EtherScope™ Series II

Network Assistant

Getting Started Guide

PN 2633787
May 2006, Rev. 1, 9/06

LIMITED WARRANTY AND LIMITATION OF LIABILITY

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

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

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

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

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

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

4/04

Fluke Networks
PO Box 777
Everett, WA 98206-0777
USA

End User License Agreement (EULA)

The enclosed software product is furnished subject to the terms and conditions of the agreement. Retention of the software product for more than thirty days, opening the sealed wrapper surrounding the product, or use of the product in any manner will be considered acceptance of the agreement terms. If these terms are not acceptable, the unused product and any accompanying written material should be returned promptly to the Fluke Corporation or the place of purchase for a full refund of the license fee paid.

1. GRANT OF LICENSE. Fluke Networks, a division of Fluke Electronics Corporation (Fluke Networks) grants you the right to use the enclosed software in accordance with the terms of this EULA.

2. TITLE, COPYRIGHT AND TRADEMARK. This software product is owned by Fluke Networks or its suppliers and is protected by United States copyright laws and international treaty provisions. Therefore, except for the rights granted to you above, you must treat the software product like any other copyrighted material, and copies must include the proper copyright notice.

3. RESTRICTIONS. You may not reverse engineer, decompile, or disassemble the software. If the software product is an update, any transfer must include the update and all prior versions.

You may use the software only in conjunction with the Fluke Networks products for which it is intended.

You may not export or re-export the software to any country to which such export or re-export is restricted by law or regulation of the United States, or any other government having jurisdiction, without prior permission from Fluke Networks.

4. TERM. This license is effective upon your acceptance of the above agreement and shall remain in effect until termination by (a) written notification to Fluke Networks or (b) a failure on your part to comply with the license agreement. Upon termination of the license agreement, you shall return to Fluke Networks or destroy all copies of the software product and associated written materials.

5. OTHER AGREEMENTS. Where terms or conditions of this agreement conflict with the terms or conditions of other agreements, this agreement supersedes other agreements.

End User License Agreement (continued)

6. LIMITED WARRANTY. Fluke Networks warrants that the software product will perform in its intended environment substantially in accordance with the accompanying written materials for a period of 90 days from the date of license acceptance. Fluke Networks further warrants that the original copy of the software has been recorded on non-defective media. Fluke Networks does not warrant that the software will be error free or operate without interruption.

7. REMEDIES. Fluke Networks' entire liability and your exclusive remedy shall be Fluke Networks' option, (a) the return of the price paid for the product, or (b) repair or replacement of the software product that does not meet the limited warranty. This limited warranty is void if failure of the product has resulted from accident, abuse, or misapplication. Any replacement software product will be warranted for the remained of the 90-day original warranty period or 30 days, whichever is longer.

8. NO OTHER WARRANTIES. FLUKE NETWORKS DISCLAIMS ALL OTHER WARRANTIES, EITHER EXPRESS OR IMPLIED BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THE SOFTWARE PRODUCT AND THE ACCOMPANYING WRITTEN MATERIALS. In no event shall Fluke Networks or its suppliers be liable for any damages whatsoever (including, without limitations, indirect, consequential, or incidental damages, damages for loss of business profits, business interruption, loss of business information, or other pecuniary loss) arising out of the use or inability to use this software product, even if Fluke Networks has been advised of the possibility of such damages.

This agreement and license shall be governed in the Unites States by the laws of the State of Washington, U.S.A., and elsewhere by the laws of the country within which the agreement is made.

Trademark Disclosure

Qtopia™ is a trademark of Trolltech, Inc.

CompactFlash® is a registered trademark of the CompactFlash Association.

CardBus® logo is a registered trademark of PCMCIA/JEiTA.

Linux® is a registered trademark of Linus Torvalds.

All trademarks are acknowledged.

Software Notice

The EtherScope™ Series II 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) and visit the GNU web site (http://www.gnu.org) for more information.

Contains MatrixSSL™ security software licensed from PeerSec Networks Inc. See http://www.peersec.com for more information on MatrixSSL™ software.

Table of Contents

Title **Page**

List of Tables

List of Figures

EtherScope™ Series II Network Assistant

About This Guide

This *EtherScope™ Series II Network Assistant Getting Started Guide* introduces you to the features and functions of your EtherScope™ Series II Network Assistant and provides basic instructions for setting up and operating the instrument. The information in this guide is designed to help you become comfortable using your new instrument. After reading this guide, you will find the online help system the best source for answering questions and helping use the product to maintain your network and troubleshoot problems as they arise.

Introduction

EtherScope™ Series II Network Assistant (hereafter also referred to as “the instrument” or “EtherScope Network Assistant”) is a portable, integrated network test tool designed to assist you with installing, monitoring, and troubleshooting wired and/or wireless Local Area Networks (LANs). EtherScope Network Assistant gives you instant visibility into your network, providing crucial information about its health and status so that you can proactively identify and solve problems before they impact performance.

Features

EtherScope Network Assistant provides critical performance metrics about your wired and wireless LANs. The instrument's autotest feature quickly verifies performance at the physical layer, discovers networks and devices, and identifies configuration and performance problems. For in-depth analysis, the instrument also includes a group of diagnostic tools to enable you to locate devices on your network and verify inter-connectivity.

The instrument's user interface, which is presented on a color, touch-sensitive screen, is straightforward and intuitive. Simply by tapping a screen button, a navigation icon, or other on-screen element, you can "drill down" and obtain more detailed information or perform a specific operation.

Available Models

EtherScope Network Assistant is available in the following models:

- Wired LAN model (ES2-LAN): a base model that supports monitoring and testing of 10/100/1000 IEEE 802.3 (10BaseT, 100BaseTX, and 1000BaseT) networks through an RJ-45 interface, and the optional SFP fiber interface that supports 1000BaseSX, 1000BaseLX, and 1000BaseZX fiber. Discovers devices, networks, and VLANs, enabling you to view individual configurations, obtain health and status information, and view network activity, errors, and protocols used.

- Wireless LAN model (ES2-WLAN): a base model that supports monitoring and testing of 802.11 a/b/g devices connected to a wireless LAN. Automatically scans all channels to gather and report statistics on the health and status of the network. Discovers access points (APs) and client devices, identifies "top talkers", locates rogue devices and flags security problems. Enables you to perform site surveys so that you can make sure that all areas of your network have adequate signal coverage. Also performs security login verification.

- EtherScope Pro (ES2-PRO): a single integrated wired/wireless analyzer that combines the features of the wired and wireless models (described earlier).

- EtherScope Pro with the Internet Throughput Option (ES2-PRO-I): a single, integrated wired/wireless analyzer that combines the features of the wired and wireless models (described earlier). This model includes the Internetwork Throughput Option (ITO). See the description of the ES-ITO-OPT option under "Available Options".

Available Options

You can expand your ability to monitor and troubleshoot your site's LANs by adding the following options to a base-model EtherScope Network Assistant:

- ES2-WLAN OPT: extends the network test capability of an ES2-LAN to include support for monitoring and testing of 802.11 a/b/g wireless LAN. See the description of ES2-WLAN model under "Available Models".

- ES2-LAN OPT: extends the network test capability of an ES2-WLAN to include support for monitoring and testing of 10/100/1000 IEEE 802.3 (10BaseT, 100BaseTX, and 1000BaseT) networks through an RJ-45 interface. See the description of ES2-LAN model under "Available Models".

- ES2-ITO-OPT: (Internetwork Throughput Option) enables you to test the bandwidth available between two nodes on a network. This option enables the EtherScope Network Assistant to generate a background traffic load to test new systems and configuration or to simulate the impact of additional users on a network.
- ES2-SX-OPT: enables the SFP fiber interface. Supports 1000BaseSX, 1000BaseLX, or 1000BaseZX fiber.

For information on these options, contact Fluke Networks.

Package Contents

Take a moment to check the shipping container to make sure that the contents match each numbered standard accessory that is shown in Figure 1 and the accompanying list in Table 1.

If any item is damaged, call the carrier at once for inspection and request an inspection report. Please do not write the factory until you have notified the carrier, since this will delay your claim. If this precaution is not taken, we cannot assist you in recovering the amount of the claim against the carrier.

After you obtain the carrier's inspection report, immediately return the instrument along with a copy of the inspection report to the factory. See “Contacting Fluke Networks” on page 13 for various ways to contact us.

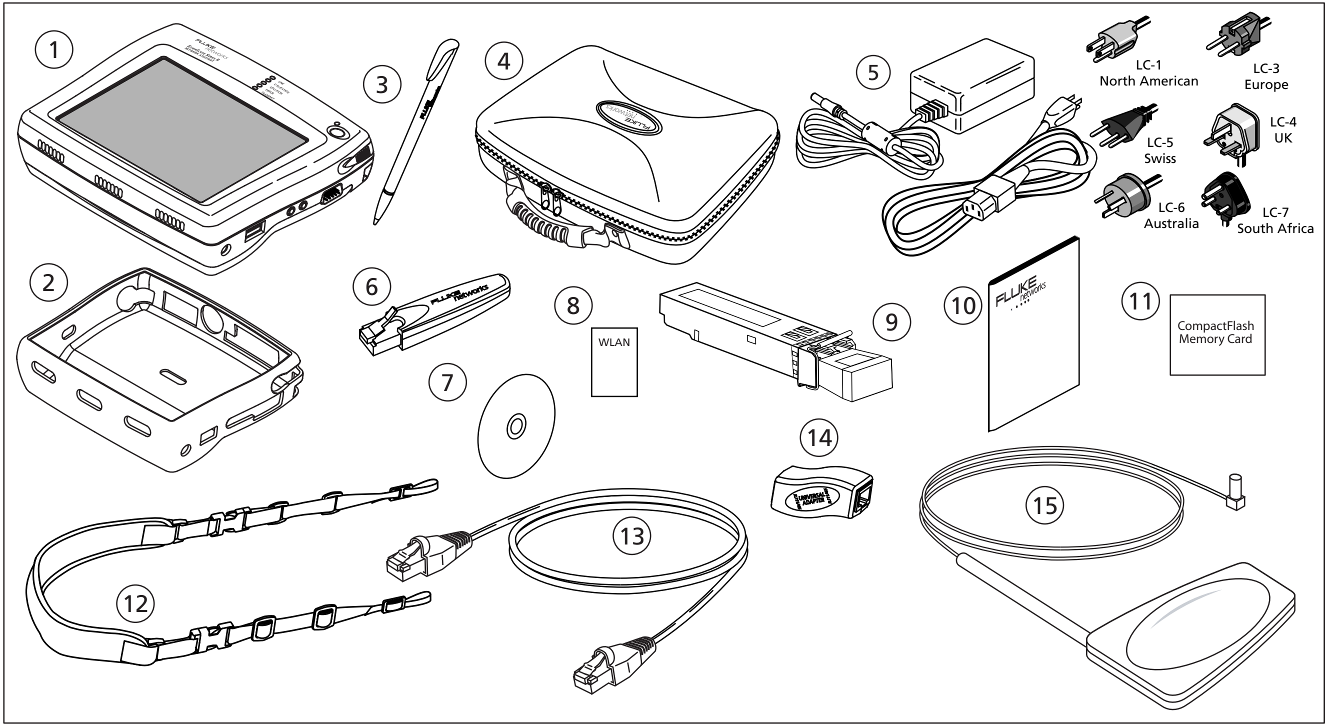


Figure 1. Standard Accessories

Table 1. List of Standard Accessories

Item Number	Item	Description
①	EtherScope™ Series II Network Assistant	EtherScope Series II Network Assistant mainframe.
②	Holster	Removable, form-fitting yellow holster.
③	Stylus	Stylus for use with the instrument’s touch screen display.
④	Storage Case	Case for carrying and storing the instrument.
⑤	External AC adapter, charger, power cord	Input: 90V -264V AC, 50/60Hz; Output: 15V DC, 1.3A (20W); Power Cord termination varies by country.
⑥	WireView™ wiremap adapter (office locator)	Cable termination device with office locator ID #1. Used to perform the Cable Test wiremap operation and used as an office locator.

Table 1. List of Standard Accessories (continued)

Item Number	Item	Description
⑦	CD-ROM	EtherScope Resource CD. Includes On-line Help and Getting Started Guides.
⑧	WLAN card	Fluke Networks EtherScope Wireless LAN Adapter IEE 802.11 a/b/g. This is a standard accessory for the ES2-WLAN, ES2-PRO, and ES2-PRO/I models.
⑨	ES2-SX-Pro fiber adapter	Fluke Networks EtherScope Fiber LAN Adapter 1000BASE-SX. This is a fiber accessory for the ES2-SX-PRO, and ES2-SX-PRO/I models. Also available are the 1000Base-LX and 1000BASE-ZX option.
⑩	Getting Started Guide	Provides basic operating and introductory troubleshooting information, lists of accessories, and specifications.
⑪	CompactFlash® memory card	CompactFlash® memory card used for saving reports.
⑫	Carrying Strap	Strap clips to the instrument for easy carrying.

Table 1. List of Standard Accessories (continued)

Item Number	Item	Description
⑬	Network Patch Cord	1 meter patch cord.
⑭	Universal adapter	RJ-45 Female to female adapter. It is intended to be used to connect a RJ-45 Ethernet cable from the instrument to a WireView™ wiremap adapter.
⑮	External directional antenna	Directional antenna for use with WLAN card to locate WLAN devices
Not Shown	Battery Pack	Rechargeable Lithium Ion battery pack installed in the instrument.

Optional Accessories

Additional accessories available for purchase for your EtherScope Network Assistant are listed in Table 2. Contact Fluke Networks for buying information (see "Contacting Fluke Networks" on page 13).

Table 2. Optional Accessories

Item	Description
EtherScope Extended Test Kit	The EtherScope Extended Test Kit includes additional accessories: spare rechargeable battery, external battery charger, external mini keyboard, wiremap adapters (#2-6)
WireView wiremap adapters	Set of five wiremap adapters with office locator IDs #2 through #6
External Keyboard	USB mini keyboard
Battery Pack	Rechargeable Lithium Ion battery pack
External Battery Charger	External battery charging station

Safety and Operational Information

The international electrical symbols used in this document and on the instrument are described in Table 3.

Table 3. International Electrical Symbols

⊗	Not for connection to public telephone systems	SP ® c US	Complies to CSA C22.2 No. 950 Canadian standards, and UL 1950 (US standards)
⚠	Please read the manual for safety information	☒ Li	Do not dispose of Lithium Ion batteries in garbage, recycle
CE	Complies with European Union Directive	✓ N10140	Meets Australia EMC requirements
⚡	Shock hazard	♻	Recycle Lithium Ion batteries
✺	Class 1 Laser Product. Do not look into the laser.		

Please observe the following safety regulations when using your EtherScope Network Assistant:

⚠ ⚠ Warning Class 1 Laser Product

This product contains a Class 1 laser (EtherScope Fiber Models). Do not look into the laser port because this may cause eye injury.

⚠⚠Warning

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

- **Do not use this product if it is damaged. Before using the product, inspect the case. Look for cracked or missing plastic.**
- **Do not operate the product around explosive gas, vapor, or dust.**
- **Do not open the case. There are no user-serviceable parts inside.**
- **Do not connect a telephone line to this product.**
- **If this product is used in a manner not specified by the manufacturer, the protection provided by the product may be impaired.**

⚠Caution

- **To avoid possible damage to the instrument and to the equipment under test, use the proper terminals and cable for all connections.**
- **Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposure (EtherScope Fiber Models).**

Registering Your EtherScope Series IINetwork Assistant

Take the time to register your instrument. The EtherScope Resource CD contains registration information and instructions.

You can also register the instrument by going to our website at www.flukenetworks.com. To register:

1. Click **support**, then click the **Registration** link to display a login screen.
2. Do one of the following:
   - If you are a returning visitor, follow the login instructions.
   - If need to set up an account, click **Create** then follow the new account instructions.
3. Click **Register your product** and fill out the online registration form.

As a registered user, you are entitled to entry-level product support. This includes basic access to the online Knowledge Base library of product operation and application information and web-based trouble ticketing. In addition, you will receive Fluke Networks company and product information updates.

After registering the product, make sure that you have the latest software installed. See “Updating the Instrument’s Software” on page 17 for details.

Care and Maintenance

To obtain reliable test results, always follow proper cleaning and maintenance procedures:

- To prevent moisture from entering the instrument, clean the front panel touch screen with a moist cloth only.
- Do not spray water directly on the front panel touch screen. Wipe the case with a damp cloth.
- Do not use organic solvents, acid, or alkali solutions.

Contacting Fluke Networks

To order accessories or to find out the location of the nearest Fluke Networks distributor or service center, contact us using any one of the following methods:

ℹ www.flukenetworks.com

✉ support@flukenetworks.com

☎ +1-425-446-4519

- Australia: 61 (2) 8850-3333 or 61 (3) 9329 0244
- Beijing: 86 (10) 6512-3435
- Brazil: 11 3044 1277
- Canada: 1-800-363-5853
- Europe: +44 –(0)1923 281 300
- Hong Kong: 852 2721-3228
- Japan: 03-3434-0510
- Korea: 82 2 539-6311
- Singapore: +65-6799-5566
- Taiwan: (886) 2-227-83199
- USA: 1-800-283-5853

Visit our website for a complete list of phone numbers.

Before You Begin

The information in this section acquaints you with the basic operations and functions of your instrument so that you can start using it immediately. You will learn how to:

- Turn on the instrument and configure the interface type for testing an Ethernet 802.3/802.1x wired or an 802.11 wireless network
- Adjust the brightness of the screen
- Set the date and time
- Update the instrument’s software
- Charge the battery
- Navigate the user interface and understand the meanings of the LEDs
- Get Help

Turning the Instrument On and Off

To turn the EtherScope Network Assistant on, press the green **On/Off** button. This button is located on the right side of the instrument’s front panel.

The front page **Test Results** screen is displayed (see Figure 6 or Figure 24).

Note

When you turn on the instrument (wired mode only), you may hear a series of clicks. These sounds are a normal part of the boot-up and cable testing process and do not indicate a problem with the instrument.

To turn off the instrument, press and hold the **On/Off** button until the instrument turns off (approximately two seconds). The **On/Off** LED will blink when the instrument is turned off and connected to the AC adapter charger indicating that the battery is charging.

Using the Stylus

The stylus, which is used for navigating the user interface, is stored in the right side panel near the green **On/Off** button.

In the same way that you use a mouse to click elements on your computer screen, you use the stylus to “tap” elements on the instrument’s touch-sensitive screen.

To select elements and execute commands, simply tap the item with the point of the stylus. In addition, use the stylus to drag a slider or move the scroll box on the scroll bar.

Note

Always use the point of the stylus to tap the screen. We do not recommend that you use a pen or pencil or any other sharp object that might scratch the finish.

Selecting the LAN or WLAN Interface

If your instrument has the capability to test both a wired LAN (RJ-45 or SFP fiber interfaces) and a wireless LAN, you need to specify which technology you are testing.

1. On the front page, do the following:

   - Tap WLAN Tests (see Figure 6) to test wireless interfaces.

     OR

   - Tap LAN Tests (see Figure 24) to test the RJ-45 or SFP fiber interfaces.

2. On the **Change Active Port** screen, tap OK to change the interface.

   The instrument resets itself and runs autotest on the selected interface.

   Note

   The interface type you select remains the same even after you power off the instrument.

Adjusting the Brightness of the Screen

Note

> *The degree of brightness is a significant factor in conserving battery power. Turning the brightness up causes the instrument to use more battery power.*

To adjust the brightness:

1. Tap then select **Settings**.
2. Tap the **Light & Power** icon.
3. On the **Light and Power** screen, you can do the following:
   - Select the desired **Power saving** settings. To do this, tap (to check) an option. Then, for each option, specify a time interval.
   - Adjust the brightness. To do this, tap and drag the slider control until the desired level of brightness is achieved.
4. Click OK to save the settings.

Setting the Time and Date

The current time is displayed in the lower right corner of the status bar. To change the time and date, do the following:

1. Tap the current time.
2. Select **Set time** to display the **Date/Time** screen.
3. Select date and time settings and formats.
4. Tap OK to save your changes.

   The instrument now displays the new time on the status bar.

Updating the Instrument’s Software

To update the instrument’s software, do the following:

1. Insert a CompactFlash memory card into **SLOT 2**.
2. Tap the EtherScope Network Assistant icon , which is located in the upper-left corner of the screen
3. From the drop-down list, select **Instrument Settings**.
4. In the preview pane, tap **Version**.

   The **Instrument Settings—Version** screen displays the versions of currently installed software and hardware.
5. To check for updates, tap Check for software updates.

   The instrument automatically checks to determine whether a software update is available.
6. When prompted, tap Yes to download the update files to the CompactFlash memory card.

   Note

   All files and reports on the CompactFlash memory card will be erased.
7. After you are notified that the download is completed, tap OK.
8. With the CompactFlash card in **SLOT 2,** restart the instrument to begin installing the software.

   Note

   A software update can take up to five minutes.

After installation is completed, the instrument automatically restarts and you can resume testing.

If you encounter trouble updating the software, contact our Technical Assistance Center. See “Contacting Fluke Networks” on page 13 for contact information.

Recalibrating the Screen

The touch-sensitive screen is calibrated at the factory. Though unlikely, the instrument may not respond properly when you tap the stylus on the screen. If this happens, you may need to recalibrate the screen. Recalibration aligns the instrument's internal circuitry with the screen so that it can correctly detect taps with the stylus.

To recalibrate your screen:

1. Using the stylus, tap the desktop icon , which is located in the lower-left corner of the screen. From the menu, select **Settings**.
2. On the **Settings** screen, tap the **Recalibrate** icon .

Follow the prompts to complete the recalibration.

Enabling Software Options

If you purchased a software option for your EtherScope Network Assistant, you received a proof-of-purchase code along with a software option activation instruction card. Follow the instructions on the card to obtain a key code from the Fluke Networks website and use that key code to activate your option.

Note

If you need help obtaining your key code, contact Fluke Networks for assistance. See "Contacting Fluke Networks" on page 13 for information on how to contact us.

To enable one or more software options, have your instrument's key code handy, and then do the following:

1. Tap (located in the upper-left corner of each screen).
2. From the drop-down list, select **Instrument Settings**. Then, in the preview pane, tap the **Options** hyperlink.

   The **Options** screen is displayed.

3. In the **Current Key Code** box, enter your key code.

   Note

   You can use a remote keyboard or tap ⌨ to access the virtual keyboard.

4. In the **EtherScope Options** group, tap (to check) each software option that you want to activate.

5. Tap Apply

   The software options you selected are now enabled.

Displaying Hardware and Software Version Information

1. Tap the EtherScope Network Assistant icon, which is located in the upper-left corner of the screen

2. From the drop-down list, select **Instrument Settings**.

3. In the preview pane, tap **Version**.

   The **Instrument Settings—Version** screen displays the versions of currently installed software and hardware.

The Power Supply

You can operate the instrument by using the rechargable Lithium-Ion battery. Alternatively, you can use the supplied AC adapter charger (with or without the battery installed).

Note

Although the instrument can run on the AC adapter without the battery pack installed, this method is not recommended. The battery pack provides stability for the instrument when you are using the stand.

Operating the Instrument on Battery Power

When the instrument is running on battery power, it is capable of approximately four full hours of operation in wired mode and 3.5 hours in wireless mode. The instrument comes packaged with the battery installed. To operate on battery power, simply turn the instrument on.

Although the battery is pre-charged at the factory, you should fully charge it before you begin using the instrument. This is an important step because if the power source is interrupted while you are operating the instrument, you will lose data.

Charging the Battery

Figure 2 shows you how to charge the battery. Note that you can charge the battery while it is installed or you can remove it and charge it in an external battery charger.

Note

*The **On/Off** led will blink when the instrument is turned off and connected to the AC adapter charger.*

You can purchase an extra battery and/or charger separately or as part of the EtherScope Network Assistant Extended Kit (see Table 2).

When fully discharged, the battery takes approximately 4 1/2 hours to reach a full charge if the instrument is powered off. It takes approximately 7 hours to fully charge the battery if the instrument is powered on.

Checking the Status of the Battery Charge

To find out how much battery power remains, tap the battery icon 🔋, which is located in the lower-right corner of every screen.

Conserving Battery Power

One way to conserve battery power is to put the instrument in **Suspend** mode. This is a low-power usage mode, in which the instrument is not completely turned on or off. While in **Suspend** mode, the instrument cannot collect data.

- To put the instrument in **Suspend** mode, tap 🟩 then select ⏻ **Suspend**. Alternatively, press the green **On/Off** button for less than one second.

  The green LED turns amber and the screen changes to blank.

- To take the instrument out of **Suspend** mode, press the **On/Off** button. Release this button as soon as the LED turns green.

  The screen that was displayed prior to your putting the instrument in **Suspend** mode is redisplayed.

Note

Another way to save battery power is to use a lower backlight setting. See "Adjusting the Brightness of the Screen" on page 16 for details.

Removing and Installing the Battery

The battery is located behind the product stand.

To remove the battery, refer to the diagram in Figure 2 and do the following:

1. Make sure that the instrument is turned off.
2. Remove the yellow holster and pull the stand up.
3. Push the release tab away from the battery.
4. Pull up on the end of the battery that is close to the release tab to disengage the connections. Then, lift the battery out of the compartment.

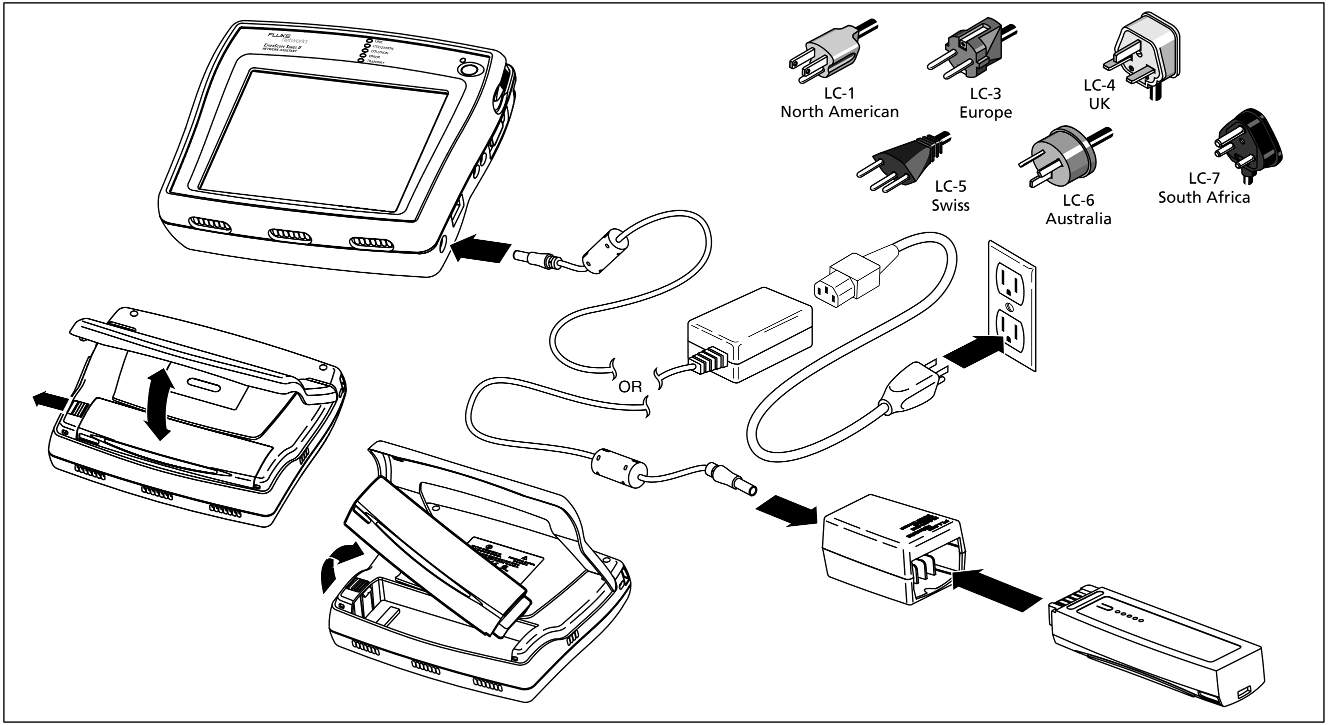
To install the battery, insert it into the battery compartment. Then, press on the battery near the release tab until it locks into place. Finally, push the release tab toward the battery to secure its position.

Operating the Instrument on AC Power

When the instrument is connected to AC power, you can use the power supply as a continuous power source. In this way, you can test for long periods of time without depleting the battery.

To operate the instrument using AC power, refer to Figure 2 and do the following:

1. Connect the power cord to the external AC adapter charger.
2. Connect the AC adapter charger to the power jack on the instrument’s side panel.
3. Turn on the instrument.



eih30f.eps

Figure 2. Charging and Removing the Battery

EtherScope Network Assistant's Physical Features

The EtherScope Network Assistant is designed to be used as a dispatched or desktop network test device. The instrument is shipped with a removable yellow holster that provides more protection for dispatched tasks.

The instrument is also packaged with a stand for use on a desktop. To access the stand, remove the yellow holster. Then, pull the stand out from the bottom of the instrument (see Figure 3).

A stylus for navigating the user interface is stored in the right side panel near the green **On/Off** button.

Figure 3 illustrates the EtherScope Network Assistant's physical features.

Locating the Network Connections

The instrument's network connections are located on the top side panel:

- **LAN copper**: an RJ-45 port that provides direct connection to IEEE 802.3 10/100/1000 BASE-TX networks.
- **LAN fiber**: an SFP port that provides direct connection to networks through the optional 1000BaseSX, 1000BaseLX, or 1000BaseZX fiber connection.
- **SLOT 1**: a PCMCIA/CardBus® interface that supports an 802.11 wireless network. Accepts Fluke Networks EtherScope Wireless LAN Adapter IEEE 802.11 a/b/g.

Locating the External Interfaces

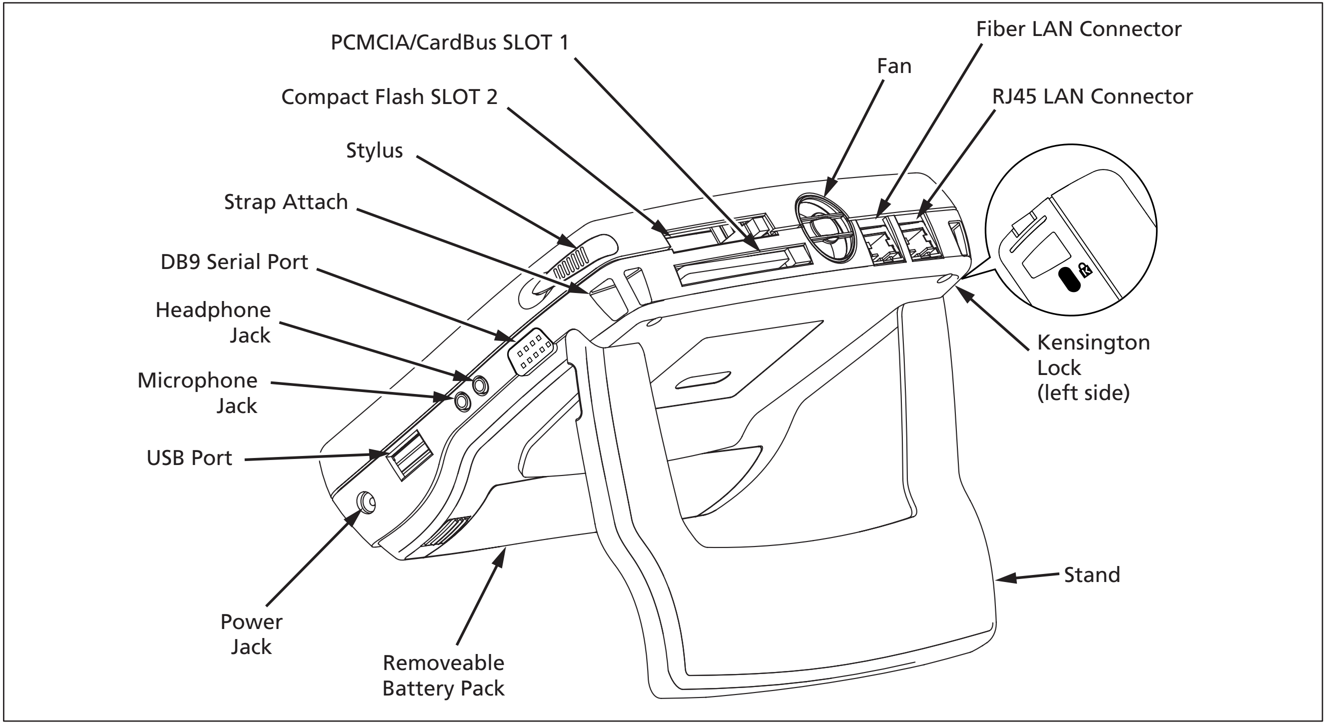
The following external interfaces are located on the instrument's right side panel:

- Serial DB-9: provides a network device connection via a serial cable
- Headphone: enables quiet operation of the instrument (for future applications)
- Microphone: (for future applications)
- USB port: connection for an accessory, such as a keyboard or mouse

SLOT 2 is located on the top side panel. This interface accepts a CompactFlash® (type 1 and 2) memory card.This memory card enables you to store test data and temporarily hold files that are transferred from a PC during a software update.

Locating the External Power Connection

The DC power jack is located on the instrument's right side panel. Plug the supplied AC adapter into this jack to provide external power to the EtherScope Network Assistant and to charge the battery.

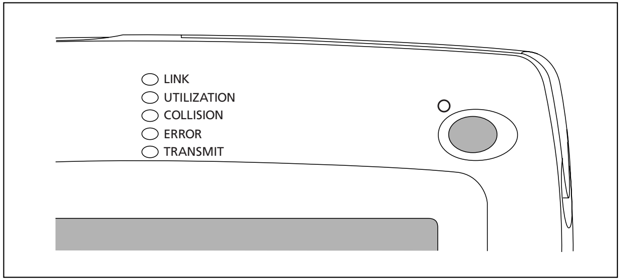


eih31f.eps

Figure 3. EtherScope Network Assistant's Physical Features

Status LEDs

Five status LEDs are located at the top of the front panel, as shown in Figure 4:



avs01f.eps

Figure 4. Status LEDs

These LEDs provide instant, visible feedback on the state of your network and indicate conditions relative to the type of of interface (LAN RJ-45 or wireless) you are testing.

This section describes the LEDs for wired LAN and wireless LAN interfaces.

LAN (RJ-45 or Fiber) Interface LEDs

LINK LED

- Green (solid): indicates that a link is present for all speeds.
- Off: indicates that no cable or no link is present.

UTILIZATION LED

Represents the percent bandwidth consumed on the local network:

- Green (blinking): 0% to 50%.
- Amber (blinking): 51% to 89%.
- Red (blinking): 90% to 100%.

COLLISION LED

Amber (blinking): indicates that collisions have been detected by the instrument on the local network. The more collisions detected, the faster the LED blinks.

ERROR LED

Red (blinking): indicates that errors have been detected on the local network segment. Possible errors include the following:

- Bad FCS: a packet that has an invalid checksum.
- Undersized packet: a packet that has fewer than 64 bytes.
- Oversized packet: a packet that has more than 1518 bytes.
- Jabber: a packet that has more than 1518 bytes and also has an invalid checksum.
- Ghost: energy on a cable that appears to be a real frame but the frame does not have a valid start-frame delimiter.

TRANSMIT LED

Green (blinking): indicates the instrument is transmitting packets. Note that the more transmit activity, the faster the LED blinks.

Wireless LAN Interface LEDs

LINK LED

- Green: 802.11b link established.
- Amber: 802.11a or 802.11g link established.
- Off: no link is present.

UTILIZATION LED

Represents the percent bandwidth consumed on the current channel:

- Green: 1.0 % - 30.0 %.
- Amber: 31.0 % - 60.0 %.
- Red: 61 % - 100 %.

COLLISION LED

Amber: indicates that a retry packet was received.

ERROR LED

Red: indicates an FCS error was detected in a received packet.

TRANSMIT LED

Green: indicates that packets are being transmitted.

Power LED

- Green: instrument turned on (same for both operating on battery and operating with AC power adapter connected)
- Flashing Green: instrument turned off with AC power adapter connected and charging
- Off: instrument turned off; no AC power adapter connected.

The User Interface

The user interface is presented on a touch-sensitive, color screen. You navigate the interface by tapping the touch-sensitive targets with the supplied stylus.

This section describes the layout of the user interface and describes the elements that appear on some or all of the screens. Suggestions are also provided to help you locate screens and navigate your way around.

Screen Layout

The display screen is divided into two main areas:

- A preview pane (on the left), which provides an overview or summary of information for the item that is selected in the right (main) pane. The preview pane may also have hyperlinks (displayed in blue text) that link to other screens in the user interface.
- A main pane (on the right), which provides detailed information, such as test results, graphs, and status information.

Title Bar

The title bar is the horizontal area at the top of every screen that shows the name of the screen that is currently displayed.

In the upper-left corner, the title bar contains the ▣ EtherScope Master Menu icon. This icon displays a menu that lists all of the “details” screens.

Selection Indicator

When you select an item, it is highlighted in a contrasting color to let you know that it is selected. When you first display a screen, the default selection is always highlighted.

Toolbar

The toolbar is the first row of buttons located at the bottom of every screen. The toolbar contains buttons and icons that are used to perform basic tasks.

Note

The toolbar buttons that are available depend on the test that is selected.

- ⇄ 100Mb: (RJ-45 LAN only) reports the actual link speed and duplex mode of the connection. Two solid arrows (shown) indicate a full-duplex connection; one solid and one outlined arrow represent a half-duplex connection.
- ⇄1000Mb SX: (Fiber only) reports the link speed, full duplex (always), and the SFP hardware module installed (FX, LX, or ZX).
- Scan 13b/g: (WLAN only) indicates the current channel being scanned and shows linked status when the instrument is in a WLAN linked state.
- Details: displays detailed information or results for the selected test or device.
- WLAN Tests: changes the interface type to WLAN.
- LAN Tests: changes the interface type to RJ-45 copper and fiber.
- Restart all: restarts all tests.

- (Back): displays the previously displayed screen.
- ⌂ (Home): displays **Test Results**, the top-level user interface screen.
- ?: displays screen-specific help. See “**Error! Reference source not found.**” on page **Error! Bookmark not defined.** for details.
- : displays a menu of troubleshooting tests and productivity tools.

Status Bar

The status bar is located at the bottom of every screen. The following icons appear on the far left:

- Desktop icon. Tap to display a menu containing the following selections:

  Applications: displays a submenu containing the instrument’s desktop tools (see “Using the Desktop Tools” on page 117).

  Reports: displays a directory that lists all saved reports.

  Settings: displays the **Settings** menu (see “Personalizing Your EtherScope Network Assistant” on page 34).

  Suspend: puts the instrument in **Suspend** mode (see “Conserving Battery Power” on page 21).

- Keyboard icon. Tap it to display a virtual keyboard that you can use to enter numbers and text. Tap again to put the keyboard away.
- EtherScope Network Assistant icon. Tap this icon from any screen to return to the **Test Results** screen.

To the far right, the instrument displays the currently set time. To change the date and time, see “Setting the Time and Date” on page 16.

Additional icons give you status on the following;

- 🔊 **Sound:** Tap it to view and adjust the volume of the touch screen’s audible taps.
- 💡 **Light & Power**: Tap it to view and adjust the brightness of the screen (see “Adjusting the Brightness of the Screen” on page 16).
- 🔋 Battery level: Tap it to find out how much battery power remains. If the battery is low on power, see “Charging the Battery” on page 20 for instructions.

The Clipboard icon 📋 is also located on the bottom right. Tap it to display a menu with cut, copy, and paste options. These options come in handy when you are working on screens requiring you to enter a lot of text.

Navigating the User Interface

Following are some general guidelines for navigating the user interface:

- All **blue text** represents a hyperlink. Tap the hyperlink to go to the desired screen.
- To display the detailed results screen for a specific test:
  - Tap ▣ (EtherScope Master Menu icon located in the upper-left corner of each screen). From the drop-down list, select the “details” screen for the selected item.
  - Tap Details to go to the detailed results screen.
- To expand a group so that you can see individual items within it, tap ⊞. To collapse a group, tap ⊟.

- To sort data in a table, tap the desired column heading. A directional arrow indicates the column you are sorting on and the direction (ascending △ or descending ▽) of the sort.
- Tap (Back) to return to the previously displayed screen.
- Tap (Home) to return to the **Test Results** screen.
- Tap ✕ to close a screen.

Personalizing Your EtherScope Network Assistant

You can customize your instrument so that it suits your particular operating style and work preferences.

Tap and then tap **Settings** to display the **Settings** screen. On this screen, you can make the following changes to your instrument:

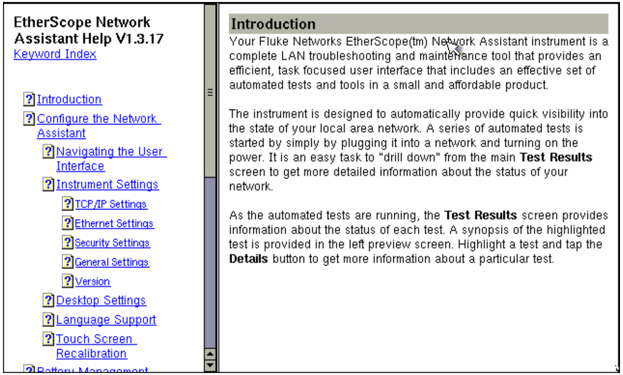
- **Appearance**
  Changes the style and background color of the screen and the visual appearance of the buttons.
- **Date/Time**
  Sets the date and time and changes the date/time formats.
- **Language**
  Changes the default Help language from English to one of the following: French, German, Japanese, Portuguese, Simplified Chinese, or Spanish.
- **Light & Power**
  Adjusts the brightness of the screen (see "Adjusting the Brightness of the Screen" on page 16) and identifies the power source.
- **Sound**
  Adjusts the volume of system sounds (taps on the touch screen and clock alarm).

Getting Help

Screen-level Help is context-sensitive. It provides detailed “how to” and explanatory information that is related to the currently displayed screen.

To obtain this type of help, tap ? (located in the bottom right corner of the tool bar).

EtherScope Network Assistant Help is displayed, as shown in Figure 5:



EtherScope Network Assistant Help V1.3.17
Keyword Index

- Introduction
- Configure the Network Assistant
  - Navigating the User Interface
  - Instrument Settings
    - TCP/IP Settings
    - Ethernet Settings
    - Security Settings
    - General Settings
    - Version
  - Desktop Settings
  - Language Support
  - Touch Screen Recalibration
- Battery Management

Introduction

Your Fluke Networks EtherScope(tm) Network Assistant instrument is a complete LAN 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 local area network. A series of automated tests is started by simply by plugging it into a network 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.

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

avs55s.bmp

Figure 5. Screen-Level Help

Note that Help for the current screen is displayed in the main pane. To move through the information, drag the scroll box. The browser window is resizable so that you can view test information alongside the context-sensitive Help text.

The main pane displays a table of contents. When you tap a topic in this list, you are directed to its Help. To see a list of entries, tap the **Keyword Index** link.

Note

The Help file is also available on the EtherScope Resource CD.

Accessing the Documentation Online

This *Getting Started Guide* is provided in PDF format on the EtherScope Resource CD. The guide is available in the following languages: English, German, French, Spanish, Portuguese, Japanese, and Chinese.

Monitoring and Troubleshooting a Wired LAN

After you connect the instrument to your network and power it on, the instrument attempts to become an active device on the network by obtaining an IP address. By default, it tries to acquire an address by using DHCP.

Note

> *If your network policy requires the use of fixed IP addresses or if you need to change other network configuration data (such as the default router), see "Configuring the Instrument for a Wired LAN" on page 74.*

If the instrument acquires a valid IP address, it automatically runs a series of tests that include verifying the cable and signal, gathering network utilization and bandwidth statistics, and actively discovering networks, services, and devices using the network. It reports its findings on the **Test Results** screen.

If the instrument cannot acquire a valid IP address, it can still analyze traffic for statistics and passively discover devices. However, without a valid IP address, the instrument cannot run its active discovery tests. The basic steps for monitoring and troubleshooting a wired LAN are given below. Detailed information for a step can be obtained by going to the referenced section provided at each step:

1. Power on the instrument (see "Turning the Instrument On and Off" on page 14) and, if necessary, configure the interface type (see "Selecting the LAN or WLAN Interface" on page 15).

2. Connect to the network (see “Connecting to a Wired Network “on page 37).

   After you turn on and connect the instrument, it goes through a complete power-up sequence, which entails initializing the processor and memory, performing a self-test, and loading the operating system and application software. When this process is completed, the autotest results screen (Figure 6) is displayed.

3. View autotest results for each test. See “Viewing AutoTest Results” on page 38.

4. Make any needed configuration changes to match your testing environment. See “Configuring the Instrument for a Wired LAN” on page 74”.

Connecting to a Wired Network

To connect to the network, plug one end of an Ethernet cable into the instrument’s RJ-45 LAN connector and the other end of the cable into the network segment you are testing.

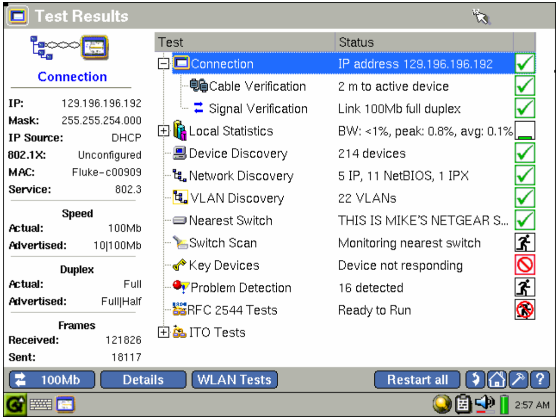
If you have purchased the optional Fiber SFP adapter for 1000BaseSX, 1000BaseLX, or 1000BaseZX, connect the fiber cable from the adapter to the network segment you are testing.

Note

Make sure you are using the correct fiber cable type for the installed optional fiber adapter type, or you may experience no link or bad test results.

Viewing AutoTest Results

After you power on the EtherScope Network Assistant and connect to the network, the instrument runs a series of automated tests and displays its findings on the **Test Results** screen, as shown in Figure 6.



Test Results

Connection

IP: 129.196.196.192
Mask: 255.255.254.000
IP Source: DHCP
802.1X: Unconfigured
MAC: Fluke-c00909
Service: 802.3

Speed
Actual: 100Mb
Advertised: 10|100Mb

Duplex
Actual: Full
Advertised: Full|Half

Frames
Received: 121826
Sent: 18117

Test	Status	
Connection	IP address 129.196.196.192	✓
Cable Verification	2 m to active device	✓
Signal Verification	Link 100Mb full duplex	✓
Local Statistics	BW: <1%, peak: 0.8%, avg: 0.1%	
Device Discovery	214 devices	✓
Network Discovery	5 IP, 11 NetBIOS, 1 IPX	✓
VLAN Discovery	22 VLANs	✓
Nearest Switch	THIS IS MIKE'S NETGEAR S...	✓
Switch Scan	Monitoring nearest switch	🏃
Key Devices	Device not responding	🚫
Problem Detection	16 detected	🏃
RFC 2544 Tests	Ready to Run	
ITO Tests		

epi40s.bmp

Figure 6. LAN Test Results Screen

The **Test Results** screen gives you at-a-glance visibility into the state of your network. The main pane on the right displays the name of each test and reports its status. Note the status icons that appear along the right. They give you a visual indication of the progress and status of each test:

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

The preview pane on the left provides a summary of the results of the selected test.

Note

*When autotest finishes, the **Connection** test (the default selection) is highlighted.*

You can get quick idea of the overall health of your network and see what devices and services are running by tapping each test in the main pane and then viewing a summary of its findings in the preview pane. To view in-depth results for any test, select the test from the list in the main pane. Then, tap Details.

The individual tests that comprise the autotest are described in this section.

Connection Test

The **Connection** test checks your network's performance at the physical layer. Results from higher layer tests are misleading if the equipment or cabling is faulty or installed incorrectly. Therefore, before you investigate higher layers of the network as the source of any problems, you should first identify and eliminate any problems occurring at the physical or link layer of your network.

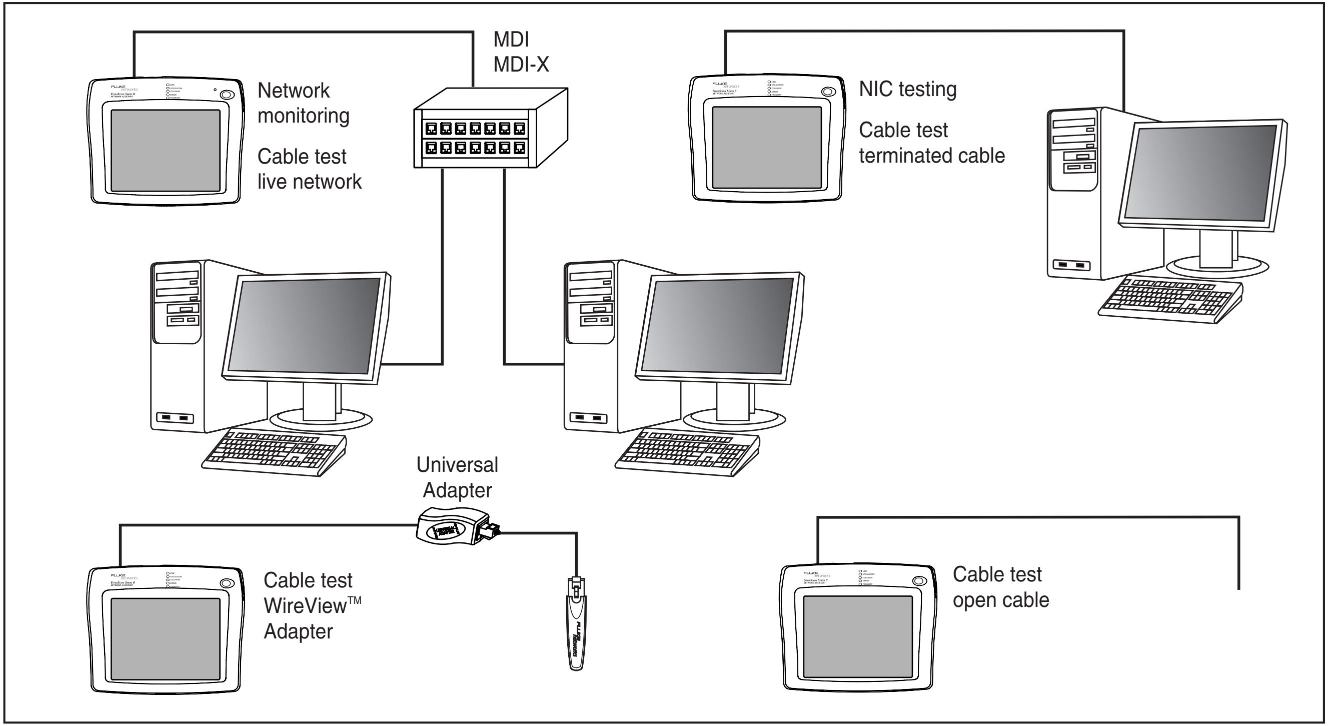
Results from the **Connection** test can help you isolate the source of network problems due to malfunctioning cabling or equipment.

Figure 7 illustrates various cabling test configurations. After you connect and power on the instrument, it automatically detects the type of connection (for example, to a patch cable, an Ethernet network, NIC, or a wiremap adapter) and then determines the appropriate cable tests to run.

Note

You do not have to disconnect the far end of a cable for length to be measured. Length can be measured while a cable is connected to a wiremap adapter, active hub, switch or NIC, or a cable that is not terminated.

If no problems are found, a green checkmark ✓ indicates that the **Connection** test passed. If problems are detected, a test failed symbol ⊘ is displayed.



eih32f.eps

Figure 7. Testing Cables

The **Connection** test consists of two subtests:

Cable Verification: provides cable length and impedance information and identifies any problems with the cable.

Signal Verification: verifies that the instrument is detecting a proper signal at the input.

Note

Cable Verification and Signal Verification do not apply when testing a fiber connection. For a fiber connection, the Connection Test displays the Fiber Loss Test which requires that the optional Fluke Networks' Fiber Optic Meter be attached to the RJ45 port.

In the main pane, tap the ⊞ next to **Connection** to expand the list so that you can see these two tests.

Cable Verification

Cable Verification includes tests that check the physical layer cable and equipment to verify that they are working properly.

Note

To run these tests, the instrument must disconnect from the network, which causes other tests that are running to stop. If you are operating the EtherScope Network Assistant remotely, the connection is lost, preventing the instrument from being able to verify the duplex of the connection.

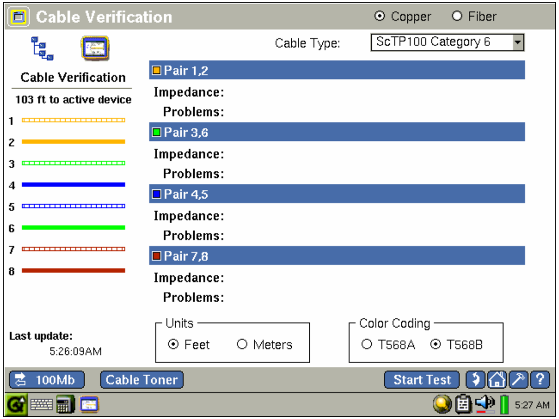
After you run the autotest, tap **Cable Verification** to view initial autotest results for the cable:

- The preview pane displays the length of the cable to the active device or termination. Individual wires are numbered and color-coded to identify pairs.

- The main pane displays results of the **Cable Verification** test. A ✓ indicates that the instrument detects a valid cable. A 🚫 indicates that there is a problem with the cable.

To view detailed results, tap **Details**.

The **Cable Verification** details screen (Figure 8) displays results for each wired pair. The main pane displays breakout of the cable by wired pairs so you can obtain specific termination and impedance information and identify problems.



Cable Verification

● Copper ○ Fiber

Cable Type: ScTP100 Category 6

Cable Verification

103 ft to active device

1
2
3
4
5
6
7
8

Pair 1,2
Impedance:
Problems:

Pair 3,6
Impedance:
Problems:

Pair 4,5
Impedance:
Problems:

Pair 7,8
Impedance:
Problems:

Last update:
5:26:09AM

Units
● Feet ○ Meters

Color Coding
○ T568A ● T568B

epi60s.bmp

Figure 8. Cable Verification Screen

To run the detailed test, tap Start Test.

Note

> *To run this test, the instrument must unlink from the network. Current test results are discarded.*

If you want to trace the cable to a switch, hub, or patch panel, tap Cable Toner to set up and run a **Cable Toner** test.

Note

> *This test requires a companion probe device for locating and tracing cable.*

To test signal power and loss on a fiber optic cable, select the **Fiber** option. Then, set up and run a **Fiber Optic Meter** (FOM) test.

Note

> *This test requires a (separately purchased) Fiber Optic Test Kit Accessory.*
>
> *You will need to use the supplied universal adapter to perform a wiremap (test a patch cable).*

Signal Verification

The **Signal Verification** test is comprised of a suite of tests that analyze the quality of the signal and establish connectivity at the physical layer.

To provide comprehensive link signal information, the **Signal Verification** test does a complete auto-negotiation regardless of the current link configuration. For example, if the instrument is configured to link at 100 Mbit half-duplex, the **Signal Verification** test temporarily overrides that configuration to measure the complete auto-negotiation process. When you exit the test, the previous link configuration settings are restored.

To view initial autotest results, select **Signal Verification**.

The preview pane shows the type of service on the connection. In addition, the actual and advertised speed and duplex of the connection is provided, enabling you to compare determined values with negotiated values. By default, the instrument auto-negotiates to the highest speed and duplex allowed by the link partner.

Note

You can configure the instrument to link at a specific speed and duplex. See "Configuring the Instrument for a Wired LAN" on page 74".

To run the full suite of signal verification tests, do the following;

1. Tap Details. Then tap Start Test.
2. Tap OK to disconnect the instrument from the network.

Notes

To run these tests, the EtherScope Network Assistant must disconnect from the network, which causes other tests that are running to stop. If you are operating the instrument remotely, the connection is lost, preventing you from viewing the test results or regaining remote control of the instrument until it is manually reset.

*The **Solicit for 802.3af Power over Ethernet** check box enables soliciting for PoE voltage information through a PoE (802.3af standard only, non-standard is not supported) connection. Press the Start Test button after checking this box to initiate this test.*

The main pane (see Figure 9) displays results from the four Signal Verification tests. The tests are designed to provide visibility into possible link quality and configuration issues that could be contributing to connectivity or performance problems.

- **DC Voltage Scan**: cable line voltages are scanned for DC-level content and over-voltage conditions. In this section, voltage levels are reported.

  Note

  The presence of high voltages may indicate telephone connections, early versions of applied hard-wired power-over-Ethernet (PoE), or 802.3ae or 802.3af probe voltages.

  A green checkmark indicates that either no DC voltage is being detected or no significant DC voltage is being detected. If some other DC voltage is detected (for example, 802.ae), a red check mark is displayed.

- **Signal Levels**: No signal, NLP (Normal Link Pulse), FLP (Fast Link Pulse) and Data signals and their amplitudes are monitored and displayed.

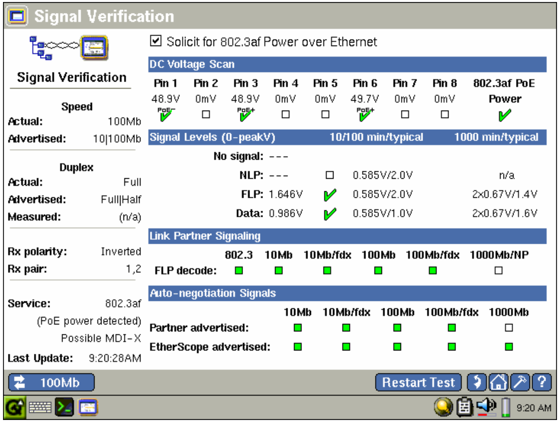
  A green checkmark indicates that signal levels are acceptable. If signal levels are below the minimum specification, a red check mark is displayed.

- **Link Partner Signaling**: these signals indicate the device-supported signaling capabilities of the cable source (link partner) before the auto-negation sequence begins.

  The presence or absence of a signal is indicated by a green box or an empty box, respectively.

- **Auto-negotiation Signals**: FLP signals from the auto-negotiation sequence display what the cable connection source (link partner) advertised and what the EtherScope Network Assistant advertised.

  The presence or absence of a signal is indicated by a green box or an empty box, respectively.



Signal Verification

☑ Solicit for 802.3af Power over Ethernet

Signal Verification

Speed
Actual: 100Mb
Advertised: 10|100Mb

Duplex
Actual: Full
Advertised: Full|Half
Measured: (n/a)

Rx polarity: Inverted
Rx pair: 1,2

Service: 802.3af
(PoE power detected)
Possible MDI-X
Last Update: 9:20:28AM

DC Voltage Scan

Pin 1	Pin 2	Pin 3	Pin 4	Pin 5	Pin 6	Pin 7	Pin 8	802.3af PoE Power
48.9V	0mV	48.9V	0mV	0mV	49.7V	0mV	0mV	
PoE- ✓	□	PoE+ ✓	□	□	PoE+ ✓	□	□	✓

Signal Levels (0-peakV)			10/100 min/typical	1000 min/typical
No signal:	---			
NLP:	---	□	0.585V/2.0V	n/a
FLP:	1.646V	✓	0.585V/2.0V	2x0.67V/1.4V
Data:	0.986V	✓	0.585V/1.0V	2x0.67V/1.6V

Link Partner Signaling

	802.3	10Mb	10Mb/fdx	100Mb	100Mb/fdx	1000Mb/NP
FLP decode:	🟩	🟩	🟩	🟩	🟩	□

Auto-negotiation Signals

	10Mb	10Mb/fdx	100Mb	100Mb/fdx	1000Mb
Partner advertised:	🟩	🟩	🟩	🟩	□
EtherScope advertised:	🟩	🟩	🟩	🟩	🟩

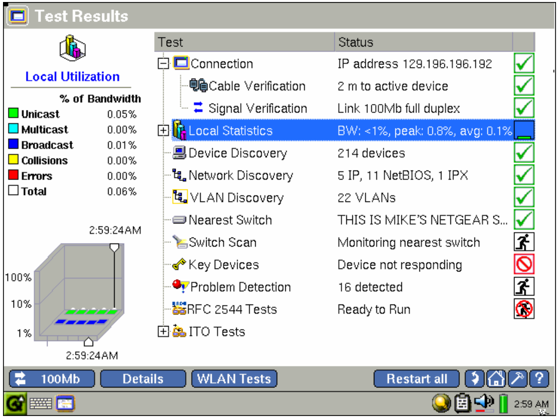
epi84s.bmp

Figure 9. Signal Verification Screen

Local Statistics Test

The **Local Statistics** test reports local and remote bandwidth utilization and errors seen on the network.

1. In the main pane, tap **Local Statistics**.



Test Results

Local Utilization

	% of Bandwidth
🟩 Unicast	0.05%
🟦 Multicast	0.00%
🟦 Broadcast	0.01%
🟨 Collisions	0.00%
🟥 Errors	0.00%
□ Total	0.06%

Test	Status	
⊟ Connection	IP address 129.196.196.192	✓
Cable Verification	2 m to active device	✓
Signal Verification	Link 100Mb full duplex	✓
⊞ Local Statistics	BW: <1%, peak: 0.8%, avg: 0.1%	
Device Discovery	214 devices	✓
Network Discovery	5 IP, 11 NetBIOS, 1 IPX	✓
VLAN Discovery	22 VLANs	✓
Nearest Switch	THIS IS MIKE'S NETGEAR S...	✓
Switch Scan	Monitoring nearest switch	🏃
Key Devices	Device not responding	🚫
Problem Detection	16 detected	🏃
RFC 2544 Tests	Ready to Run	🚫
⊞ ITO Tests		

epi64s.bmp

Figure 10. Local Statistics Summary

The preview pane (Figure 10) presents a profile of the types of traffic seen on the network. In the top half of the pane, the types of traffic are classified (for example, unicast frames and collisions) and the percentage of bandwidth consumption for each group is reported. Traffic types are color-coded for easier viewing.

The graph at the bottom of the pane plots the types of local traffic seen according to the percentage of bandwidth utilization (y-axis) over time (x-axis). Tap the graph to view statistics for a particular time period.

2. Tap the ⊞ next to **Local Statistics** to expand the list and show its subtests:

   - **Protocol Statistics**
   - **Top Talkers**
   - **VLAN Statistics**

3. To view summary results for a particular subtest, select it from the list:

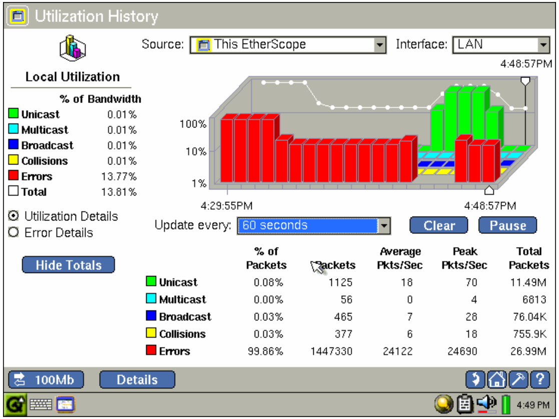
   - **Protocol Statistics**: identifies the top 12 network services, applications, and devices discovered on the local network segment and provides a breakout by percent of bandwidth utilization of all packets.
   - **Top Talkers**: identifies the top 10 devices that are the highest consumers of bandwidth on the local network segment and provides a breakout by percent of all packets sent.
   - **VLAN Statistics:** identifies VLANs (up to 12) that are most active on the local network segment and provides a breakout by percent of all packets detected. The status line shows the total number of VLANs discovered and the top VLAN ID with its percentage of total packets.

Viewing the Local Statistics Details

If the summary reports indicate problems, check the detailed results to see if you can determine the source of a problem.

1. On the **Test Results** screen, select **Local Statistics** and then tap Details.

   The **Utilization History** screen (Figure 11) is displayed:



Utilization History

Source: This EtherScope

Interface: LAN

Local Utilization

	% of Bandwidth
🟩 Unicast	0.01%
🟦 Multicast	0.01%
🟦 Broadcast	0.01%
🟨 Collisions	0.01%
🟥 Errors	13.77%
□ Total	13.81%

● Utilization Details
○ Error Details

Update every: 60 seconds

	% of Packets	Packets	Average Pkts/Sec	Peak Pkts/Sec	Total Packets
🟩 Unicast	0.08%	1125	18	70	11.49M
🟦 Multicast	0.00%	56	0	4	6813
🟦 Broadcast	0.03%	465	7	28	76.04K
🟨 Collisions	0.03%	377	6	18	755.9K
🟥 Errors	99.86%	1447330	24122	24690	26.99M

epi50s.bmp

Figure 11. Utilization History Screen

On this screen, you can:

- Look at the different types of traffic present on the network segment. This information can help you determine if the network is experiencing or has experienced high utilization, excessive collisions, or unusual error conditions.
- Monitor local utilization (select **Utilization Details** in the preview pane) or errors (select **Error Details**) on the port that the instrument is connected to.

- Get visibility into remote devices and segments without directly connecting to them. To do this, choose a discovered switch and interface source from the **Source** selection box. Then monitor the source’s utilization and errors.

  Note

  The EtherScope Network Assistant monitors and trends the source throughout the session or until you change the source. It also continues to monitor local utilization and errors in the background.

- View utilization statistics during a particular period of time. To do this, tap the graph directly.

  A white vertical bar marks the sampling period.

  Note

  *The graph is updated according to the frequency set in the **Update every** selection box. To change the frequency, select a value from the drop-down list.*

Viewing Details for Protocol Statistics, Top Talkers, and VLAN Statistics

To view details:

1. On the **Test Results** screen, tap the ⊞ next to **Local Statistics** to expand the list and show its subtests:
   - **Protocol Statistics**
   - **Top Talkers**
   - **VLAN Statistics**
2. Select the desired subtest.
3. Tap Details to display detailed results for the selected subtest:
   - **Protocol Statistics**: the main pane lists all of the network protocols that have been discovered on the local network segment.

- **Top Talkers**: the main pane lists all the discovered devices that are generating traffic on the local network segment.
- **VLAN Statistics**: the main pane lists all VLANs discovered on the local network segment.

Notes

The number of VLANs discovered by VLAN Statistics and VLAN Discovery (described later) frequently differs. VLAN Statistics monitors the local segment only and generates a list of VLANs discovered. The VLAN Discovery test, on the other hand, uses active SNMP discovery to determine the number of VLANs on your entire network.

If the instrument is connected to a port that is configured with 802.1Q VLAN tagging and the instrument is not so configured, or if 802.1Q is enabled on the instrument but not on the port, DHCP will fail and device discovery will probably show one device (This EtherScope). VLAN Statistics, on the other hand, will show whether any VLAN tagged packets are on the network segment. To fix this problem, you should either disable 802.1Q on the instrument, or to configure the instrument for the correct VLAN (try configuring the instrument for the VLAN with the highest packet count). See "802.1Q/IP TOS Settings" on page 76 for details.

Device Discovery Test

As soon as the EtherScope Network Assistant is connected, it performs active SNMP discovery for all network devices. The instrument examines each device it discovers to learn more about the device's capabilities and to detect possible problems. The **Device Discovery** test lets you know what devices the instrument sees on your network. As devices are discovered, they are added to the instrument's discovery database.

Notes

- *For best results, the instrument needs to be configured with the SNMP community strings being used on your network. See "Instrument Security Settings" on page 79 to find out how to enter additional community strings.*
- *If the instrument does not automatically discover a device, the device can be manually added to the discovery database. See "Adding a Device to the Discovery Database "on page 55.*

To view results:

1. In the main pane, tap **Device Discovery**.

   The preview pane displays an inventory of the devices the instrument discovered. You can find out the total number of devices found. In addition, the devices are categorized into the following groups and the number of devices within each group is provided:

   Total Devices

   Routers

   Switches

   Servers

   Printers

Key Devices

SNMP Agents

Hosts

A device that is an SNMP agent may be counted twice; that is, in the SNMP Agents group and in the device group to which it belongs. Therefore, the sum of devices in all categories can be greater than that reported for **Total Devices**.

2. To view detailed results, tap Details to display the detailed **Device Discovery** screen.

   On this screen, you can find out information about each discovered device, such as its DNS name, IP address, and key device status.

   You can also see whether the device is experiencing any problems.

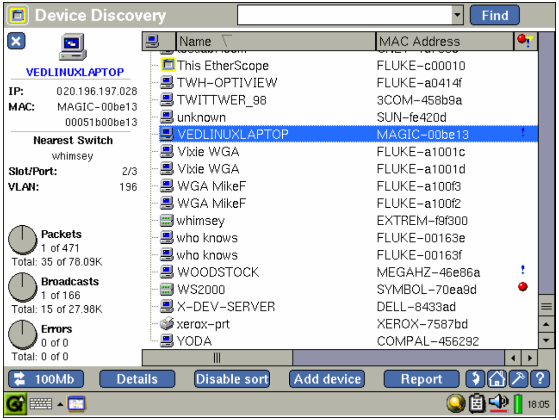
   a. Drag the scroll bar or tap the directional arrows at the bottom of the main pane to bring all of the information about a device into view.

      Alternatively, check one of the **Show** buttons at the bottom of the preview pane to move selected information about the device (for example, switch information) into view.

   b. Rearrange the information on this screen by choosing a particular column heading as the basis for the sort. To do this, tap the heading you want to sort on. A directional arrow indicates the column you selected and the direction (ascending △ or descending▽) of the sort.

3. To obtain device-specific information, select the desired device.

   The upper portion of the preview pane (Figure 12) shows the IP and MAC address information for the device you selected while the lower portion graphically shows utilization details (relative percents of packets, broadcasts, and errors).



VEDLINUXLAPTOP

IP: 020.196.197.028
MAC: MAGIC-00be13
00051b00be13

Nearest Switch
whimsey
Slot/Port: 2/3
VLAN: 196

Packets
1 of 471
Total: 35 of 78.09K

Broadcasts
1 of 166
Total: 15 of 27.98K

Errors
0 of 0
Total: 0 of 0

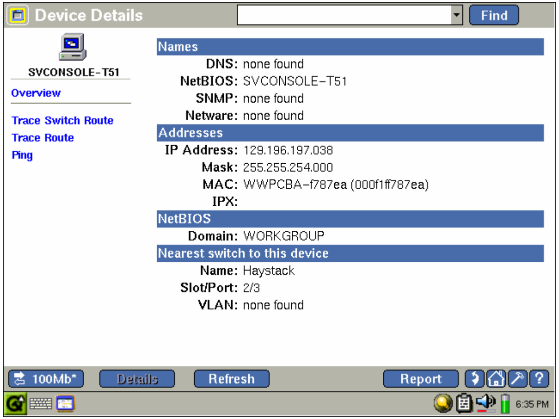
Name	MAC Address
This EtherScope	FLUKE-c00010
TWH-OPTIVIEW	FLUKE-a0414f
TWITTWER_98	3COM-458b9a
unknown	SUN-fe420d
VEDLINUXLAPTOP	MAGIC-00be13
Vixie WGA	FLUKE-a1001c
Vixie WGA	FLUKE-a1001d
WGA MikeF	FLUKE-a100f3
WGA MikeF	FLUKE-a100f2
whimsey	EXTREM-f9f300
who knows	FLUKE-00163e
who knows	FLUKE-00163f
WOODSTOCK	MEGAHZ-46e86a
WS2000	SYMBOL-70ea9d
X-DEV-SERVER	DELL-8433ad
xerox-prt	XEROX-7587bd
YODA	COMPAL-456292

epi43s.bmp

Figure 12. Device Discovery Screen

4. Tap **Details** to view obtain detailed information about the device.

   The **Device Details** screen provides name, address, domain, and nearest switch information about the device, as shown in Figure 13:



SVCONSOLE-T51

Names
DNS: none found
NetBIOS: SVCONSOLE-T51
SNMP: none found
Netware: none found

Addresses
IP Address: 129.196.197.038
Mask: 255.255.254.000
MAC: WWPCBA-f787ea (000f1ff787ea)
IPX:

NetBIOS
Domain: WORKGROUP

Nearest switch to this device
Name: Haystack
Slot/Port: 2/3
VLAN: none found

epi68s.bmp

Figure 13. Device Details Screen

From this screen, you can also run specialized tests (such as Trace Switch Route, Trace Route, or Ping) to troubleshoot connectivity or performance problems associated with the device. These tests are started by tapping the desired hyperlink in the preview pane. See "Running the Diagnostic Tests" on page 108 for descriptions of these tests.

Adding a Device to the Discovery Database

If the instrument does not automatically discover a device, you can manually add the device to its discovery database. After a device is added to the database, the instrument keeps track of it and reports its statistics on the **Device Discovery** test screens.

To add a device to the discovery database:

1. Tap ▣ (located in the top left corner of the screen) and then select **Instrument Settings**.
2. Tap the **General** hyperlink to display the **Instrument Settings—General** screen.
3. Tap Edit user-defined devices.
4. On the **User-defined Devices** screen, tap Add device. Then use a keyboard to supply the required information.

   If you want to identify the device as a key device, check the **Add to key device list** button.
5. Tap OK.

   The device you added is now in the discovery database.

Network Discovery Test

The **Network Discovery** test scans the local segment, looking for what networks are present and how they are configured. This test enables you to see discovered networks by IP subnets, NetBIOS domains, and IPX networks.

1. Select **Network Discovery**.

   The preview pane identifies the types of networks found and reports the number of networks per type. EtherScope Network Assistant organizes discovered networks into the following groups.

   - **IP Subnets**
   - **NetBIOS Domains**
   - **IPX Networks**

   Within each group, you can also find out the number of devices discovered.

2. To view detailed results for **Network Discovery**:

   - In the preview pane, tap the desired network group.

     OR

   - Tap **Details**.

     Subnet details include IP address ranges and subnet masks, while domain details identify master browsers and domain controllers.

3. If you need to quickly locate a device within your network environment, use the **Find** facility. Do the following:

   a. Tap inside the text entry box. Use a remote keyboard or tap ⌨ to display the virtual keyboard and enter a full or partial name, IP address or MAC address.

   b. Tap **Find** to begin the search.

VLAN Discovery Test

The **VLAN Discovery** test identifies all of the VLANS discovered on the network segment that the instrument is connected to. The test informs you of VLAN membership configurations and interface status. You can also get details on connected hosts and view trending data.

Note

The VLAN Discovery test differs from the VLAN Statistics test discussed earlier. VLAN Discovery queries all switches that the instrument communicates with and generates a list of VLANs discovered. The VLAN Statistics test monitors the frames only on the switch port/interface that the instrument is connected to and generates a list of VLANs discovered.

1. Tap **VLAN Discovery**.

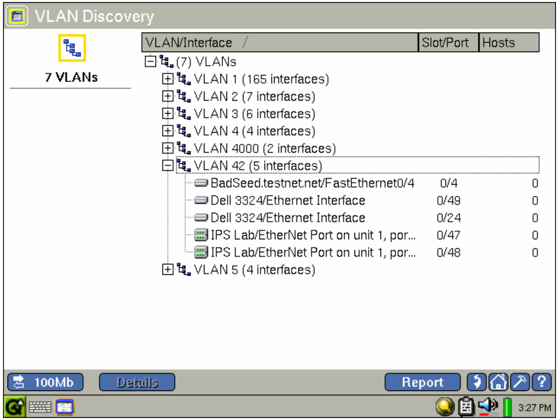
   The preview pane (see Figure 14) displays the total number of discovered VLANs.

   The main pane shows inventory of the discovered VLAN trunks and lists associated switch interfaces. For each VLAN interface, you can obtain the VLAN and slot/port numbers and find out how many hosts belong to the VLAN.

   Note

   You can sort the information on any of the VLAN discovery screens. To do this, tap the heading you want to sort on. A directional arrow ▽△ indicates the column you selected and the direction (ascending or descending) of the sort.

2. Tap **Details** to display the **VLAN Discovery** screen.



VLAN Discovery

7 VLANs

VLAN/Interface	Slot/Port	Hosts
⊟ (7) VLANs		
⊞ VLAN 1 (165 interfaces)		
⊞ VLAN 2 (7 interfaces)		
⊞ VLAN 3 (6 interfaces)		
⊞ VLAN 4 (4 interfaces)		
⊞ VLAN 4000 (2 interfaces)		
⊟ VLAN 42 (5 interfaces)		
BadSeed.testnet.net/FastEthernet0/4	0/4	0
Dell 3324/Ethernet Interface	0/49	0
Dell 3324/Ethernet Interface	0/24	0
IPS Lab/EtherNet Port on unit 1, por...	0/47	0
IPS Lab/EtherNet Port on unit 1, por...	0/48	0
⊞ VLAN 5 (4 interfaces)		

epi48s.bmp

Figure 14. VLAN Discovery Screen

3. To see the member switch interfaces within a particular VLAN, select the desired VLAN. Then tap ⊞ to expand the list.

   VLANs that have no associated switch interfaces simply display the switches that reference this VLAN.

4. To get general information for a particular VLAN/Interface, select it.

   The preview pane identifies the IP address of your selection.

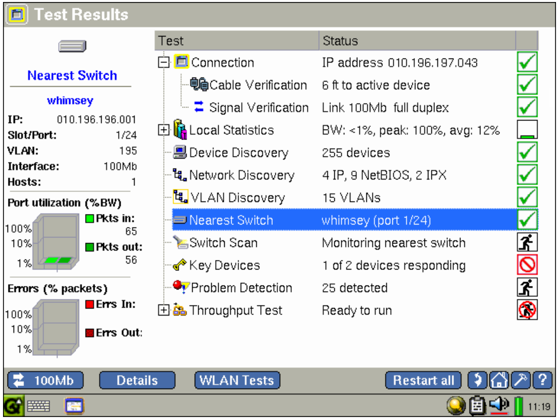
5. To obtain a detailed report on a particular interface, select it from the list, then tap **Details**.

   You can view the port traffic and the devices configured for that interface.

Nearest Switch Test

An integral part of discovery is locating the switches on the network. The **Nearest Switch** test uses SNMP to search for and find the switch that is closest to the port that the instrument is connected to. After the nearest switch is discovered, its active ports are monitored for utilization and errors.

1. To check the status of the nearest switch, tap **Nearest Switch.**



Test Results

Nearest Switch

whimsey

IP:	010.196.196.001
Slot/Port:	1/24
VLAN:	195
Interface:	100Mb
Hosts:	1

Port utilization (%BW)

Pkts in: 65

Pkts out: 56

Errors (% packets)

Errs In:

Errs Out:

Test	Status	
Connection	IP address 010.196.197.043	✓
Cable Verification	6 ft to active device	✓
Signal Verification	Link 100Mb full duplex	✓
Local Statistics	BW: <1%, peak: 100%, avg: 12%	
Device Discovery	255 devices	✓
Network Discovery	4 IP, 9 NetBIOS, 2 IPX	✓
VLAN Discovery	15 VLANs	✓
Nearest Switch	whimsey (port 1/24)	✓
Switch Scan	Monitoring nearest switch	
Key Devices	1 of 2 devices responding	🚫
Problem Detection	25 detected	
Throughput Test	Ready to run	

epi66s.bmp

Figure 15. Nearest Switch Summary

As shown in Figure 15, the preview pane displays the IP address of the switch along with its VLAN identifier and port number. You can also see the speed of the interface and find out how many hosts are connected to the ports on the switch.

The graphs update you on bandwidth utilization and errors found on the busiest port.

2. To see a detailed report on the nearest switch, tap Details.

On the **Switch Details** screen, you can run also one of the diagnostic tests (for example, Trace Switch Route or Ping) to troubleshoot connectivity or performance problems associated with the switch.

3. To set up and run a test, tap the associated hyperlink in the preview pane. (See “Running the Diagnostic Tests” on page 108 for descriptions of these tests).

Switch Scan Test

The **Switch Scan** test continuously monitors the nearest switch plus a second (user-selected) switch so that you can determine their health and status.

1. Tap **Switch Scan**.

   The preview pane shows you the name of the switch that is being monitored and the number of active ports on the switch. In addition, you can find out whether bandwidth utilization is excessive and whether the switch is experiencing any errors.

2. Tap Details.

   Note

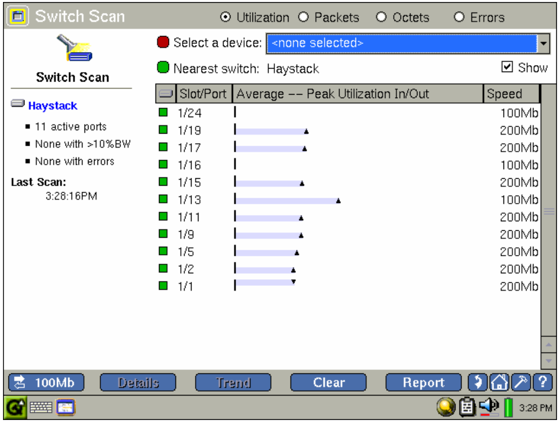
   If no switch is selected, select one from the ***Select a device*** *list box.*

   The **Switch Scan** details screen (Figure 16) identifies the slot/port number of the switch and shows a breakout of utilization statistics by port.

3. Select the type of statistic that you want to view for the switch by tapping one of these options in the title bar:

   - **Utilization**
   - **Packets**
   - **Octets**
   - **Errors**

   The main pane redisplays switch statistics based on your selection.



● Utilization ○ Packets ○ Octets ○ Errors

🟥 Select a device: <none selected>

🟩 Nearest switch: Haystack ☑ Show

Haystack
- 11 active ports
- None with >10%BW
- None with errors

Last Scan: 3:28:16PM

	Slot/Port	Average -- Peak Utilization In/Out	Speed
🟩	1/24		100Mb
🟩	1/19		200Mb
🟩	1/17		200Mb
🟩	1/16		100Mb
🟩	1/15		200Mb
🟩	1/13		100Mb
🟩	1/11		200Mb
🟩	1/9		200Mb
🟩	1/5		200Mb
🟩	1/2		200Mb
🟩	1/1		200Mb

epi49s.bmp

Figure 16. Switch Scan Screen

4. To select an additional switch to scan, select it from the **Select a device** box.

5. By default, the nearest switch is monitored. To prevent this switch from being monitored, tap (to uncheck) the **Show** box.

6. To view details for a particular interface:

   a. Select the desired interface.

      The top portion of the preview pane shows the port number, VLAN identifier, speed of the interface, and number of connected hosts. The lower portion displays a graph that lets you see the relative percentage of packets and bandwidth.

   b. If you want to see interface statistics over a period of time, select the desired interface. Then tap Trend.

      The **Utilization History** is displayed. On this screen, you can specify a time period during which errors and utilization statistics for the interface are gathered and reported.

   c. Tap Details to obtain more detailed information for the selected interface.

Key Devices Test

The **Key Devices** test checks the availability of critical or "key" devices on your network. You can use this test to verify connectivity between certain network devices and critical network services (for example, print or email servers).

For the **Key Devices** test to operate properly, you need to specify which devices you want EtherScope Network Assistant to track. Devices you might include in this category are servers, switches, and routers because these are the devices that you most likely want to monitor on a regular basis.

When you define a network device as "key", the instrument periodically checks its status (up or down) to determine its availability. An occasional intermittent non-response is ignored, but if no response is received from a key device after several consecutive attempts, the instrument reports its status as **Fail** 🚫. In addition, the instrument always generates a message when the status of a key device changes so that you are always made aware of any problems it is experiencing.

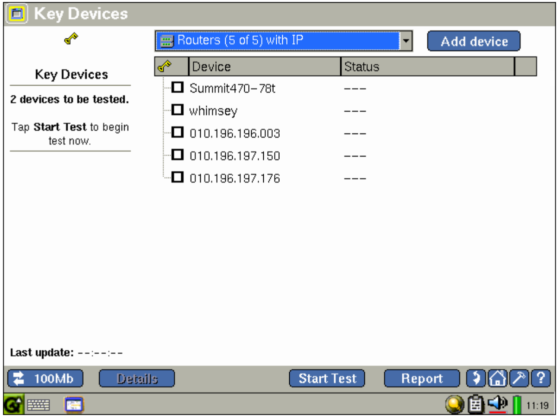
Defining Key Devices

To define a key device, do the following:

1. On the **Test Results** screen, select **Key Devices**.
2. Tap Details to display the **Key Devices** screen:

Note

If EtherScope Network Assistant is operating in WLAN mode, the screen is slightly different from the one shown in Figure 17.



Key Devices

2 devices to be tested.

Tap **Start Test** to begin test now.

Device	Status
□ Summit470-78t	---
□ whimsey	---
□ 010.196.196.003	---
□ 010.196.197.150	---
□ 010.196.197.176	---

Last update: --:--:--

epi41s.bmp

Figure 17. Key Devices Screen

3. Do one of the following:

   - If the instrument discovered the device:

     a) Tap the arrow in the drop-down list box at the top of the screen. Then, select a category (for example, **Hosts** to see all of the devices in that category.

     b) Find the desired device in the list and then tap (to check) the box to mark it as a key device.

   - If the instrument did not discover the device:

     a) Tap Add device.

     b) Tap ⌨. Then in the **Add Key Device** box, supply the IP address of the device.

     c) To ensure that the instrument discovers the device, tap (to check) the **Add to device discovery?** box and supply the MAC address.

     d) Tap OK to close.

   As you add devices to the **Key Devices** group, the preview pane keeps track of the number of devices to be tested.

4. To run the **Key Devices** test, tap Start Test.

   As the test runs, detailed status on each device is reported in the main pane.

Problem Detection

The **Problem Detection** test checks each discovered device to determine if it is experiencing any problems. If a problem is detected, the instrument enters a problem report in the **Problem Log**.

The **Problem Log** is an extremely useful troubleshooting and management tool because it lets you know what types of problems are occurring on your network and specifically identifies which devices are having problems. Knowing what types of errors are present and where they are coming from can help you identify the cause of network problems.

To check for errors:

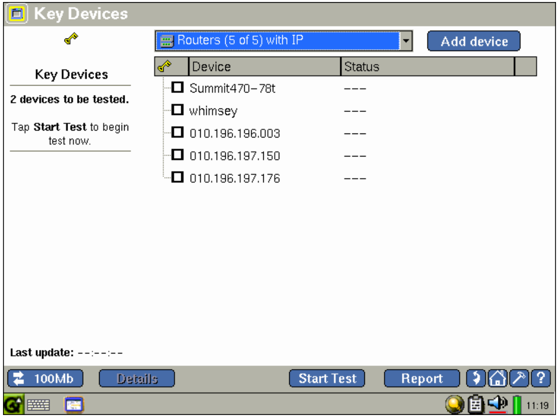
1. Select **Problem Detection**.

The preview pane shows the number of problems detected in each of the following severity groups:

- 🔴 Errors: indicates that a severe problem exists with the network or the device; the problem is disrupting or severely impeding normal use.
- ▽ Warnings: indicates that a condition exists that can possibly cause a problem with the network or device.
- ! Information: indicates that the device or network is functioning normally, but there is an event or condition that you need to be aware of.
- ✓ Resolved: indicates that the problem has been fixed or that there has a been a change in the failure state.

The 🗑 **Deleted** category maintains a count of problems that you delete from the **Problem Log** (see “Deleting a Problem from the Log” on page 66).

2. If errors are indicated, tap Details to look at the **Problem Log** (Figure 18):



Key Devices

2 devices to be tested.

Tap **Start Test** to begin test now.

Device	Status
□ Summit470-78t	---
□ whimsey	---
□ 010.196.196.003	---
□ 010.196.197.150	---
□ 010.196.197.176	---

Last update: --:--:--

epi41s.bmp

Figure 18. Problem Log

The main pane lists each device that is experiencing a problem. The **Description** column provides a brief description of the nature of the problem along with its assigned severity level.

Note

You can sort the information in the main pane by tapping one of the column headings. For example, to sort on problem severity, tap ●. A directional arrow ▽△ indicates the column you are sorting on and the direction of the sort.

3. To obtain information on a specific device, select the device.

   The preview pane shows the IP and MAC address of the problem device along with a description of the problem. A timestamp indicates when the problem was detected.

4. Tap Details to view detailed information about the device.

   The **Device Details** screen (Figure 13) is displayed. On this screen, you obtain specific information about the device.

   Follow the **Problems** link to view a **Problem Log** that lists only those problems associated with the selected device.

   You can also tap the **Interfaces** link to see the I/F status of the device or you can tap the **SNMP System Group** link to view SNMP information for the device.

Deleting a Problem from the Log

To delete a problem from the log:

1. Select the problem.
2. Tap Delete.

The deleted problem is moved to the **Deleted problems** folder in the main pane, and the number of problems is incremented in the 🗑 **Deleted** category (preview pane).

To cancel the deletion:

1. Tap ⊞ to expand the **Deleted problems** folder.
2. Select the desired problem and then tap Undo.

The problem is re-entered into the **Problem Log**, and the count of **Detected** problems in the preview pane is incremented.

RFC 2544 Tests

The RFC 2544 tests enable you to measure the performance of your network. Each test requires a second (remote) EtherScope Network Assistant running Version 3.0 software (or later) to communicate with your network.

Note

*The RFC 2544 tests are a separately purchased software option. To enable this option, you need to supply the key code for **RFC 2544/ITO ES_ITO_OPT**. For instructions on enabling software options, go to "Enabling Software Options" on page 18.*

The following tests are in the RFC 2544 test group:

- **RFC 2544 Throughput**: measures the throughput speed and efficiency of your network.
- **RFC 2544 Latency**: measures how much time it takes for frames to travel through your network.
- **RFC 2544 Loss**: measures your network's frame loss rate.

The Remote Device

The remote device operates as the DUT (Device under Test). The remote device must be an EtherScope Network Assistant.

Configuring the Remote Device

The remote device must be enabled to use the RFC 2544 test option (see "Enabling Software Options" on page 18).

In addition, the remote device must be configured with the same port number and timeout setting as the local device. To configure these settings, follow the procedure under "Configuring the Remote Unit" on page 72.

Specifying the IP Address of the Remote Device

You can designate a device for use in all of the RFC 2544 tests or you can designate a particular device for each individual test.

1. Select **RFC 2544 Tests** and then tap Details.

2. Do one of the following:

    - To specify a device for all RFC 2544 tests, tap **RFC 2544**.

    - To specify a device for a specific test, tap the name of the test or device.

3. Tap Add Device.

4. In the **Add Device** box, select the device from the drop-down list box or select **(User Defined)** and supply the IP address of the device.

5. Click OK.

Note

Repeat this procedure to add additional devices for use in the individual tests. The device name or IP address is added to the list of devices under the individual test and can be selected when you run a test.

Configuring the RFC 2544 Tests

You need to configure the test parameters and the parameters for the remote device participating in the test. You can set global configuration parameters that apply to all devices used and all tests in this suite or you can configure the devices and tests individually.

The following procedures show you how to access the configuration screens. See the online Help for detailed descriptions of the RFC 2544 test configuration parameters.

Global Configuration Parameters

To set configuration parameters that apply to all RFC 2544 tests and devices:

1. Select **RFC 2544 Tests** and then tap Details.
2. Tap Configure to display the **RFC 2544 Configuration** screen.
3. Select the desired RFC 2544 test parameters and then tap Apply to save your changes.

Individual Test and Device Parameters

Individual settings apply only to the selected test and/or device. These settings override any global parameters set under **RFC 2544 Tests**.

To set parameters for an individual test or device:

1. Select **RFC 2544 Tests** and then tap Details.
2. Tap Configure to display the **RFC 2544 Configuration** screen.
3. Tap ⊞ next to **RFC 2544** to display the list of subtests and devices.
4. Select the desired subtest or device and then tap Details to display the configuration screen and set the desired parameters.
5. Tap Apply to save your changes.

Restoring the Default Configurations

Tap Defaults to restore the configuration to factory default settings. Then, tap Apply to save the changes.

Running an RFC 2544 Test

To run a test:

1. Select the desired test from the **RFC 2544 Performance Tests** screen.
2. Tap Start.

Results

The **Status** column indicates whether results are available for the selected test.

- To view Throughput test results:
    1. Select a device under **RFC 2544 Throughput** and then tap Results.
    2. Use the radio buttons to select the **Display Mode** (FPS (Frames/Sec) or BPS (Bits/sec) and **View Mode** (table or graph).
- To view Latency test results:
    1. Select a device under **RFC 2544 Latency** and then tap Results.
    2. Use the radio buttons to select the **View Mode** (table or graph).
- To view Loss test results:
    1. Select a device under **RFC 2544 Loss** and then tap Results.
    2. Use the pull-down menu in the **Show** field to select the frame sizes to be displayed. Use the radio buttons to select the **View Mode** (table or graph).

ITO Tests

The EtherScope Network Assistant features two ITO (Internet Throughput Option) tests:

- Traffic Generator: enables you to generate background test traffic into the network. This test is helpful when you are testing new systems and configurations because it allows you to simulate diverse mixes of traffic which can help you identify and isolate network performance issues.

- Throughput: a double-ended test of bandwidth between two network nodes. This test enables you to test throughput and evaluate a link's capacity.

Traffic Generator

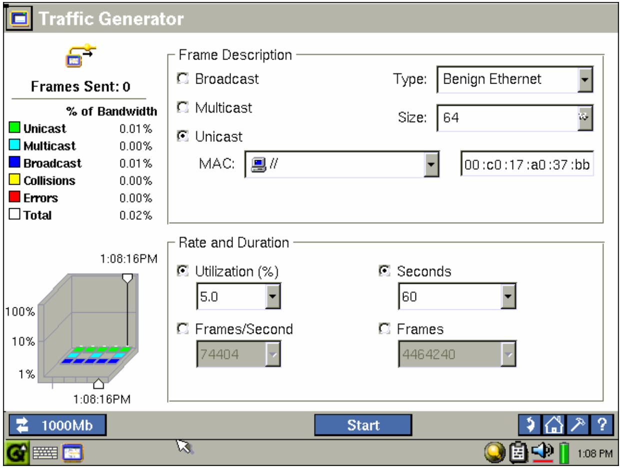
To run the **Traffic Generator** test:

1. In the main pane, tap ⊞ next to **ITO Tests** to view the subtests.

2. Tap **Traffic Generator**. Then tap Details to configure the parameters for the test (see Figure 19):

   - **Frame Description**: specify the packet type and size; in addition, provide the destination IP and MAC address.

   - **Rate and Duration**: specify the transmit rate and duration.


Traffic Generator

Frames Sent: 0

	% of Bandwidth
🟩 Unicast	0.01%
🟦 Multicast	0.00%
🟦 Broadcast	0.01%
🟨 Collisions	0.00%
🟥 Errors	0.00%
□ Total	0.02%

Frame Description
○ Broadcast
○ Multicast
● Unicast
Type: Benign Ethernet
Size: 64
MAC: // 00:c0:17:a0:37:bb

Rate and Duration
● Utilization (%) 5.0
● Seconds 60
○ Frames/Second 74404
○ Frames 4464240

epi81s.bmp

Figure 19. Traffic Generation Screen

3. Tap Start to begin the test.

The preview pane shows results of the test. You can see the number of packets the instrument is transmitting and bandwidth utilization statistics.

Throughput Test

To run the Throughput test, you need two instruments: one that functions as the local unit and a second that serves as the remote unit. The remote unit can be any of the following: a second EtherScope Network Assistant, a OneTouch™ Network Assistant with the Internet Throughput Option (ITO) installed, or an OptiView INA V4.0 analyzer.

During the test, both instruments simultaneously transmit packets to each other at a user-configurable bit rate for a specified duration. When the test is completed, the local instrument displays results for both the local and remote units (see Figure 20).

Configuring the Remote Unit

Note

This procedure assumes that the remote unit is an EtherScope Network Assistant. If you are using an OptiView INA analyzer or a OneTouch Network Assistant as the remote unit, refer to that instrument's documentation for instructions on configuring it as the remote server.

1. On the remote EtherScope Network Assistant, tap ▣. Then, select **Instrument Settings.**
2. In the preview pane, tap the **General** hyperlink. In the **Remote Throughput Testing** section:

   a) Tap (to check) **Enable as throughput remote**.

   b) Specify values for the following:

   - **Port**: identifies the port to use for the throughput protocol. Configure the same port number on both the local and remote units. This number can be changed to allow throughput testing through firewalls that block some ports.
   - **Timeout**: number of seconds the remote server should wait for additional throughput traffic from the local unit before timing out and terminating packet transmission.
3. Tap **Save Remote Throughput Settings**.

Configuring the Local Unit and Starting the Test

On the local unit, complete the following:

1. Tap the ⊞ next to **ITO Tests** to expand the list and show its subtests.
2. Select **Throughput Test.**
3. Tap **Details** to configure the following parameters for the test:
   - **Frame Description**: specify the remote device's IP address. Select the frame data pattern to be transmitted, timeout, the frame length, and the port number.

     Note

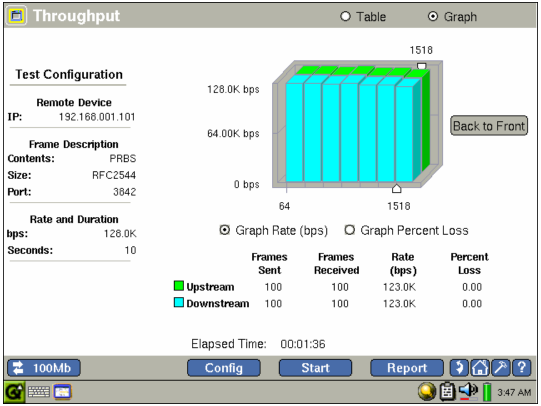
     Both the local and remote devices must be configured on the same port.
   - **Rate and Duration**: specify the transmit rate (in bits per second) and the duration of the test

4. Tap **Start** to begin the test.

   As the test progresses, **Throughput** results are continuously updated.

   The local unit keeps track of the number of frames sent, the percent received, and the percent loss for both the local and remote units.

5. To see results displayed graphically (see Figure 20), tap **Graph** (located in the title bar).



Throughput ○ Table ● Graph

Test Configuration

Remote Device
IP: 192.168.001.101

Frame Description
Contents: PRBS
Size: RFC2544
Port: 3842

Rate and Duration
bps: 128.0K
Seconds: 10

● Graph Rate (bps) ○ Graph Percent Loss

	Frames Sent	Frames Received	Rate (bps)	Percent Loss
🟩 Upstream	100	100	123.0K	0.00
🟦 Downstream	100	100	123.0K	0.00

Elapsed Time: 00:01:36

epi72s.bmp

Figure 20. Throughput Test Results

6. Tap **Stop** to end the test.

Configuring the Instrument for a Wired LAN

Although EtherScope Network Assistant is designed to provide as much automated configuration as possible, every network is different. For the instrument to provide you with the best network analysis possible, you may need to change some of the default configuration settings.

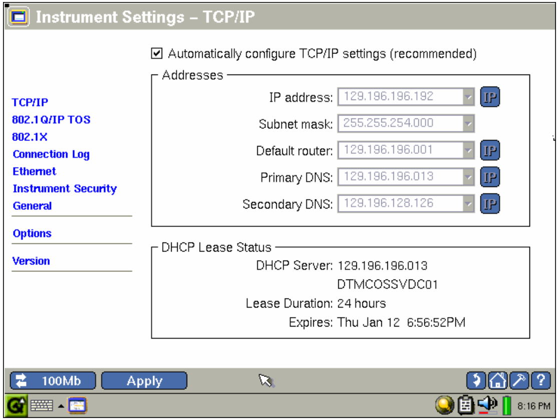
To access the instrument's configuration screens, do the following:

1. Tap the EtherScope Network Assistant icon , which is located in the upper-left corner of the title bar.

2. From the drop-down list, tap **Instrument Settings.**

   The **Instrument Settings —TCP/IP** screen (Figure 21) is displayed.

On this screen, you configure the instrument's TCP/IP settings:



Instrument Settings – TCP/IP

☑ Automatically configure TCP/IP settings (recommended)

Addresses
IP address: 129.196.196.192
Subnet mask: 255.255.254.000
Default router: 129.196.196.001
Primary DNS: 129.196.196.013
Secondary DNS: 129.196.128.126

DHCP Lease Status
DHCP Server: 129.196.196.013
DTMCOSSVDC01
Lease Duration: 24 hours
Expires: Thu Jan 12 6:56:52PM

epi86s.bmp

Figure 21. Instrument Settings—TCP/IP Screen

The hyperlinks in the preview pane take you to other configuration screens, which are described in the sections that follow.

TCP/IP Settings

If DHCP is available, the **Instrument Settings—TCP/IP** screen (Figure 21) displays the address that the instrument is able to obtain.

If you want to manually configure the IP address or change the subnet mask, do the following:

Note

When manually assigning an IP address, you can use an address for an alternate subnet but that address must be in the same broadcast domain as the EtherScope Network Assistant.

1. Clear the **Automatically configure TCP/IP settings** checkbox to disable auto-configuration of the IP settings.

2. For the address field that you want to change, do the following:

   - Tap IP and use the keyboard to type an IP address.

     OR

   - Select an address from the drop-down list.

3. Tap Apply to save your changes.

802.1Q/IP TOS Settings

The 802.1Q/IP TOS settings define the VLAN tag in the header of an Ethernet packet. The instrument uses these settings during discovery, traffic generation, RFC 2544 tests, and network service tests to make decisions about routing traffic.

In the preview pane, tap **802.1Q/IP TOS** to display the **Instrument Settings— 802.1Q/IP TOS** screen. This screen enables you to configure the instrument for tagged VLAN (802.1Q) and/or IP Type of Service (TOS) operation. These settings are applied globally to traffic from the instrument and remain in memory even after you turn off the instrument.

It is important that you configure these settings correctly. If you select a VLAN ID that is not configured on the port that the instrument is connected to, the instrument may not be able to communicate with the network. DHCP will fail and active discovery will not work. You can experience the same failure, if you enable 802.1Q on the instrument but plug it into a port that is not enabled for 802.1Q. If this happens, you can use the VLAN Statistics test to identify the VLANS that are active on the port. Then, try configuring the 802.1Q settings for the VLAN that has the highest packet count.

1. In the **8021Q Settings** section, do the following:

   a) Check **Enable 802.1Q** to select 802.1Q tagging mode.

   This setting denotes a new frame format whereby every packet that is transmitted by the instrument contains an extra four bytes in the header to include fields for the VLAN ID and a priority level for the frame (see next two items). On the receive side, the instrument extract and process this information from incoming packets.

   b) Supply the **VLAN ID** (values range from 1 to 4095)

   c) Set **Priority**: select a value between 0 and 7 (low to high) to specify a priority level for the frame.

2. In the **TOS** (Type of Service) section, select one of the following:

   - **TOS with IP Precedence** then check one of the type of service parameters (**Delay**, **Throughput**, **Reliability**, or **Cost**) and select a priority in the **IP Precedence** box.

   - **TOS with DSCP** then supply a value for DSCP (Differentiated Service Code Point).

3. Tap Apply to save your settings. The instrument restarts its tests with the new configuration.

802.1X Settings

The 802.1X standard defines the mechanism for port-based network access control. This provides a means of authenticating and authorizing devices attached to a LAN port. This screen allows for the configuration of the 802.1X security.

The supported authentication types are:

- --None—
- EAP TLS
- EAP GTC
- EAP MD5
- EAP MSCHAPV2
- PEAP GTC
- PEAP MD5
- PEAP MSCHAPV2
- PEAP TLS
- TTLS PAP
- TTLS CHAP
- TTLS MSCHAP
- TTLS MSCHAP-V2
- TTLS EAP-MD5
- TTLS EAP GTC
- TTLS EAP MSCHAP-V2
- TTLS EAP-TLS

The TLS authentication types (also called SmartCard) allow you to import a User Certificate provided by your IT administrator and use alternate IDs (in Advanced Options) in the encryption.

The other encryption types allow you to enter a User Name and Password. These encryption types are not as secure as the TLS encryption types.

Connection Log

The **Connection Log** provides detail about the 802.1X authentication and authorization process, and indicates whether it passed or failed. It also provides DHCP detail to which servers reply to DHCP requests and which DHCP offers were ignored by EtherScope.

Ethernet Settings

On **Instrument Settings—Ethernet** screen, you can override the instrument’s link auto-negotiation process and force EtherScope Network Assistant to link at a user-selected speed and duplex.

To link at particular duplex setting, tap **Use Forced Setting.** Then select one of the settings in the **Forced Setting** group.

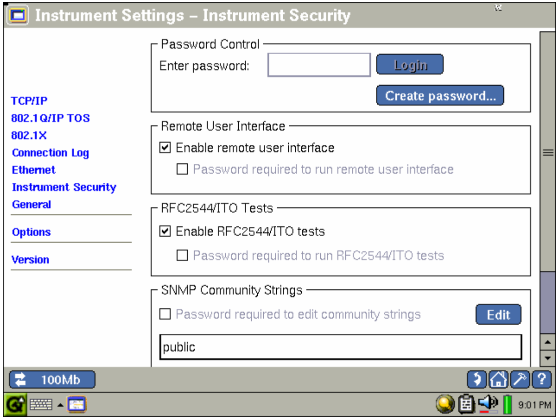
Note

*An asterisk (*) next to the value on the link button (located in the lower- left corner of the task bar) indicates the speed/duplex is a forced setting.*

At the bottom of this screen, a factory assigned MAC address is shown. You can change this address to enable testing of switch forwarding tables and ARP caches as part of the troubleshooting process.

Instrument Security Settings

On the **Instrument Settings—Instrument Security** screen (Figure 22), you can provide password-level security for your EtherScope Network Assistant. This screen enables you to password-protect access to EtherScope Network Assistant through the remote user interface, authorize running of RFC 2544/ITO tests, and prevent unauthorized users from editing the instrument’s SNMP community strings or viewing the remote user interface.



Password Control
Enter password:

Remote User Interface
☑ Enable remote user interface
□ Password required to run remote user interface

RFC2544/ITO Tests
☑ Enable RFC2544/ITO tests
□ Password required to run RFC2544/ITO tests

SNMP Community Strings
□ Password required to edit community strings
public

epi85s.bmp

Figure 22. Instrument Settings–Security Screen

If a field is password-protected, this symbol denotes that the field is secure: "*".   The fields and controls on the **Security** screen are disabled until a user successfully enters the password and logs in using the **Login** button.

On the **Security** screen, you can also configure the instrument's SNMP community strings. The default community strings are "public", "private", and "security". You can change the default strings to strings that are used on your network.

Note

The discovery process successively tries the community strings in the order in which they are listed. For a quicker discovery, you should list the strings in order of frequency of use.

General Settings

On the **Instrument Settings— General** screen, you can change the following settings for your EtherScope Network Assistant:

- **Restore Defaults**: resets the instrument to the factory default settings. These include interface configurations and address settings. If you restore the instrument's default settings, any changes that you made to the instrument and all current data is lost.

- **Edit user-defined devices:** lets you edit or delete existing user-defined devices, or add a new device that is either outside of the local broadcast domain or not being discovered.

- **Remote RFC 2544/ITO Throughput Testing**: enables/disables the instrument to serve as the RFC 2544/ITO Throughput remote server and to interoperate with another EtherScope Network Assistant serving as the local unit during a remote throughput test.

- **Preferences**

    - **Show vendor prefix with MAC address**: lets you control how a device's MAC address is shown. By default, it is shown with a vendor prefix. When the box is unchecked, the MAC address is shown in raw hexidecimal format.

- **Enable fast connect mode** (applies to wired LAN only): lets you quickly obtain a network link and DHCP address.

  By default, when EtherScope Network Assistant is first plugged into a network, it tries to determine whether it is connected to the same broadcast domain it was previously connected to. If it is, it saves the data it previously collected.

  Use the **Enable fast connect mode** setting when you repeatedly connect EtherScope Network Assistant to different networks because usage results in a faster response time. For example, select **fast connect mode** when you are verifying the connectivity of multiple office cubicles in a new installation. In this mode, the instrument automatically resets its discovery database when changing the network connection or when returning to the **Test Results** screen from the **Cable** or **Signal Verification** screens.

- **Edit SNMP System Name**: tap Edit and then supply a new SNMP system name for the instrument. Tap OK to save.

Monitoring and Troubleshooting a Fiber LAN

The ES-FIBER-OPT option supports 1000BaseSX, 1000BaseLX, and 1000BaseZX fiber. The basic steps for monitoring a fiber LAN are listed below.

1. Install the SFP fiber adapter (see “Installing and Removing an SFP Fiber Adapter” on page 83.
2. Power on the instrument (see “Turning the Instrument On and Off” on page 14).
3. If necessary, change the interface type to LAN (see “Selecting the LAN or WLAN Interface” on page 15).

All the existing LAN features are supported when EtherScope is connected to gigabit fiber interface with the following exceptions:

- The link speed displays 1000MB and the fiber type (SX, LX, or ZX)
- The Cable Verification and Signal Verification tests are replaced with the fiber Loss Test (requires an optional Fiber Optic Meter)

Note

If both the RJ-45 copper and SFP fiber (SX, LX, or ZX) adapter are connected to the network at the same time and the instrument is trying to establish link, the fiber connection has priority over the copper connection.

Installing and Removing an SFP Fiber Adapter

To install an SFP fiber adapter:

1. With the instrument turned off, remove the protective cap as shown in Figure 23.
2. Insert the fiber adapter, making sure that it is firmly seated into the connector.

⚠Warning

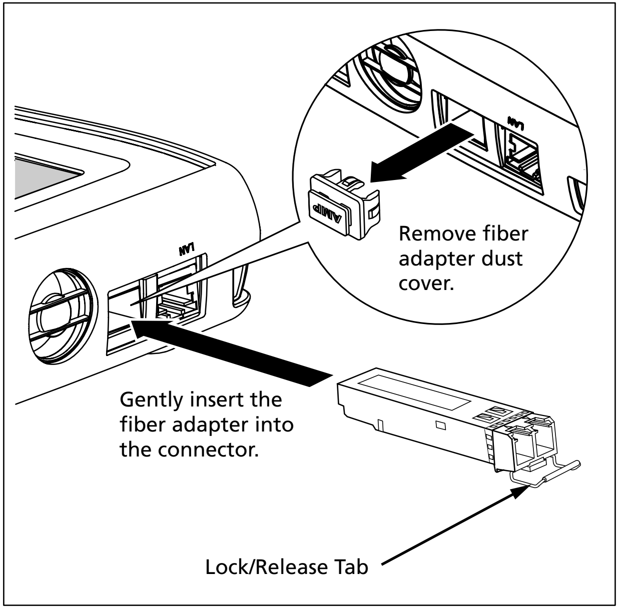
SFP fiber adapters are Class 1 laser light-emitting products. Avoid staring into the SFP module while the EtherScope Network Assistant is on; otherwise injury to the eyes may occur.

To remove the fiber adapter:

1. Make sure the instrument is turned off.
2. Press the release tab located on the back of the adapter.

⚠ Caution

Do not pull the fiber adapter without pressing the release tab or damage to the adapter may occur.


LAN
AMP
LAN
Remove fiber adapter dust cover.
Gently insert the fiber adapter into the connector.
Lock/Release Tab

eih85f.eps

Figure 23. Inserting the Fiber Adapter

Monitoring and Troubleshooting a Wireless LAN

The basic steps for monitoring a wireless LAN (WLAN) are listed below. Detailed information for a step can be obtained by consulting the referenced section.

1. Install the WLAN Card.
2. Power on the instrument (see “Turning the Instrument On and Off” on page 14).
3. If necessary, change the interface type to WLAN (see “Selecting the LAN or WLAN Interface” on page 15).

   Note

   If you are operating EtherScope Network Assistant for the first time, you should configure a default SSID to automatically test link and to use active discovery methods. See “Wireless Instrument Security Settings” on page 101. If operating the instrument in passive scan mode, you do not have to configure security settings.

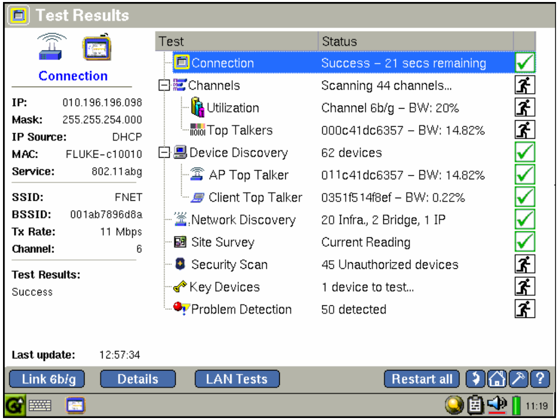
   EtherScope Network Assistant runs a series of passive scan tests then attempts to establish a link to an AP that is configured with the default SSID.
4. View autotest results. See “Viewing AutoTest Results” on page 38.
5. Make any needed configuration changes to match your wireless network. See “Configuring the Instrument for a Wireless LAN” on page 98.

Installing the WLAN Card

To install the wireless LAN card, insert it into **SLOT 1**, which is located on the top side panel (see Figure 3).

Viewing AutoTest Results

After you power on the instrument, it runs the automated tests and displays the **Test Results** screen, as shown in Figure 24.



Test Results

Connection

IP: 010.196.196.098
Mask: 255.255.254.000
IP Source: DHCP
MAC: FLUKE-c10010
Service: 802.11abg

SSID: FNET
BSSID: 001ab7896d8a
Tx Rate: 11 Mbps
Channel: 6

Test Results:
Success

Last update: 12:57:34

Test	Status	
Connection	Success – 21 secs remaining	✓
Channels	Scanning 44 channels...	🏃
Utilization	Channel 6b/g – BW: 20%	🏃
Top Talkers	000c41dc6357 – BW: 14.82%	🏃
Device Discovery	62 devices	✓
AP Top Talker	011c41dc6357 – BW: 14.82%	✓
Client Top Talker	0351f514f8ef – BW: 0.22%	✓
Network Discovery	20 Infra., 2 Bridge, 1 IP	✓
Site Survey	Current Reading	✓
Security Scan	45 Unauthorized devices	🏃
Key Devices	1 device to test...	🏃
Problem Detection	50 detected	🏃

epi73s.bmp

Figure 24. Wireless LAN Test Results Screen

The **Test Results** screen gives you at-a-glance visibility into the state of your WLAN.

The main pane displays the name of each test and reports its status. The icons along the right side give you a visual indication of the progress and status of each test:

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

The preview pane provides a summary of the results of the test that is selected in the main pane.

Note

*When autotest finishes, the **Connection** test (the default selection) is highlighted.*

You can get a quick idea of the overall health of your network and see what devices and services are running by tapping each test listed in the main pane and then viewing its summary results in the preview pane.

The individual autotests are described in this section. To obtain in-depth results for a test, select it from the main pane. Then tap Details.

Connection Test

The **Connection** test checks the status of the link and determines whether EtherScope Network Assistant established an association with a wireless access point. The instrument first scans the wireless network, and then attempts to link to an AP that is configured with the default SSID.

After autotest runs, the **Connection** test is highlighted. The **Status** column reports the results of the attempt to connect:

- If the attempt to link to the default SSID/AP is successful, this status icon is displayed: ✓. The IP address that the instrument acquired is identified in the **Status** line.

  The preview pane shows you information about the connection, including the SSID, IP address, and channel.

- If the attempt to link to the default SSID/AP fails, this status icon is displayed 🚫 , and the reason for the failure (for example, no Access Point found) is reported.

EtherScope Network Assistant runs in active scan mode, in which it continuously monitors active channels. The **Scan** button in the lower left corner updates you on which channels are being scanned.

To view details about the connection, tap Details.

The **Connection** details screen is displayed. This screen shows you the connection settings (the results of auto-configuration using DHCP) and configuration options. You can change the current configurations from this screen (see "Configuring the Instrument for a Wireless LAN" on page 98 for assistance).

Channels Test

The **Channels Test** scans all channels in the 802.11a and 802.11 b/g spectrums to locate active channels, active APs, active clients, and ad hoc devices. For each active channel discovered, the test focuses on key metrics that give you information about a channel's configuration and health.

To view results:

1. Tap **Channels**.

   The main panel indicates how many channels are being scanned. The preview pane shows separate summaries of results for the 802.11a and 802.11b/g networks. A small graph, which accompanies each summary, visually displays the percentage of local utilization.

2. To view statistics for individual channels, tap Details.

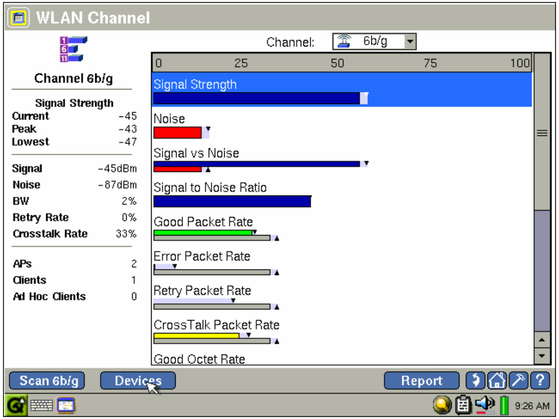
   The list of all channels is displayed.

3. To monitor basic vital signs, such as signal strength or noise, select the desired metric from the **Channel Metric** box.

   The main pane redisplays the list of channels and for each channel reports results for the metric you selected.

4. To focus in on a particular channel, select it from the list and view its summary information in the preview pane. Then, tap Details.

   The main pane (Figure 25) displays all of the metrics for the selected channel.



WLAN Channel

Channel: 6b/g

Channel 6b/g

Signal Strength	
Current	-45
Peak	-43
Lowest	-47
Signal	-45dBm
Noise	-87dBm
BW	2%
Retry Rate	0%
Crosstalk Rate	33%
APs	2
Clients	1
Ad Hoc Clients	0

epi74s.bmp

Figure 25. Channel Test Details Screen

5. To find out what APs and clients are on the channel, tap Devices.

The **Channels** test contains two subtests:

- **Utilization**
- **Top Talkers**

Tap the ⊞ next to **Channels Test** to expand the list so that you can see these two subtests.

Utilization Test

The **Utilization** test reports utilization and error statistics for the busiest channels (up to five) in both the 802.11a and 802.11 b/g spectrums.

1. Tap **Utilization**.

   The **Status** column in the main pane identifies the channel consuming the most bandwidth.

   The preview pane displays up to five of the most active channels. For each channel, you can view bandwidth utilization (%) and transmission rates (packets per second). This information is continuously updated.

2. To view channel details, do one of the following:

   - To focus on a particular channel, tap the desired hyperlink in the preview pane.
   - To focus on the busiest channel, tap Details.

   The **Channel Utilization** screen is displayed. On this screen, you can view (in graphic and tabular form) the types of traffic (for example, FCS Errors or Retries) seen on the network and the percentage of bandwidth each traffic type is consuming.

   Note that you can look at a different channel's statistics. To do this, select the desired channel from the **Channel** box.

   You can also tap the graph and look at statistics for a particular time period. The statistics for the time period you select are also given in the accompanying table. To change the sampling frequency (default = 5 seconds), select a time period from the **Update every** list box.

Top Talkers

The **Top Talkers** test monitors the network to locate devices that are consuming the most bandwidth.

1. Tap Top Talkers.

   The **Status** column in the main pane identifies the device using the most bandwidth (util %).

   The preview pane shows you the most active (up to five) devices and displays bandwidth usage (util %) for each.

2. To view details, tap the hyperlink (in the preview pane) for the desired device.

   The **Top Talkers** screen is displayed. On this screen, you can view bandwidth utilization and packet rates for all discovered devices.

   To filter by channel or SSID, select from the **Channel** or the **SSID** drop-down list box, respectively.

Device Discovery Test

After a successful autolink, the instrument performs active discovery, searching for APs and network devices. The instrument examines each device it discovers to learn more about the device's capabilities and to detect possible problems.

The **Device Discovery** test lets you know what devices the instrument sees on your network. As devices are discovered, they are automatically added to the instrument's discovery database.

1. Tap **Device Discovery**.

   The preview pane shows you the total number of discovered devices.

A break out of the number of devices in each of the following categories is displayed:

- **Access Points**
- **Mobile Clients**
- **Hosts**
- **Bridges**

2 Tap Details.

The **Device Discovery** details screen is displayed. On this screen, you can obtain specific information (for example, the SSID and MAC address) about each discovered device. This screen also informs you whether any discovered device is experiencing problems.

3. To obtain detailed information for a particular device, select it. Then, tap Details.

Note

If a device you are interested in tracking is not discovered by the instrument, you can add it to the discovery database from the details screen. See "Adding a Device to the Discovery Database" on page 55.

Device Discovery has two subtests:

- **AP Top Talker**
- **Client Top Talker**

Select **Device Discovery**. Then tap ⊞ to expand the list so that you can see the subtests.

AP Top Talker

The **AP Top Talker** test identifies the access point that is consuming the most bandwidth.

1. Tap **AP Top Talker**.

   The preview pane identifies the device (by name and SSID) and shows the channel it is active on. You can also see utilization and security information for the device.

2. Tap **Details** to obtain more detailed information about the AP.

   On the Device "details" screen, you can tap one of the hyperlinks to look view specific metrics, such as signal strength or Tx/Rx information.

   If the AP is experiencing problems, you can also follow a link to navigate to the **Problem Log** to find out what specific problems it is having. Depending on the type of problem detected, you may need to run one of the diagnostic tests. To run a test, tap the desired hyperlinks (for example, **Wireless Throughput** or **Trace Route**).

Client Top Talker

The **Client Top Talker** test identifies the device that is consuming the most bandwidth.

1. Tap **Client Top Talker**.

   The main pane identifies the device and shows you the amount of bandwidth it is consuming. The preview pane identifies the client (by name and SSID) and reports the channel it is active on. You can also view utilization and access point information for the device.

2. Tap Details to obtain more detailed information about the device.

   The **Device Details** screen is displayed. In the main pane, you can view device-specific information (for example, device type and security). In the preview pane, you can follow a hyperlink to view its signal strength, WLAN statistics, or Tx/Rx rate information.

   You can also follow one the hyperlinks to run one of the diagnostic tests.

Network Discovery

The **Network Discovery** test scans the wireless environment and discovers all networks within range.

1. Tap **Network Discovery**.

   The preview pane categorizes the number and types of networks discovered:

   - **Infrastructure** (802.11a/b/g)
   - **Adhoc**
   - **Bridge**
   - **IP Subnets**

   Within each category, EtherScope Network Assistant reports the number of devices it discovered.

2. To view details for one of the network components, tap the associated hyperlink in the preview pane.

   The **Network Discovery** details screen shows you the network hierarchy, which provides an indication of how the WLAN is configured.

   Your selection is highlighted so that you can see where it fits in the network structure. You can also see whether any network or device within the network is experiencing problems.

3. To obtain greater detail, tap a hyperlink or select a device and tap Details.

Site Survey

The **Site Survey** test enables you to gather information on the APs in your WLAN. You can use **Site Survey** information as a starting point for planning and designing your WLAN. Specifically, it can help you figure out if you have enough APs and whether your APs are appropriately located to give you the best signal coverage.

1. Tap **Site Survey**.

   The **Status** column in the main pane displays **Current Reading**.

   The preview pane displays the four APs with the strongest signal strength. The MAC address, SSID, channel number, and signal strength are shown for each AP.

2. Do one of the following;

- To look at detailed information for a particular AP, tap the associated MAC address hyperlink in the preview pane.

  The details screen shows a list of all of the APs in your WLAN. The AP you selected is highlighted and its detailed information is displayed in the preview pane.

  OR

- Tap Details to view a list of all of the APs in your WLAN.

  From this list, you can select a particular AP and tap Details to view specifics.

  If necessary, you can run the diagnostic tests listed in the preview pane.

3. If you want to save the data obtained from a site survey. Do the following:

- Tap Save.

  The data is timestamped and saved in the **Previous Survey** list. To view a survey's data, select it from the drop-down list.

  OR

- Tap Report.

  The survey report is created and saved to a CompactFlash memory card.

Security Scan

Note

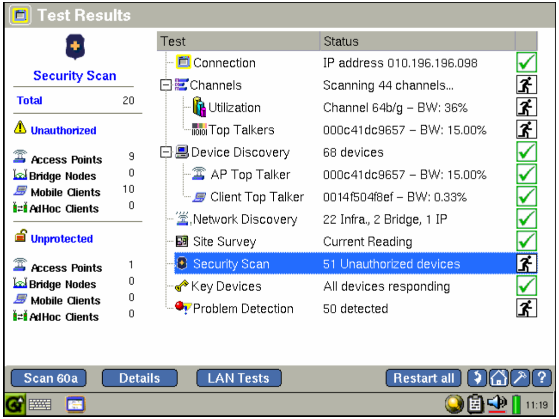
> *To obtain meaningful results from a **Security Scan**, you should first configure the instrument to identify authorized devices. See "Wireless Authorization Settings" on page 102 to find out how to set a device's authorization level.*

The **Security Scan** test performs a security check on your network. It identifies unauthorized (rogue) and unprotected devices within each category.

To view **Security Scan** results:

1. Tap **Security Scan**.

   The preview pane (see Figure 26) summarizes the number of ⚠ unauthorized (rogue) and 🔓 unprotected APs and clients that were detected.



Test Results

Security Scan

Total	20
⚠ Unauthorized	
Access Points	9
Bridge Nodes	0
Mobile Clients	10
AdHoc Clients	0
🔓 Unprotected	
Access Points	1
Bridge Nodes	0
Mobile Clients	0
AdHoc Clients	0

Test	Status	
Connection	IP address 010.196.196.098	✓
Channels	Scanning 44 channels...	
Utilization	Channel 64b/g – BW: 36%	
Top Talkers	000c41dc9657 – BW: 15.00%	
Device Discovery	68 devices	✓
AP Top Talker	000c41dc9657 – BW: 15.00%	✓
Client Top Talker	0014f504f8ef – BW: 0.33%	✓
Network Discovery	22 Infra., 2 Bridge, 1 IP	✓
Site Survey	Current Reading	✓
Security Scan	51 Unauthorized devices	
Key Devices	All devices responding	✓
Problem Detection	50 detected	

epi75s.bmp

Figure 26. Security Scan

2. Tap **Details**.

   The **Security Scan** details screen lists the names and SSIDs of devices with security issues within the category you selected.

3. To obtain in-depth information about a specific device, select it and then tap **Details**.

Key Devices Test

The **Key Devices** test verifies connectivity between your EtherScope Network Assistant and network devices you designate as "key". Before running the **Key Devices** test, you first need to create a list of devices that you want the instrument to keep track of. See "Defining Key Devices" on page 62 for instructions on setting up your list.

Problem Detection

The **Problem Detection** test checks each discovered device in your WLAN for problems. If a problem is detected, it is entered into the **Problem Log**. For a detailed description of this log, see "Problem Detection" on page 64.

Configuring the Instrument for a Wireless LAN

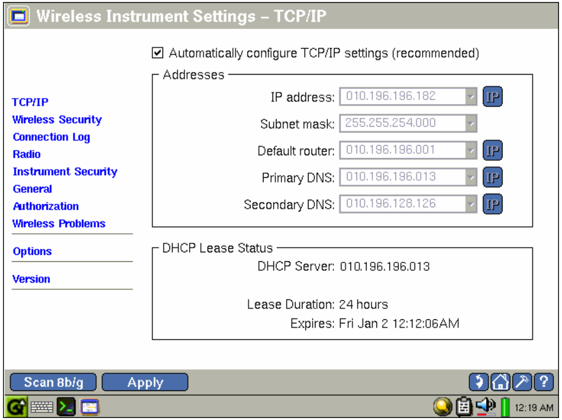
For the instrument to provide you with the best analysis possible of your wireless WLAN, you may need to change some of the default configuration settings.

To access the configuration menus, do the following:

1. Tap ▣.

2. From the drop-down list, select **Instrument Settings**.

   The **Wireless Instrument Settings —TCP/IP** screen (Figure 27) is displayed:



Wireless Instrument Settings – TCP/IP

☑ Automatically configure TCP/IP settings (recommended)

Addresses

IP address: 010.196.196.182

Subnet mask: 255.255.254.000

Default router: 010.196.196.001

Primary DNS: 010.196.196.013

Secondary DNS: 010.196.128.126

DHCP Lease Status

DHCP Server: 010.196.196.013

Lease Duration: 24 hours

Expires: Fri Jan 2 12:12:06AM

epi79s.bmp

Figure 27. Wireless Instrument Settings—TCP/IP Screen

From this screen, select a hyperlink in the preview pane to view screens that enable you to configure your EtherScope Network Assistant. These screens are briefly described in the following sections.

Wireless TCP/IP Settings

To configure your wireless LAN’s TCP/IP settings, tap the **TCP/IP** hyperlink. For information about this screen, see “TCP/IP Settings” on page 75.

Wireless Security Settings

This screen enables you to manage the instrument’s security parameters. In order for the instrument to perform active discovery of wireless devices (including discovery of IP addresses and DNS names), you must configure a default SSID and set its security appropriately.

1. Tap the **Wireless Security** hyperlink.

2. On the **Wireless Instrument Settings—Security** screen, configure the following:

   - **SSID**
     From the drop-down list, select the Service Set Identifier (SSID) that identifies the WLAN to link to. As part of the discovery process, the instrument attempts to obtain details about all devices it sees in the WLAN network using the SSID you select.

     Tap (to enable) **Default** to make the SSID you select the default SSID.

   - **Security**
     In this section, select the authentication type. For advanced security, tap (to check) **Advanced Options** then supply the desired information.

3. Tap Apply to save the changes.

Connection Log

The **Connection Log** provides detail about the wireless authentication and authorization process, and indicates whether it passed or failed. It also provides DHCP detail to which servers reply to DHCP requests and which DHCP offers were ignored by EtherScope.

Wireless Radio Settings

To ensure correct radio performance, you need to configure the radio card that is installed in **SLOT 1**.

1. Tap the **Radio** hyperlink.

2. On the **Wireless Instrument Settings—Radio** screen, configure the following:

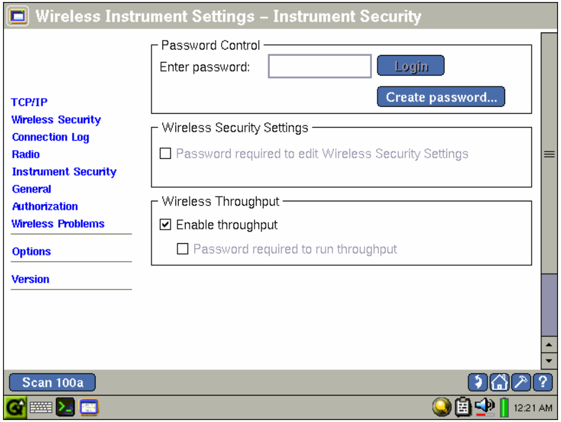
   - **Country Setting**: select a country from the list. The country you choose determines which channels the radio card uses. If you choose Global, all channels are configured.

- **Signal Strength**: if necessary, drag the slider to fine tune signal strength settings. The Offset is only available if **Show dBm** is selected.
- **Show dBm/Show Percent**: select to specify how you want signal strength displayed (in dBm or as a percent) for test results.
- **Active Bands**: selects the frequency range that you want the instrument to use.
- **Transmit Settings: Enable Transmit** (default) allows the instrument to link to the SSID specified on the **Wireless Instrument Settings — Wireless Security** screen and perform active discovery. If this feature is not checked, the instrument performs passive discovery only.

3. Tap **Apply** to save the changes.

Wireless Instrument Security Settings

Tap the **Instrument Security** hyperlink to display the **Instrument Security** configuration screen (Figure 28):



Wireless Instrument Settings – Instrument Security

Password Control
Enter password:

Wireless Security Settings
☐ Password required to edit Wireless Security Settings

Wireless Throughput
☑ Enable throughput
☐ Password required to run throughput

epi76s.bmp

Figure 28. Wireless Instrument Settings—Instrument Security Screen

On the **Instrument Security** screen, you can create a password to control access to the instrument and prevent unauthorized users from changing its security settings.

Wireless General Settings

Tap the **General** hyperlink to display the **General** settings screen. On this screen, you can change the instrument's global settings. You can also reset your instrument to the factory default settings. In addition, you can edit or delete any user-defined devices or add a new device to the instrument's discovery database.

If you have the Internet Throughput Option (ITO) installed, you can enable the instrument as a remote throughput device. In addition, you can configure how the MAC address for a device is shown on the instrument's result screens; that is, with a vendor prefix or in raw hexadecimal format.

Wireless Authorization Settings

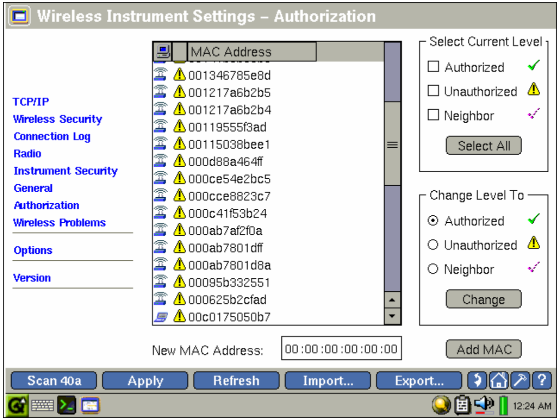
On the **Authorization** screen, you can classify discovered clients and access points as **Authorized**, **Unauthorized**, or **Neighbor**. This feature can help you manage security because EtherScope Network Assistant automatically flags any unauthorized device it discovers.

Note

> *All discovered devices are initially classified as **Unauthorized** ⚠.*

To reclassify a device, do the following:

1. Tap the **Authorization** hyperlink to display the **Wireless Instrument Settings – Authorization** screen (Figure 29):



Wireless Instrument Settings – Authorization

TCP/IP
Wireless Security
Connection Log
Radio
Instrument Security
General
Authorization
Wireless Problems
Options
Version

MAC Address
001346785e8d
001217a6b2b5
001217a6b2b4
00119555f3ad
00115038bee1
000d88a464ff
000ce54e2bc5
000cce8823c7
000c41f53b24
000ab7af2f0a
000ab7801dff
000ab7801d8a
00095b332551
000625b2cfad
00c0175050b7

Select Current Level
□ Authorized ✓
□ Unauthorized ⚠
□ Neighbor ✓

Change Level To
● Authorized ✓
○ Unauthorized ⚠
○ Neighbor ✓

New MAC Address: 00 :00 :00 :00 :00 :00

epi77s.bmp

Figure 29. Wireless Instrument Settings — Authorization Screen

2. Select an individual device from the list or select an authorization level from the **Select Current Level** group box and then tap Select All to select all devices with that authorization level.

3. Select one of the **Change Level To** settings and then tap Change.

4. Tap Apply to save your changes and update the list of devices.

Wireless Problem Settings

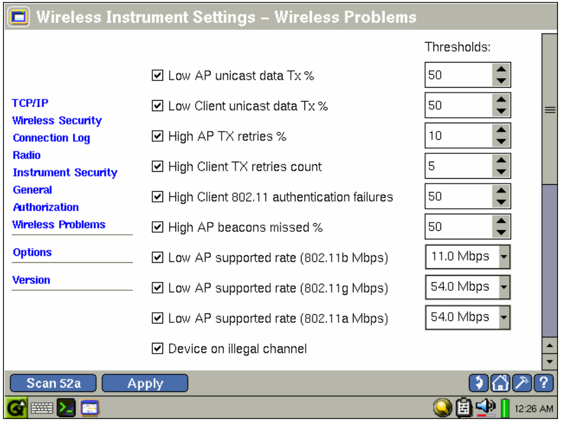
The **Wireless Problems** screen enables you to change the threshold setting for a problem and select which problems are reported.

Note

*The threshold setting specifies a value above or below which a monitored class of events is considered a problem. If the instrument detects a value above or below the setting you specify, it responds by entering the problem into the **Problem Log**.*

To set problem thresholds:

1. Tap the **Wireless Problems** hyperlink to display the **Wireless Instrument Settings—Wireless Problems** screen (Figure 30).



	Thresholds:
☑ Low AP unicast data Tx %	50
☑ Low Client unicast data Tx %	50
☑ High AP TX retries %	10
☑ High Client TX retries count	5
☑ High Client 802.11 authentication failures	50
☑ High AP beacons missed %	50
☑ Low AP supported rate (802.11b Mbps)	11.0 Mbps
☑ Low AP supported rate (802.11g Mbps)	54.0 Mbps
☑ Low AP supported rate (802.11a Mbps)	54.0 Mbps
☑ Device on illegal channel	

epi78s.bmp

Figure 30. Wireless Instrument Settings—Wireless Problems Screen

This screen lists all of the wireless problems EtherScope Network Assistant detects that have configurable threshold values.

2. For each problem whose threshold you want to change, select a value in the selection box.
3. Tap Apply.
4. To turn off problem reporting, tap (to uncheck) the box to the left of the desired problem.

Documenting Your Network (LAN and WLAN)

Having a well documented network can help you solve problems quickly when they arise and can even assist you with managing the security of your network. EtherScope Network Assistant enables you to document the state of your network. You can record network attributes, baseline performance, a device inventory, a problem log, and switch-port statistics – all in XML-formatted files.

Saving a Report

On most screens, a Report button is available that enables you to create reports and save them in a web-viewable file. Reports are saved in the **Reports** directory.

To save a report:

1. Make sure that the CompactFlash memory card is installed in **SLOT 2**.

Note

If a CompactFlash memory card is not detected, you are reminded to insert the card.

2. Tap Report.
3. Tap **New Report**.

   A default name is provided in the **New Report** text entry box.

4. Tap ⌨ and then supply a name for the report.

5. Tap OK to save.

Managing Reports

The **File Manager** provides access to your saved reports, enabling you to view and rename them, and delete those that you no longer need.

To access the **File Manager**:

1. Tap .

2. Select 📄 **Applications** from the drop-down list.

3. Tap **File Manager** to display the list of saved files.

Viewing a Report

To view a report:

Note

*The following procedure shows you how to view a report from the **File Manager**. You can also view a report by tapping followed by 📄 **Reports**, and then tapping the report that you want to view.*

1. From the **File Manager** list, select the file you want to view.

2. Tap **File**. From the **File** menu, tap **Open** to view the contents of the file.

Renaming a Report

To rename a report:

1. From the **File Manager** list, select the file you want to rename.
2. Tap **File**. From the **File** menu, tap **Rename**.

   The selected report is highlighted.
3. Use the keyboard to type a new name for the file.

Deleting a Report

To delete a report:

1. From the **File Manager** list, select the file you want to delete.
2. Tap **File**. From the **File** menu, tap **Delete**.
3. When prompted, tap Yes.

   The file is deleted from the CompactFlash memory card.

Performing a Site Survey (WLAN only)

Another way to document your WLAN is to do a site survey. A site survey can help ensure that your WLAN has the best coverage and has no "dead spots".

A site survey enables you to test your network from a number of specific locations so that you can determine how to segment the WLAN to balance network capacity, ensure adequate signal coverage, and to manage interference.

It is good practice to perform site surveys at the start of a project. You can save those surveys and use them as baselines when troubleshooting changes or problems.

For instructions on performing a site survey, see "Site Survey" on page 95.

Running the Diagnostic Tests

EtherScope Network Assistant provides a set of specialized tests that you can use to diagnose specific network problems, such as connectivity and performance, and to obtain critical information about hosts, devices, and services on your network. These tests include the following:

- Ping
- Trace Route
- Trace Switch Route (LAN only)
- Wireless Throughput (WLAN only)
- Locate (WLAN only)
- Link (WLAN only)
- Login Diagnosis (WLAN only)
- Signal Strength (WLAN only)
- WLAN Statistics (WLAN only)
- Tx/Rx Rate (WLAN only)

You can access the diagnostics tests in one of two ways:

Note

The list of available tests differs depending on which method you use to access the tests.

- Tap 🔨 and select the desired test from the drop-down list.

  OR

- Select a device. Then, tap **Details**.

  If the diagnostic test is available, it appears as a blue hyperlink in the preview pane. Tap the name of the diagnostic test to access it.

Ping

The **Ping** test is a general-purpose connectivity tool that you can use to determine if a device on the network is reachable.

Ping results are displayed on the EtherScope Console screen. Results include the number of packets transmitted and received and the response time (in ms).

Trace Route

The **Trace Route** test “traces the route” to a specific device. This test can help you identify slow, congested links since the results show the number of hops and the travel time.

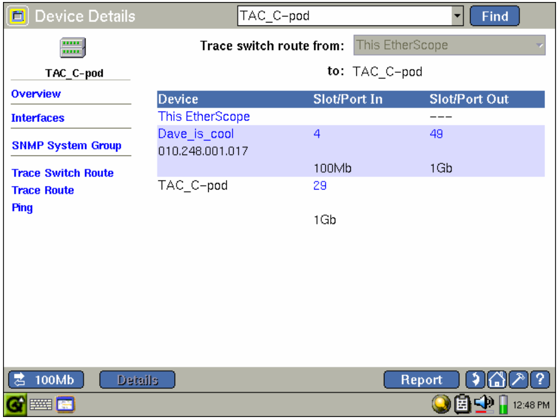
Trace Route can also detect split routes taken to the destination device. Load balancing problems or intermittent physical problems resulting from the cycling up or down of a link (called “route flapping”) can cause split routes.

Trace Switch Route

The **Trace Switch Route** test can help you solve connectivity and configuration problems by tracing the route of a packet between the instrument and a host or device on the network. The test narrows the domain and can help you identify the physical location of a problem within the network.

If the **Trace Switch Route** test is available, you can run it by tapping the hyperlink **Trace Switch Route** in the preview pane of the **Device Details** screen (see Figure 13).

Figure 31 shows a trace from EtherScope Network Assistant to a host computer. The trace identifies the In and Out ports on the switches along with the names, MAC address, and status of each device in the trace.



TAC_C-pod

Trace switch route from: This EtherScope

to: TAC_C-pod

Device	Slot/Port In	Slot/Port Out
This EtherScope		---
Dave_is_cool 010.248.001.017	4 100Mb	49 1Gb
TAC_C-pod	29 1Gb	

epi47s.bmp

Figure 31. Trace Switch Route Screen

Wireless Throughput

The **WLAN Throughput** test measures the bandwidth of the connection to a WLAN (SSID) or to a specific AP. The device must be connected as a client to the network. The test uses the following methods to test the bandwidth:

- Ping: used to test with any remote device that supports Ping.

  To use Ping, select **Ping**. Then select the IP address of the target device from the drop-down list box.

- FTP: used only with a device running an FTP server. Measures the time it takes to send or receive a file.

  To use FTP, select **FTP** then select the IP address of the target device from the drop-down list box. In addition, supply the **Username** and **Password**.

Throughput results are measured in Kbps and include **last**, **min** (best), **avg**, and **max** (worst) values. You can view these results in a graph or a table.

Locate

Note

> *To run this test, you need to use an omni-directional antenna. You can use the internal omni-directional antenna, which is built into the WLAN card, or you can attach the external omni-directional antenna (supplied) to the WLAN card.*

The **Locate** test enables you to use your instrument to find wireless devices using your network. The test can help you track down the location of an unauthorized or interfering device that is using your network.

The **Locate** test detects the signal strength of a wireless device. The closer you are to the device of interest, the greater its signal strength. Using these signal strength measurements, you can home in on the location of the device.

Signal strength measurements are displayed in a bar graph; power levels are shown in dBm’s. You use the pull-down menus and buttons to operate the graph:

- **Period**: sets how often the graph is updated.
- **Range**: changes the scale of the graph. If you set the range to **Auto**, the scale automatically adjusts to fit the samples.
- **Pause/Resume**: Stops/restarts the sampling.
- **Clear**: clears all signal strength measurements.

For complete information on **Locate** test functions and for helpful search strategies, consult the online Help.

Link

Note

> *Before running this test, you need to configure the appropriate SSID. See "Wireless Security Settings" on page 99.*

The **Link** test applies only to APs. The test determines the instrument's ability to connect to a selected AP. If a connection is made, the test reports signal strength and the signal strength of the RF of the associated AP. It also reports information returned by the DHCP server.

Login Diagnosis

The **Login Diagnosis** test monitors a wireless client's attempt to authenticate on the wireless LAN. The test monitors the EAP (Extensible Authentication Protocol) communication process between a selected client and the access point it is attempting to associate and authenticate with. This test can help you troubleshoot problems that a device is having with connecting to the WLAN.

Signal Strength

The **Signal Strength** test measures signal strength and noise for the selected device.

Tap the graph to view signal strength and noise data for a particular time period.

The graph is continuously updated according to the interval specified in the **Update every** box. You can change the sampling period by selecting a different time interval from this box.

WLAN Statistics

The **WLAN Statistics**test enables you to view data for the traffic to and from the selected device. The following packet types are analyzed and results are shown in tabular and graphic form:

- Broadcast
- Cross Talk

- Unicast
- Retries
- Errors

You can change the sampling period by selecting a time interval from the **Update every** box.

You can look at Tx packets, Rx packets, or both by selecting one of the option buttons.

Tx/Rx Rate

The **Tx/Rx Rate** test shows you the number of packets that the selected device is sending and receiving at various transmission rates.

The information is presented in tabular form and is continuously updated according to the interval specified in the **Update every** box. You can change the sampling period by selecting a different time interval from this box.

Accessing the Instrument Remotely (LAN only)

You can control EtherScope Network Assistant and view its result screens from a remote location. The instrument contains a Virtual Network Connection (VNC) server that is used for remote access.

To access the remote user interface:

1. Start Internet Explorer.

Note

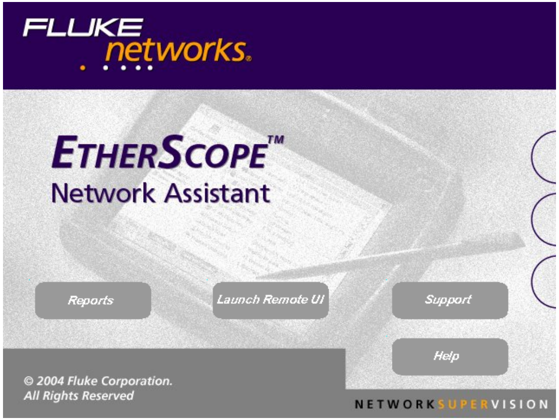
EtherScope Network Assistant supports Internet Explorer only.

2. In the **Address** field, enter the IP address of the EtherScope Network Assistant that you want to connect to.

Note

The instrument's IP address is located in the preview pane for the ***Test Results*** *screen when the* ***Connection*** *test is highlighted.*

The **EtherScope™ Network Assistant** web server home page (Figure 32) is displayed.



avs56s.bmp

Figure 32. Web Server Home Page

From this screen, you can do the following:

- Remotely access the instrument.

  Note

  The remote instrument can be accessed by multiple users, but can be controlled by only one user at a time.

- Access reports saved on the CompactFlash memory card or real-time reports in the instrument's active test results memory.
- Initiate a support incident at the Fluke Networks website.
- Access the Help screens.

3. To remotely access the instrument:

   a) Click Launch Remote UI.

   b) Use the keyboard to type the Remote Authentication password. Then, click OK.

   Note

   The instrument's default factory setting requires no password. Therefore, clicking OK with no entry in the password filed displays the Test Results screen. However, for security reasons, you can set a password to restrict usage to authorized users only. See "Instrument Security Settings" on page 79 for instructions.

   The remote instrument's **Test Results** screen is displayed. You are now connected and can control the instrument remotely.

4. To access real-time reports:

   a) Click Reports.

      The **EtherScope Real-Time Reports** screen is displayed.

   b) Locate the report that you want to view, and then click a link to display it.

5. To access saved reports:

   a) Click Reports.

      The **EtherScope Real-Time Reports** screen is displayed.

   b) Click **View Saved Reports**.

   c) Select the saved report that you want to view, and then follow the link to view it.

User Interface Events that will Terminate a Remote Session

The active TCP/IP session between the remote user interface software and the instrument can be severed under the following conditions:

- If IP parameters are manually changed on the instrument and Apply is selected on the **Instrument Settings—TCP/IP** screen

- If the **Start Test** button is selected on the **Cable Verification** Details screen.

- If the **Start Test** button is selected on the **Signal Verification** Details screen.

- If the instrument's MAC address is changed in the **Instrument Settings—Ethernet** screen.

- If the Ethernet link goes down.

Using the Desktop Tools

EtherScope Network Assistant is packaged with a number of tools to increase your productivity. The tools are listed in this section along with a brief description of their function.

Applications Menu

The following tools are on the **Applications** menu. To display this menu, tap then select **Applications**.

- **Calculator**: performs basic arithmetic operations, such as addition and subtraction.
- **Calendar**: provides weekly and monthly views for scheduling events; a Notes function enables you to add information about an event.
- **Clock**: displays the time currently set on the instrument; includes a stop watch and alarm function. To change the time, see "Setting the Time and Date" on page 16.
- **EtherScope Console**: provides a command line interface and terminal emulation (Telnet).
- **EtherScope Network Assistant**: displays the top-level user interface screen (**Test Results)**.
- **File Manager**: displays the contents of the CompactFlash memory card where reports are stored.

- **Report Viewer**: displays a saved report.
- **System Info**: displays resource usage (memory, CPU, and storage) and version information of the Linux operating system.
- **Web Browser**: displays EtherScope Network Assistant's web browser, Konqueror. You can use the browser to view and change the configuration of switches and other network devices.

Tools Menu

You can access the following tools from the **Tools** menu. To display the menu, tap (located on the toolbar).

- **Web Browser**: enables you to connect to a device so that you can check or change its configurations. To connect, select the desired device, and then select **Web Browser**. EtherScope Network Assistant's web browser, Konquerer, attempts to connect to the device.
- **Telnet**: lets you access a remote computer so that you can check or change its configurations. When you run this program, EtherScope Network Assistant acts as if it is a terminal connected to the remote device.
- **Terminal**: lets you use EtherScope Network Assistant as an ASCII terminal. You can tap ⌨ to display the virtual keyboard or you can use a remote keyboard to enter commands.
- **FTP**: starts an FTP (File Transfer Protocol) session with a device. Use this utility to transfer files between computers. To start a session, select a device, then select **FTP**.

- **Port Reporter**: a command-line utility that uses the Cisco Discovery Protocol (CDP) to discover switches and switch details. You can use this utility in a Cisco environment to quickly discover and display information about a switch.
- **TFTP**: stands for Trivial File Transfer Protocol, a data transfer utility that enables you to do firmware updates on switches that support its use.
- **SSH Telnet**: stands for Secure Shell Telnet, a more secure version of Telnet. To provide security, SSH Telnet requires login credentials. It also encrypts the data sent between the logical and remote device.
- **Report**: displays reports on the CompactFlash memory card. You can create a new report or delete a report.

Troubleshooting Your Instrument

This section lists some problems you might experience with your EtherScope Network Assistant and provides suggestions to help you solve them. Before calling technical support, try these suggestions to see if you can solve the problem on your own.

Problem: The instrument or the application is not responding.

Suggestion: If you suspect that the application environment or the instrument (hardware) has locked up, you may have to completely shut down the instrument. To do this, press and hold the **On/Off** button for approximately six seconds.

Problem: The instrument does not power on.

Suggestion: Connect the instrument to the AC adapter. If the instrument powers on only when connected to the AC adapter, the internal battery may be completely discharged. Recharge the battery.

Problem: The user interface does not appear.

Suggestion: The **Test Results** screen should be displayed after you turn on the instrument.

If the screen does not display, press and hold the **On/Off** button for six seconds to completely shut down the instrument. Then, press the **On/Off** button again to power the instrument back on.

Problem: The IP Discovery and/or Tools results screens are not displaying the expected results.

Suggestion: Check the following:

- Does the instrument have a valid IP address? Select **Connection** on the **Test Results** screen to see if the instrument is configured with a valid IP address.

- Verify that the DHCP capability on the **Instrument Settings—TCP/IP** screen is not disabled. If an IP address is entered manually, it must not be an address within the local subnet.

Problem: The touch-sensitive screen responds slowly or erratically to the stylus.

Suggestion: Try navigating around the display to determine whether the touch-screen requires calibration (this is rare). If you suspect a problem with the calibation, see “Recalibrating the Screen” on page 18.

Problem: The instrument does not connect to the network.

Suggestion: The **Link** LED lights solid green (or amber in WLAN mode) if a link exists. In addtion, you should see some activity on **Transmit** and/or **Utilization** LEDs. If the LEDs indicate no activity on the link, do the following:

- Check the **Connection** test results on the **Test Results** screen. Select **Connection** and then check to see that an IP address for the connection is displayed in the preview pane.
- (LAN mode only) Confirm that the **Cable Verification** test passed. Try a different cable, if necessary. From the **Test Results** screen, tap ⊞ to expand the **Connection** test group and then select **Cable Verification**. Check the status and the test results information in the preview pane.
- (WLAN mode) Examine the Connection Log to try to determine the cause of a failed WLAN network connection.

Problem: The instrument cannot connect to the network.

Suggestion: A network connection cannot be made if the **Cable Verification** test (LAN only) does not pass.

Check status of the **Connection** test on the **Test Results** screen. Information in the **Status** column shows you whether or not a cable is detected. Do the following:

1. Tap ⊞ to expand the **Connection** test group.
2. Select **Cable Verification** and check the results of the test.

   If the test fails, this icon is displayed: 🚫.
3. Tap Details to view detailed results to see if you can determine what is causing the problem.
4. To retest the cable, tap Start Test.

Problem:

- The battery charge state appears erratic or inconsistent.
- The battery does not hold a normal charge.

Suggestion: Charge the battery pack for at least seven hours.

Problem: The touch-sensitive screen does not respond at all to input.

Suggestion: Press the **On/Off** button to place the instrument in suspend mode. Press the **On/Off** button again to take the instrument out of this mode.

If the problem continues, press and hold the **On/Off** button for six seconds to completely shut down the instrument. Press the **On/Off** button again to power the instrument back on.

Specifications

Weight	0.82 kilograms (2 lbs)
Dimensions	19.1 x 15.2 x 4.4 centimeters, (7.5 x 6 x 1.75 inches)
LCD touch screen display	640 x 480 pixels, TFT (active) color panel, active area 129.6 (H) mm x 97.4 (V) mm
LED indicators (mainframe)	6
Battery	Lithium Ion 7.2 V DC (nominal), 4.2 Ah
Battery life	Wired LAN mode: approximately 4 hours; Fiber Mode: approximately 3.5 hours; WLAN mode: approximately 3.5 hours
External AC adapter/battery charger	AC input: 120 V – 240 V, 50/60 Hz, 1.5 A; DC output: 15 V, 3.3 A
Communication and accessory ports	One USB, one PCMCIA /Cardbus (PC Card type II), one CompactFlash memory card (Card Type I/II), one DB-9 serial, headphone jack

Specifications (continued)

Network analysis ports	RJ-45 10/100/1000 BASE-T Ethernet (EtherScope2 LAN/Pro), 1000BASE-SX/LX/ZX Fiber (ES2-LAN-SX, ES2-LAN-SX-I, ES2 Pro-SXLX-I/S), PCMCIA/Cardbus 802.11a/b/g Wireless (EtherScope WLAN/Pro)
Vibration	Meets requirements of MIL-PRF-28800F for Class 2 random vibration
Laser	⚠ Class 1 Laser Product. Complies with 21 CFR Subchapter J and EN 60825-1/01
Environmental	Operating temperature: 0° C – 40° C with 95 % relative humidity Non-Operating (storage) temperature: – 20° C to + 60° C CE Electromagnetic Interference complies to EN61326, Class A. Criteria C ⊘ The product network interfaces are NOT FOR CONNECTION TO PUBLIC TELEPHONE SYSTEMS and should only be connected to the public phone network through regulatory agency compliant modem devices
EtherScope Certifications and Approvals	CSA Canada & United States, CE, FCC Part 15 Class A, C-TICK N10140; UL and CSA approvals for universal AC adapter
WLAN Adapter Certifications and Approvals	FCC Part 15 (USA); Telec (Japan); ETSI, EN301893, EN60950 (Europe); C-TICK N10140 (Australia)

Cable Types

- Unshielded Twisted Pair LAN cables (100 UTP category 3, 4, 5, 5E, and 6 ISO/IEC Class C and D)
- Foil-screened Twisted Pair cables (100 and 120 Ohm ScTP category 3, 4, 5, and 6 ISO/IEC Class C and D)
- Identifies and operates with the optional fiber adapter, LX (1310nm, -3 dBm (0.50 mW max)), SX (850nm, -2 dBm (0.63 mW max)), and ZX (1550nm, +4 dBm (2.5 mW max)).

Cable Length

Note

*Length accuracy depends on the cable type selected on the **Cable Verification** screen.*

Open, shorted or with wiremap adapter	1 to 305 m (3 ft. to 1000 ft.)
Terminated with ≥ 20 % reflection	1 to 305 m (3 ft. to 1000 ft.)

Receive Level

100 to 5000mVp-p

Datalink Signal

500mVp-p to 4000mVp-p

Measuring Terminated Cables

Cable Verification tests individual twisted-pairs of a cable that are terminated into most equipment vendors' Ethernet ports, such as on a hub, switch or NIC.

All cable tests other than WireView wiremap and office locator ID are operational in the presence of datalink signal.

Fault Tolerance

The RJ-45 10/100/1000 BASE-T Ethernet connection on the instrument is designed to withstand a maximum of 100 volts.

WireView Wiremap Adapter/Office Locator Compatibility

Detects combinations of shorts, opens, and connector miswires. Compatible with Fluke Networks WireView wiremap adapter/office locator.

Index