seconds before turning completely off.

Note: (On EtherScope Series II instruments) When the unit is powered off but plugged in to AC power, the power button LED will blink green to indicate that the battery is being charged.

If you encounter difficulty turning the instrument off, press and hold the green power button about 5 seconds. This forces the instrument into a hardware power down. When powered off, the instrument draws no power from the battery.

- Put the instrument into **Suspend** mode. This provides a low power mode without turning off the instrument. When Suspend mode is activated, the instrument goes into a partial power down sequence that takes several seconds. The display will go blank, but the instrument will not turn completely off. In Suspend mode, the instrument uses about 1/3 the power of its full "on" state by shutting down all tests. Using Suspend mode allows the instrument to be turned back on instantly, without requiring boot-up.

The product can be put into Suspend mode in several different ways:

- Press the green power button until the power button LED turns amber (about 2 seconds), and then release.

- Tap the Desktop icon icon, located on the left side of the status bar, and select **Suspend**.
- Use the Light and Power settings to configure the instrument to automatically enter suspend mode

© 2004 - 2008 Fluke Corporation

after a certain amount of inactivity.

You can take the instrument out of suspend mode by either briefly holding the power button until the LED color changes from amber to green.

- Configure the **Light and Power** settings. These settings provide power saving alternatives such as dimming or turning off the display or entering Suspend mode after a certain amount of time. You can also adjust the display brightness. See the Desktop Settings topic for information on how to access the **Light and Power** settings.

9 Desktop Applications

The instrument includes several convenient applications in addition to the EtherScope Network Assistant. To access these applications, tap the Desktop icon found on the left side of the Status bar and select **Applications**. The **Applications** tab includes several tools, including a **Calculator**, **Calendar**, **Clock**, **EtherScope Console**, **File Manager**, **Report Viewer**, and Web Browser.

Tap any of the icons in the lower right corner of the status bar to view or set the display brightness , cut or paste text , adjust the speaker volume , check the battery level , or set the date/time 10:03 PM .

The **EtherScope Console** application provides a user interface for the Terminal, Ping and Trace Route tools.

The **File Manager** allows you to view the contents of the user accessible portion of the instrument's file system. You can rename or delete files that are stored in memory or on the CompactFlash. You can open text files (indicated by the icon) and view them on the instrument's **Text Viewer**. Tap **File** on the toolbar for a list of commands. You can navigate by tapping a subdirectory (indicated by the icon) or tap the icon to return to the previous directory. Files with a format that is unknown to the File Manager are indicated with the icon.

You can use the **Report Viewer** to open reports that have been stored on the CompactFlash. Open the **Report Viewer**, tap **File**, and select **Open** to view the list of available reports. Highlight your selection and tap **Open Report** to view it.

The **Web Browser** application opens the Konqueror browser. Konqueror is used to display the on-line help for the product. The browser application is limited in size and capability and does not support all browsing functions. For example it does not support Java virtual machine.

The other tools available from the **Applications** tab are provided for convenience and do not directly interact with the EtherScope Network Assistant application.

10 Software Update

Do the following steps to check for, download, and install software updates:

1. Tap the EtherScope icon , located on the left side of the title bar.
2. On the resulting drop-down menu, select **Instrument Settings**. The **Instrument Settings** screen appears.
3. Tap **Version** in the Preview pane.
4. The **Instrument Settings - Version** screen displays the versions of currently installed software and hardware.

5. To check for updates, tap the **Check for software updates** button.
6. The application connects to the Internet and the Fluke Networks web site to check if a software update is available.
7. If a newer revision is available, follow the on-screen instructions to download the software and install the software.

A software update can take 10-12 minutes. After the process is completed, the instrument automatically restarts and you can resume testing.

You can also manually check for updates and install them by using your PC to download software from the Fluke Networks web site:

1. Direct your web browser to the following URL: http://www.FlukeNetworks.com/Software.
2. Select the appropriate update and follow the instructions. (You can check the hardware and software versions that are currently loaded on your instrument on the Version screen.)
3. Copy the downloaded file to a CompactFlash card (64 Mb or larger; one is supplied with your EtherScope Network Assistant).
4. Power off your instrument, install the CompactFlash containing the update file in slot 2 of the instrument, and then power on.
5. The instrument will automatically update its software. Once the process has completed, the EtherScope application will automatically restart.

Caution: Any previous versions of software on the CompactFlash card will be lost. Data, reports, custom logo graphics, or Performance Test configuration scripts will not be lost.

After the software update is completed, an updated language file will be on the CompactFlash card that was used for the update. To load the updated language file onto the instrument, follow the instructions given in the Language Settings topic.

If you encounter trouble updating this software, contact the Technical Assistance Center. See the Contacting Fluke Networks topic for contact information.

11 Contacting Fluke Networks

To find out more about Fluke Networks and our products, visit us on the World Wide Web at http://www.flukenetworks.com or call us at 1-800-28-FLUKE (1-800-283-5853). You can also request information via e-mail at info@flukenetworks.com.

For technical support on the EtherScope instrument you can review the Fluke Networks Knowledge base at http://www.flukenetworks.com/knowledgebase. You can also send an e-mail to support@flukenetworks.com or call 1-800-28-FLUKE (1-800-283-5853). For access to the Fluke Networks Support Solutions, visit http://www.flukenetworks.com/support.

Our offices are located at the following addresses:

Fluke Networks
P.O. Box 9090
Everett, Washington, USA
98206-90902

Fluke Europe B.V.
P.O. Box 1186
5602 B.D. Eindhoven
The Netherlands

12 Trademarks and Copyrights

EtherScope(tm) Network Assistant is a trademark of Fluke Corporation
MetroScope Service Provider Assistant is a trademark of Fluke Corporation
Fluke Networks(r) is a registered trademark of Fluke Corporation
Qtopia(tm) is a trademark of Trolltech, Inc.
CompactFlash(r) is a registered trademark of the CompactFlash Association
Linux(r) is a registered trademark of Linus Torvalds
All trademarks are acknowledged

The EtherScope(tm) Network Assistant is powered in part by the Linux Operating system and other publicly available software. A machine-readable copy of the corresponding source code is available for the cost of distribution. Please contact the Fluke Networks Technical Assistance Center (1-800-283-5853) or visit the GNU web site (http://www.gnu.org) for more information.

Portions of the application are based on PeerSec Networks MatrixSSL(tm) (http://www.peersec.com)

13 Tests

13.1 Connection

The **Connection** test is automatically run when the instrument is powered on or the **Restart all** button is selected. The test shows configuration information and link status of your Network Assistant in the left-side preview pane and on the status line of the **Connection** test.

When the wireless EtherScope application is first started, it begins scanning the wireless spectrum and reports on wireless devices and networks that it finds. After making one complete channel scan of the wireless spectrum it will try to establish link with an AP that is using the configured default SSID. If link is established, the application obtains (either through DHCP or statically configured) an IP address and then performs active discovery of the network for approximately 30 seconds.

Note: Transmit must be enabled on the Radio settings.

After active discovery times out, the application unlinks and resumes a continuous scan of the wireless spectrum. After ten minutes have elapsed (and subsequently every ten minutes thereafter), link will be re-established and active discovery will commence for approximately 30 seconds.

After link has been established, the status line shows the IP address of the instrument. Depending on the TCP/IP configuration of the instrument (whether it is using DHCP to assign the address or it is a fixed address) and how IP addresses are managed on the network (e.g. how long do DHCP leases last), the IP address may change each time the instrument links to the network.

Tap the **Details** button (or the **Connection** hyperlink in the preview pane) to view or change the instrument's settings and configuration parameters. Refer to the Instrument Settings topic for more information on these settings and configuring the instrument.

13.2 Channels

The **Channels** test shows the results of the instrument's scanning of the wireless spectrum. On the **Test Results** screen, the **Channels** status line indicates the number of channels being actively scanned. The number of channels scanned is dependent on the Country Setting. The preview pane shows the following summary results for the 802.11a and 802.11b/g channels:

***** Active Channels
***** Active APs
***** Active Bridges
***** Active Clients
***** Active AdHocs (Clients)
***** % Utilization

Tap the ⊞ icon to expand the view to see the Utilization and the Top Talkers tests. Highlight the **Channels** test and tap the **Details** button to open the **WLAN Channels** screen. You can also tap the EtherScope icon on the Title bar and select **Channels** from the menu.

The **WLAN Channels** screen shows statistics that provide visibility into the health and configuration of channels for 802.11a/b/g. The channel scan is run on all channels in both 802.11a and 802.11b/g spectrums. The results are displayed in a graph reflecting information across all channels. Channel numbers that are not included in the Country setting of the radio card are shown in red. A carat on each bar of the graph indicates the maximum level seen for the statistic. The statistics are updated for each channel on each scanning sweep. Only one statistic is represented in the graph at any time. You can select the desired metric from the **Channel Metric** drop-down menu at the top of the display.

Choose from the following statistics:

***** Signal Strength (dBm or %)
***** Noise (dBm or %)
***** Signal to Noise Ratio (dBm or %)
***** Total Utilization (%)
***** Good Packet Rate (pkts/sec)
***** Good Octet Rate (pkts/sec)
***** Error Packet Rate (pkts/sec)
***** Error Octet Rate (pkts/sec)
***** Retry Packet Rate (pkts/sec)
***** Retry Octet Rate (pkts/sec)
***** Retry %
***** CrossTalk Packet Rate (pkts/sec)
***** CrossTalk Octet Rate (pkts/sec)
***** CrossTalk %

Note: You can select whether the signal strength measurement is shown as a percentage or in dBm on the Wireless Instrument Settings - Radio screen.

Highlight a channel in the table and the Preview panel gives a summary view of the channel statistics. Tap the **Devices** button to show a list of APs and Ad Hoc Clients that are using the channel. When an AP is highlighted a list of associated clients will appear in the lower of half of the screen and the preview pane will provide details about the AP.

Highlight a channel and tap the **Details** button and the Network Assistant will remain on the selected channel and display the **WLAN Channel** screen. This shows statistics for the selected channel. Use the drop-down **Channel** menu to select a different channel.

13.2.1 Utilization

The **Utilization** and **Top Talkers** tests provide information that is useful for checking and troubleshooting network traffic and performance issues. The **Utilization** test provides visibility into the amount and type of traffic on the WLAN channel.

Tap the ⊞ icon next to the **Channels** test on the **Test Results** screen to expand the view to see the

Utilization and **Top Talkers** test summaries. The status line of the **Utilization** test shows the wireless channel with the highest bandwidth utilization. The Preview panel shows the top 5 channels with the highest bandwidth utilization. The Pkts/Sec statistic is also shown for each channel.

The bandwidth utilization calculation is calculated using the results from a certain number of channel sweeps, depending on the operating mode of the instrument, 3 sweeps per sample in A/B/G mode, 5 sweeps in A only mode, and 7 sweeps in B/G only mode.

Tap the **Details** button or tap a hyperlink in the Preview panel to go to the **Channel Utilization** screen. The hyperlink that you select determines which channel information is initially displayed. You can select a different channel by using the pull-down menu in the **Channel** field. All wireless channels are available, regardless of the Country setting of the radio card.

When you go to the detailed view of **Channel Utilization**, the comprehensive utilization statistics collection is suspended and statistics are collected for the selected channel (counts begin at 0). When you exit the detailed view, the suspended statistics collection is resumed (the previous counts are used until the number of channel sweeps is completed to calculate new statistics). The statistics collected in the detailed view are discarded.

The **Channel Utilization** screen shows a Utilization graph and tables of network statistics. Select between **Frame Details** and **Protocol Details** to control which statistics are shown. The table to the left of the graph shows utilization as a percent of total bandwidth. The bar graph shows a visual representation of the statistics (the white line graph represents the total). The table on the bottom gives packet statistics for the time sample indicated by the vertical cursor on the graph. By default, the cursor is on the far right side of the graph and the table represents the most current data. You can drag the cursor to a particular data point and the table shows statistics for the selected time period. The cursor will move with the selected data point until it scrolls off and at that point the cursor is repositioned to the most current data point where it will stay until moved. You can use the **Pause** button to stop the graph from updating so that you have more time to review the data. You can move the cursor on the graph to inspect the data at different time samples. Tap the **Resume** button to resume updates (the graph will jump to the current time statistics samples). Tap the **Clear** button to reset all the statistics on the screen.

You can use the **Update Every** field to change the update frequency from 5 seconds to up to 60 minutes. Tap the **Hide Totals** button to hide the Packet Statistics table and enlarge the bar graph. Tap the **Packet Rates** button to view the **Utilization Rates** screen. This will show you an instantaneous table view of the utilization statistics broken down by data rate.

Visibility into the packet rates can be used to uncover performance issues (e.g. If a large percentage of packets including data are being transmitted or received at low rates, there may be a user that is connected at the physical edge (almost out of range) of the network. This user may consuming an excessive amount of bandwidth.)

13.2.2 Top Talkers

The **Utilization** and **Top Talkers** tests provide information that is useful for checking and troubleshooting network traffic and performance issues. The **Top Talkers** test provides visibility into the devices that are using the network.

Tap the ⊞ icon next to the **Channels** test on the **Test Results** screen to expand the view to see the **Utilization** test and the **Top Talkers** test. The status line of the **Top Talkers** test identifies the wireless device with the highest bandwidth utilization. The Preview panel shows the top 5 devices with the highest bandwidth utilization (across all channels).

Tap the **Details** button or tap a hyperlink in the Preview pane to go to the **Top Talkers** screen. This shows you a list of discovered wireless devices that are consuming bandwidth. You can filter the list by selecting the packet type on the Title Bar. You can choose to display **MAC(All)**, **Broadcast**, **Multicast**, **Retry**, or **Error** packets. Use the scroll bar at the bottom of the screen to view all of the statistics for a device. You can use the radio buttons at the bottom of the Preview panel to change what statistic is shown on the left-side view of the list of devices. Regardless of the radio button selection, the rest of the statistics are available by using the scroll bar.

Highlight a device in the list and tap the **Details** button to open Device Details for the device.

Note: If you highlight a device in the list, the Preview pane changes and the radio buttons disappear. Tap the ☒ icon in the top left corner of the Preview pane to restore the view.

You can choose to view statistics for a single channel or for an SSID (across all channels) by making the appropriate selection from the drop-down menus found just below the Title Bar (select from the **Ch** or **SSID** fields). When a single channel or SSID is selected, the comprehensive statistics collection is suspended and statistics for the selected parameter is begun (counts begin at 0). When you return to the comprehensive view, the previously suspended statistics collection is resumed and the selected parameter statistics are discarded.

Note: Because of when statistics are started and collected, the Top Talker when a single SSID or channel is selected may be different than the Top Talker for the SSID or channel when collecting comprehensive statistics.

Note: A device whose name appears in yellow (default Appearance setting) when a single Channel is selected has been detected as being configured for a different (or unknown) channel but is "crosstalking" on the selected channel.

Tap the **Clear** button to reset the statistics being collected. If a single channel or SSID is selected, then statistics are only cleared for the selected parameter (not the comprehensive statistics). If comprehensive statistics are being collected (and displayed) then tapping the **Clear** button resets those statistics.

13.3 Device Discovery

As soon as the Network Assistant is turned on, it begins wireless network discovery. Configuring the instrument for your network enables the instrument to link to an AP and perform a more thorough active discovery of your wireless network. The **Status** column on the **Test Results** screen shows the number of devices discovered. When the measurement is highlighted, the preview panel lists the categories and count of network devices.

Note: Because a device can appear in multiple categories in the summary pane (e.g. a client is also an SNMP agent), the sum of the number of devices in each category can be greater than the number reported in the **Total Devices** category.

Tap the ⊞ icon to expand the view to see the AP Top Talker, and Client Top Talker measurements. Tap the **Details** button to open the **Device Discovery** screen. Tap a category in the preview pane to see only devices of the selected type (you can also do this from the **Test Results** screen).

The **Device Discovery** screen shows a list of discovered wireless devices identified by their MAC address, an icon identifying the type of device, the SSID associated with the device, and an icon identifying whether there are any problems reported for each device. A slide-bar at the bottom of the screen allows access to additional device information that can not be seen in the initial view. A symbol (⚠ unauthorized, ✓ authorized, or ✓ neighbor) is shown next to each device icon. This symbol indicates the authorization level of the device. Highlight a device in the list and the preview panel shows a summary of information about the device. You can quickly change the authorization level for the selected device by using the pull-down authorization menu ⚠ Unauthorized ▾.

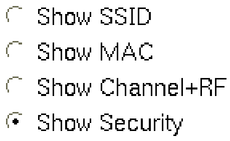
Note: See the Authorization topic for information on how to globally change the authorization levels for discovered devices.

Select a column header to sort the list. Columns can be resized by dragging the separating bar between columns in the header.

Note: A device with an SSID that begins with an **>>** character indicates a devices that is configured with multiple SSIDs. Each SSID is separated by **>>** (e.g. >>SSID1>>SSID2).

Use the **Find** window at the top of the display to locate a particular device. You can enter a partial name or address (MAC or IP, case insensitive) to find the entry. Use the pull-down menu to find a device that has been previously entered. A message will appear in the Preview Pane if the requested device can not be found.

Use the radio buttons in the lower left corner to select which device information is displayed next to the device name in the table:



○ Show SSID
○ Show MAC
○ Show Channel+RF
● Show Security

Note: This just reorders the information on the screen, use the scroll bar to access the other information.

Note: If a device is highlighted in the list, then the radio buttons are not visible. Tap the ☒ icon in the upper left corner to display the radio buttons.

As new devices are discovered, they are added to the device list and the list is automatically sorted. In an active wireless environment, this can make it difficult to select a particular device as the list appears to be "jumping around". You can temporarily disable the sort by tapping the **Disable sort** button. With the sort disabled, new devices are added to the bottom of the list. The sort is re-enabled if you leave **Device Discovery**, tap a column header to sort on that column, or tap the **Enable Sort** button.

Tap the 🔨 button, to display a list of Network Tools that you can use to troubleshoot network problems or to connect to a device.

Highlight a device in the list and tap the **Details** button to show the Device Details screen, where you can view all the discovered information about the selected device.

13.3.1 AP Top Talker

The **AP Top Talker** measurement identifies the Access Point that is consuming the most bandwidth. Tap the ⊞ icon next to the **Device Discovery** test on the **Test Results** screen to expand the view to see the **AP Top Talker** and Client Top Talker measurements. The **AP Top Talker** summary on the **Test Results** screen provides quick visibility to the most heavily used AP on your network.

Highlight **AP Top Talker** and the preview screen shows the configuration details and statistics for the device. Tap the **Details** button to open the Device Details screen for the device.

13.3.2 Client Top Talker

The **Client Top Talker** measurement identifies the wireless client that is consuming the most bandwidth. Tap the ⊞ icon next to the **Device Discovery** test on the **Test Results** screen to expand the view to see the AP Top Talker and **Client Top Talker** measurements. The **Client Top Talker** summary on the **Test Results** screen provides quick visibility to the most active client on your network.

Highlight this measurement on the **Test Results** screen and the preview screen shows the configuration details and statistics for the device. Tap the **Details** button to open the Device Details screen for the device.

13.4 Network Discovery

The **Network Discovery** test shows the configuration of your wireless network. It determines the configuration of your wireless devices (**Infrastructure**, **Ad Hoc**, **Bridge**, or **IP Subnet**) and reports the number of devices in each category. Devices can be listed in multiple categories. This test provides a summary view of the networks and devices operating in your wireless space and provides visibility into configuration issues or policy violations (e.g. Ad Hoc networking not allowed or security violations).

Note: In order to see IP Subnets, a default SSID must be designated in Wireless Security so that the instrument can link to an AP and run active discovery.

Highlight **Network Discovery** on the **Test Results** screen and the preview panel shows a summary of the discovered network types and the number of devices in each. Tap the **Details** button or one of the categories in the preview panel to bring up the **Network Discovery** screen.

The **Network Discovery** screen shows a tree of network types with the number of each type shown in parentheses (e.g. **(17) WLAN Infrastructure Networks...**) and a list of networks beneath each type. Expand a network type using the ⊞ icon to see the discovered devices associated with the network. Keep expanding the tree to "drill down" and see more details about the devices on each network. An icon (● Error, ▽ Warning, or ! Information) indicates whether any problems have been discovered for each device.

Select a device and the preview pane shows some device details and network statistics. If you select a host or mobile client, the preview pane will also show the number of Packets, Broadcasts, and Retries for the device. You can get more information by tapping the **Details** button to open the Device Details screen for the highlighted device.

13.5 Site Survey

You can use your Network Assistant to survey and store information about your wireless network. By periodically surveying given locations, you can create a recorded history of your network for later comparison (useful in troubleshooting client connection and performance problems). You can also generate a report of the survey results. By periodically running a site survey at multiple locations in your facility, you can identify uncovered as well as high usage areas. This information can be used as an aid in network design and verification and access point placement.

Highlight the **Site Survey** test on the **Test Results** screen and the Preview pane shows the four devices with the highest signal strength. Tap the **Details** button or one of the hyperlinks in the Preview pane to go to the **Site Survey** screen.

The **Site Survey** screen has two tables. The upper table shows a list of wireless devices discovered by the Network Assistant at the present location. For each device in the table, the SSID, BSSID, channel the device is using, and signal strength are shown. The lower table shows a previously stored list of devices. By comparing the devices discovered at a given location to a stored list from the same location, you can determine the changes that have occurred. For example, a device that is shown in red in the upper table indicates that it is a new device that was not in the stored survey.

Use the **Location** field to give a descriptive name to the spot where the survey is being performed. You can then use the **Save** button to store the survey results. You can save multiple surveys for each location. Use the **Edit** button that is next to the **Location** field to modify the name. You can use the **Delete this Location** on the **Edit Location** popup to remove all of the stored surveys for the specified location. The **Clear** button empties the top table; devices are automatically rediscovered. Tap the **Report** button to save the information to the CompactFlash. Select between saving a **WLAN Site Survey History**, which generates a report based on all of the stored site surveys for the selected location, or **WLAN Site Survey Current**, which generates a report based on the current survey only.

When you first enter the **Site Survey** screen, the Preview pane gives a summary of the results of the current survey. Highlight a device in either table and the Preview pane shows the current values for device and previous values (if the device is in the selected previous survey). You can select the **Details** button for a highlighted device to go to the Device Details screen.

13.6 Security Scan

The **Security Scan** test provides a quick way to identify Unauthorized ⚠ and Unprotected ? (no security enabled) devices on your network. **Security Scan** is accessible from the **Test Results** screen. Quickly knowing about security risks on your WLAN is key to maintaining a secure and healthy network.

The **Status** column on the **Test Results** screen shows the total number of unauthorized devices. Highlight the test and the preview screen shows a breakdown of the types of unauthorized and unprotected devices (Access Points or Mobile Clients). Tap the **Details** button to see a complete list of identified devices. Once you have identified a device as suspect, you can use the Locate feature to track it down so that it can be removed or properly configured.

You can use the Authorization screen to configure your wireless network devices as **Authorized**, **Unauthorized**, or **Neighbor**. For some office environments, identifying "neighbor" devices that are not part of your network but are consistently discovered improves the efficiency in troubleshooting and maintaining your WLAN.

Note: A device that is unprotected will have two entries in the table, one with an icon showing the authorization level and another entry with the unprotected icon.

13.7 Key Devices

You can designate one or more devices on your network as a Key Device and then the instrument will test them and verify that each device responds to a PING. The default condition is that no devices are designated. You must configure key devices specific to your network and troubleshooting needs. The **Key Devices** test is run whenever it is linked to an AP (see Using the Wireless Network Assistant). It can also be run from the **Key Devices** details screen.

After the instrument has linked to an AP (and subsequently closed the link), highlight **Key Devices** on the **Test Results** screen and tap the **Details** button. Use the drop-down menu at the top of the **Key Devices** screen to select a discovered device and mark it as a key device, or select the **Add Device** button and enter the IP address of a device.

Note: If you enter the IP address of a device that is not in the discovery database, it will be monitored as a Key Device but is not added to the discovery database.

The **Key Devices** preview on the **Test Results** screen shows a summary of the key device polling. A ✓indicates that all devices responded. A 🛇 indicates that one or more devices are unreachable and may be down. Four attempts will be made to contact a device before it is labeled unreachable.

Select **Key Devices** and the **Details** button to see the status of each key device.

Note: Your designated **Key Devices** are maintained after a power cycle.

Note: You can designate wireless or wired devices as key devices.

13.8 Problem Detection

Shows any devices that may be experiencing problems. Highlight **Problem Detection** on the **Test Results** screen and the status line shows the number of problems detected. The preview pane breaks down the problems into categories (**Errors** ● , **Warnings** ▼ , or **Info Messages** ! , and **Resolved** ✓). Tap the **Details** button to see a list of discovered problems.

The icon to the left of the device's MAC address indicates the device type. You can remove a problem from the list by highlighting it in the list and tapping the **Delete** button. Select the ⊞ icon next to the **Deleted problems** entry in the list to see all deleted problems.

Note: Deleted problems do not persist after a power cycle.

The problem conditions are given below:

Errors
- Rogue device
- Unprotected device
- Illegal Channel

Warnings
- AP Broadcasting SSID
- AP using Default SSID (this is the vendor designated SSID, not the configured default SSID for the Network Assistant)
- Low AP Tx Rate
- Low Client Tx Rate
- High AP Tx Retries
- High Client Tx Retries
- Client Authentication Failures
- Excessive Missed Beacons
- High Speed Not Supported

Info
There are currently no Info Messages.

14 Device Details

Highlight a device (e.g. in the Device Discovery list) and select the **Details** button to bring up the **Device Details** screen. The default view is the **Overview**. This gives you specific information about the type and configuration of the device, access to statistics information, and network tools that you can run that give you more information or help you troubleshoot your network.

Note: A device with an SSID that begins with an **>>** character indicates a devices that has multiple SSIDs. Each SSID is separated by **>>** (e.g. >>SSID1>>SSID2). Information about each SSID is shown in the **SSID** category of **Device Details**.

The preview pane gives you access to more statistics and network tools that you can use to analyze network performance or to troubleshoot network problems:

Signal Strength - monitor the Signal and Noise strength of the selected device
WLAN Statistics - monitor the packet types sent to/from the selected device
Tx/Rx Rates - monitor the packet transmission and receive rates for a device
Trace Route - determine the IP route and number of hops from the Network Assistant to another network device
Ping - test whether another network device responds to a PING
Wireless Throughput - measure the data rate to a device
Locate - use the signal strength measurement to physically locate a wireless device
Link - test whether the instrument is able to establish link with a selected AP
Login Diagnosis - monitor the communications between a device and an AP as the device establishes link

Note: Not all of the tools are available for every device. For example; Only **Login Diagnosis** can be run on devices with an unknown (unattached) SSID. Other tools require that the IP address of the device be identified or that the device be a mobile client.

15 Network Tools

Your EtherScope instrument incorporates a set of utilities that can be used for network troubleshooting and configuration. These **Network Tools** are available by tapping the 🔨 icon on the Task bar, or tools that are appropriate to a particular test can be accessed directly from the Preview Pane of a test.

The tools that are available are:

Tools Menu

Ping
Trace Route
Web Browser
Telnet
SSH Telnet
Terminal
FTP
TFTP
Wireless Throughput
Report

Preview Pane

Trace Route
Ping
Wireless Throughput
Locate
Login Diagnosis

If an individual device is selected within a test and a tool is selected, then that device is automatically selected as the target for the tool. If no device is selected, then you will be prompted to **Set Tool Target** when the tool is selected.

© 2004 - 2008 Fluke Corporation

Note: Not all of the tools are available for every device. For example; Only **Login Diagnosis** can be run on devices with an unknown (unattached) SSID. Other tools require that the IP address of the device be identified or that the device be a mobile client.

Note: In some cases, when a tool tries to connect directly to a device (e.g. when the Web Browser connects to a switch port), you will get a message that JavaScript language is required. Your EtherScope instrument does not support Java Virtual Machines and therefore, you will not be able to enable JavaScript language.

15.1 Ping

PING (Packet InterNet Groper) is a simple IP query and response process. Ping is an easy method to verify IP-level connectivity between the EtherScope instrument and another device. Highlight a device in a device list and run the **Ping** tool. The Network Assistant must have the SSID of the target device configured, must be able to establish link with an AP configured with that SSID, and identify the IP address of the target device.

15.2 Trace Route

Trace Route is a tool that determines the IP path used to reach a device. Trace Route shows the number of hops and the IP addresses of devices used to reach the destination device. Highlight a device in a device list and run the **Trace Route** tool. The Network Assistant must have the SSID of the target device configured, must be able to establish link with an AP configured with that SSID, and identify the IP address of the target device.

15.3 Web Browser

Select a device and then select the **Web Browser** tool. The Konqueror web browser that is included with the instrument will open and try to connect to the device that you selected. If no device is selected and the Web Browser is invoked, you will be prompted for the IP address.

Note: The Konqueror browser, as implemented, does not support Java Virtual Machines.

Among other uses, the **Web Browser** is useful for checking or changing network device configurations (also see Telnet or SSH Telnet).

Note: If you configure a proxy server for the web browser (under ▤ **| Preferences | Network**), you must use the http:// notation (e.g. http://1.160.10.240). You may also have to designate the port number as part of the IP address (e.g. http://1.160.10.240:8080, where 8080 is the designated port).

15.4 Telnet

Telnet is a program that lets you access a remote computer. When you run **Telnet**, the **Set Tool Target** popup opens where you can enter the IP address of the device to which you are trying to connect (the IP address is automatically entered if a device is already selected on a test screen). An EtherScope Console window opens where you can log in to the device and then work from the instrument as if it were a terminal that is hardwired to the remote device.

Among other uses, **Telnet** is useful for checking or changing network device configurations (also see Web Browser).

15.5 SSH Telnet

SSH Telnet is a secure version of the Telnet program that lets you access a remote computer. When you run **SSH Telnet**, the **Set SSH Target and Options** popup opens where you can enter the IP address of the device to which you are trying to connect (the IP address is automatically entered if a device is already selected on a test screen) and the Username. An EtherScope Console window opens where you can log in to the device and then work from the instrument as if it were a terminal that is hardwired to the remote device.

Among other uses, **SSH Telnet** is useful for checking or changing network device configurations (also see Web Browser).

15.6 Terminal

This tool allows you to use the instrument as an ASCII terminal. For example, you can connect a serial cable from the instrument to a network switch and use the **Terminal** tool to configure the switch. Selecting **Terminal** opens the **EtherScope Console** window for the user interface. Communication to and from the instrument is through the serial port. You can use the on-screen or a remote keyboard to enter commands.

There is a pull-down **Command List** where you can store frequently used commands or key sequences. Select **Edit Command List** on the **Options** menu to modify the available commands. You can open multiple windows by either selecting **Terminal** from the tools menu or selecting the terminal icon ▣ on the toolbar of the **EtherScope Console** window. A tab at the bottom of the window indicates which **Terminal** window is currently open.

15.7 FTP

Opens an **FTP** (File Transfer Protocol) session with a device. Highlight a device in a device list and run the **FTP** tool or select the tool and enter the IP address of the device. **FTP** can be used to move files between computers. The Network Assistant must be able to establish link with an AP, acquire an IP address for itself, and identify the IP address of the target device.

15.8 TFTP

Opens a **TFTP** (Trivial File Transfer Protocol) session with a device. **TFTP** can be used to move files between computers. Highlight a device in a device list and run the **TFTP** tool, or select the tool and enter the IP address of the device. You will also select either **Get** or **Put**, indicating the direction of the file transfer, and enter the name of the file to be transferred.

Trivial **F**ile **T**ransfer **P**rotocol is a simple form of the **F**ile **T**ransfer **P**rotocol (FTP). TFTP uses the User Datagram Protocol (UDP)and provides no security features.

15.9 Wireless Throughput

The Wireless Throughput test allows you to check the transmit and receive rate to and from a device (tx and rx checked when using Ping but rx only when using FTP). The test is available from the Preview pane of the Test Results screen. Select a device and then tap the Wireless Throughput entry. Because the test measures throughput using either Ping or FTP to generate traffic, the selected device must have an IP address identified by the Network Assistant. The instrument attempts to resolve the device's IP address before starting the test.

Prior to starting the test, the Network Assistant must link to an AP configured with the same SSID as the target device, which means that Wireless Security must be configured for the SSID associated with the device. If the SSID is not configured, then a popup is displayed indicating the inability to link. Also, you can not run the test on devices with an Unknown SSID.
If you have selected a mobile client as the remote unit for the test, then you must select an AP to which the instrument will link. When you start the test (and the SSID is configured) a popup appears that allows you to choose either the Best AP (based on signal strength) or a specific AP from the list (if you want to test throughput using that specific AP). Select OK after you have made your selection and the

Wireless Throughput test will begin automatically (after link has been established). If an AP was selected as the remote unit, then the test will start automatically.

The test starts using PINGs to test the throughput capability. If the remote unit has an FTP server, you can change the Throughput Protocol to FTP. Tap the Stop button and enable the FTP radio button. This will enable the Username and Password fields, where you can make the appropriate entries that will allow access to the remote device. Tap the Start button to begin the test.

The graph shows the Average and Last throughput rate. The table below the graph shows the Average, Last, Best, and Worst values for the current test. The test stops when you tap the Stop button or exit the screen.

When using FTP to test throughput, the test searches the remote device for a file from 1 MB to 10 MB in size and uses that file for the test. Otherwise, a file (q23k5zy7.dat) will be written to the remote device if a directory with write access can be located. This same file will then be read repeatedly. At the end of the test, the file will be removed from the remote device. However, if the directory has no delete permissions the file will be left on the device.

15.10 Report

Most tests have a **Report** button available that will save the current test results in an XML-formatted file that is stored on a CompactFlash memory card (slot 2 of the instrument). The Report capability is also available from the Tools menu.

Note: The Report selection is disabled if the feature is not available for the selected test.

When you select **Report**, you will see the **Compact Flash Reports** popup. From here, you can create a new report or delete an existing one. When you select the **New Report** button, you will be asked to name the file. You can also add a comment to the report before you save it. See the description below.

You can also view the Reports by using a PC to access them directly from the CompactFlash (directory path \Reports). Remove the CompactFlash from the instrument and install it in your PC. You can use Microsoft Internet Explorer or Microsoft Excel to view the reports (reports are in XML format).

User Supplied Graphic

You can add a custom graphic to your EtherScope report headers that will be visible when viewed from a PC. Add a .gif formatted graphic file named *yourCompanyLogo.gif* to the root directory of the CompactFlash card. The user supplied graphic will be displayed in a 180x70 pixel area on the left side of the report header. If the user chooses to not put their graphic on reports, the Fluke Networks logo will be displayed in place of the optional user graphic.

Note: The filename is case sensitive and should be named exactly as shown.

User Supplied Comment

You can add and display an optional user supplied Instrument Comment on EtherScope reports. Place a plain-text file named *instrumentComment.txt* in the root directory of the CompactFlash card. The text in the Instrument Comment file will be displayed in the footer of EtherScope Reports when viewed from a PC or printed. If no comment file is provided, the Report Comment line will not be displayed.

Note: The filename is case sensitive and should be named exactly as shown.

Job Comment

You can add a unique comment when you save a report. After you select **New Report** and enter the filename, you can enter information in the **Comment** field. This comment will be shown in the **Report Comment** field at the bottom of the report and will replace the **User Supplied Comment** described above.

Viewing Reports

A directory of saved reports can be viewed from the desktop **Reports** tab. Tap the Desktop icon on the status bar and select **Applications** from the menu and then select the **Reports** tab to view the list of saved reports. Double tap a report in the list to view its contents.

15.11 Locate

The **Locate** function uses a directional antenna and enables you to find a device by using its signal strength to home in on its location. For example, you can use the **Locate** tool to find an AP that is above the ceiling tiles in an office, or to find an unauthorized device that is on your network. The **Locate** function is available on the Device Details preview pane.

The signal strength is indicated by a "speedometer" gauge and also by sound (headphones recommended though the sound is audible). The sound allows you to focus on finding the device without looking at the gauge. You can adjust or mute the sound level by tapping the sound icon .

The signal strength is charted on a bar graph or indicated by a "speedometer" gauge and also by sound (headphones recommended though the sound is audible). The power level is shown in dBm. Use the **Style** radio buttons to switch between **Chart** and **Meter**.

In **Chart** mode, use the pull-down menus to set how often the graph is updated (**Period**) and the scale of the graph (**Range**). If you set the **Range** to **Auto**, the scale automatically adjusts to best fit the samples. Use the **Pause** button (changes to **Resume**) to stop the sampling and the **Clear** button to erase the collected samples. The red line on the graph indicates the maximum value detected for the session, while the yellow line indicates the minimum value for the session.

In **Meter** mode, increase or decrease the **Scale** value so that you get the best resolution on the graph. The scale settings multiply the signal strength (Low - .67x, Medium - 1x, High - 2x). Typically, you would use a higher scale the further away you are from the device to be located and progressively lower the scale to gain more resolution as you get closer. If the signal strength is too high on the graph and you do not have enough resolution to accurately locate the device, decrease the Scale value (i.e. High -> Medium or Medium -> Low). Likewise, if the signal strength is too low to get accurate resolution, increase the Scale value. If a device is not actively transmitting, the gauge will freeze on the last signal strength reading for about 10 seconds and then drop to 0% until the device resumes transmitting. In addition, the Last Seen time will not update and you will not hear beeps. A grey "shadow" area behind the needle on the gauge indicates the signal strength boundaries. The box directly below the needle shows the relative signal strength of the device to be located.

While carrying the instrument with the **Locate** function activated, hold the flag of the directional antenna upright (verify that it is plugged in to the radio card) and slowly rotate it. Observe the direction of the flag when the graph indicates the strongest signal. The flag points to the device in question. Move in that direction until you observe the strongest signal (the signal strength will decrease as you move past the device). As you move in the direction of the device, continue to rotate the flag and observe the signal strength. Make adjustments as necessary in the direction that you move in order to move in the direction that gives the strongest signal strength.

If you do not use the **Auto** setting for the **Range**, increase or decrease the **Scale** value so that you get the best resolution on the graph. Typically, you would use a higher scale the farther away you are from the device to be located and progressively lower the scale to gain more resolution as you get closer. If the signal strength is too high on the graph and you do not have enough resolution to accurately locate the device, decrease the **Scale** value (i.e. **High** -> **Medium** or **Medium** -> **Low).** Likewise, if the signal strength is too low to get accurate resolution, increase the **Scale** value.

You can use the **Locate** function without the directional flag, you just need to move back and forth in a grid pattern across the facility to find the location with the highest signal strength. The orientation of the instrument affects the signal strength (try holding it vertically) and your body may shield the signal. Try standing in one spot while holding the instrument vertically and close to you. Slowly rotate in a circle while observing the signal strength graph. The smallest reading should be when your back is to the device in question.

15.12 Login Diagnosis

The **Login Diagnosis** test allows you to view the link process of a wireless client connecting to an AP. The test is available on the Preview pane of Device Details when a mobile client is selected.

Note: Wireless Security for the client or the AP does not have to be configured for this test.

You must select an AP for the test. The test sends a spoofed Disassociate message to the client, which causes the client to unlink from the AP. The test then monitors and records the login process as the client relinks to the AP. You can use the pull-down menu in the **Target AP** to select a specific AP (if you know that the client will link to this AP), or select **ANY** (found at the top of the list).

After the AP is selected, tap the **Start** button. As the relink progresses, the results are shown in the **Test Phase** field of the screen. A time stamp next to each entry shows the real-time progress (relative to the start of the test) of the link process. The **Test Diagnosis** field shows the final results. Tap the Report button to save the results of the test.

Note: If the client does not accept the Disassociate message, you will need to start the test and then manually cause the client to unlink and relink from the AP (cycling power on the client (PC or laptop) is an easy way to accomplish this).

16 Signal Strength

The **Signal Strength** screen shows a graph of the minimum and maximum detected signal and noise values for the selected device. **Signal Strength** can be used to verify the quality of the RF signal of a device. Select a device in Device Details and tap **Signal Strength** in the preview pane to view the graph.

The bar graph shows four values: maximum signal strength, minimum signal strength, maximum noise strength, and minimum noise strength.

Note: You can select whether the signal strength measurement is shown as a percentage or in dBm on the Wireless Instrument Settings - Radio screen.

By default, the cursor is on the far right side of the graph and the values for the sample are shown at the bottom of the screen. You can drag the cursor to a particular data point and the values are shown for the selected time period. The cursor will move with the selected data point until it scrolls off and at that point the cursor is repositioned to the most current data point where it will stay until moved. You can use the **Pause** (changes to **Resume**) button to stop the graph from updating so that have more time to review the data. You can move the cursor on the graph to inspect the data at different time samples. Tap the **Resume** button to resume updates (the graph will jump to the current time statistics samples). Tap the **Clear** button to reset all the statistics on the screen. Use the pull-down menu in the **Update every** field to change the sample period from between 1 second and 60 minutes (default is 5 seconds).

The **Signal Strength** measurement begins when you select the test. No data is stored and the measurement stops when you exit the screen.

17 WLAN Statistics

The **WLAN Statistics** screen shows a graph of the packet types transmitted and/or received for the selected device. This test can be used to verify the type of traffic coming from a device. Identifying the types of packets coming from a device gives you a clue about its performance **-** too many **Retries** might indicate a device that is too far away from an AP or a weak WLAN NIC. Select a device in Device Details and tap **WLAN Statistics** in the preview pane to view the graph.

The bar graph at the top of the screen shows the packet types (you can also show the data in bytes) By default, the cursor is on the far right side of the graph and the values for the sample are shown at the bottom of the screen. You can drag the cursor to a particular data point and the values are shown for the selected time period. The cursor will move with the selected data point until it scrolls off and at that point the cursor is repositioned to the most current data point where it will stay until moved. You can use the **Pause** (changes to **Resume**) button to stop the graph from updating so that have more time to review the data. You can move the cursor on the graph to inspect the data at different time samples. Tap the **Resume** button to resume updates (the graph will jump to the current time statistics samples). Tap the **Clear** button to reset all the statistics on the screen. Use the pull-down menu in the **Update every** field to change the sample period from between 1 second and 60 minutes (default is 5 seconds).

The **WLAN Statistics** measurement begins when you select the test. No data is stored and the measurement stops when you exit the screen.

18 Tx/Rx Rates

The **Tx/Rx Rates** screen shows a table of the percentage of packets transmitted and received on each bandwidth of the wireless spectrum for the selected device. The transmission and receive rates for a device can give you a clue about its performance and aid in troubleshooting (e.g. a large number of packets transmitted at a very low rate can negatively impact the available bandwidth and the performance of the network). Select a device in Device Details and tap **Tx/Rx Rates** in the preview pane to view the table.

The **Tx/Rx Rates** measurement begins when you select the test. No data is stored and the measurement stops when you exit the screen.

19 Link

The **Link** utility tests whether the instrument can establish link with a selected AP. The **Link** utility is available when you select an AP device in Device Details.

Note: Wireless Security must be configured for the SSID of the AP for which link is trying to be established.

When link is established, you will see two bar graphs showing **Signal Strength** and **Signal Quality** of the AP. In addition configuration information of the Network Assistant is shown. Link is disengaged when you exit the screen.

Index

© 2004 - 2008 Fluke Corporation

Tequipment.NET USA
205 Westwood Ave
Long Branch, NJ 07740
1-877-742-TEST (8378)
Fax: (732) 222-7088
salesteam@Tequipment.NET