





# 1 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 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. Some information about your network is discovered without any instrument configuration, however, to use all of the features of the instrument it is necessary to configure it. Refer to the topic [Configure the Network Assistant](#) for more information.

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





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

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






# 2 Navigating the User Interface

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

Here are some tips for navigating the user interface:

- All blue text represents a hyperlink to a separate, related screen within the user interface.
- Tap the EtherScope icon  , located on the left side of the Title bar, for a drop-down list of tests. Select a test to go directly to that screen. You can also select a test from the **Test Results** screen.
- Select one of the Operations buttons (e.g. **Details**, **Report** ) located on the Task bar at the bottom of the screen to perform tasks specific to a test. Operations buttons are disabled when they are not applicable to a test.
- Tap **Connection** on the **Test Results** screen and select the **Details** button to navigate to the **LAN Instrument Settings** screen, or tap the EtherScope icon  in the top left corner and tap **Instrument Settings**.
- Tap a column heading to sort data by that value.
- Tap the  icon in a list to expand and view more tests or details. Tap the  icon to collapse the

expanded list.

- Tap the **Keyboard** icon  , located on the status bar at the bottom of the screen, to bring up the keyboard and tap the icon again to put it away. The keyboard allows both text and numeric entry.
- Tap the **Back** icon  to return to the previous screen.
- Tap the **Home** icon  to return to the **Test Results** (default) screen.
- Tap the **Tools** icon  for a drop-down list of network troubleshooting tools.
- To assist in finding a specific device in a list, use the **Find** button located on the Title bar at the top of the screen. Enter a partial or full name or address in the entry box and select **Find** to initiate the search.
- Tap the  icon for screen level help.
- To switch between **LAN** and **WLAN** tests, tap the **WLAN Tests** or **LAN Tests** button on the Task bar. The appropriate option must be installed in order to switch between the tests. You can check the installed options on the [Instrument Settings - Options](#) screen. Any data that has been collected will be lost when you switch.

### 3 Configure the Network Assistant

The EtherScope instrument begins a series of automated tests when it is turned on and plugged into your network.





#### Network Test

Plug one end of an Ethernet cable into the instrument's RJ-45 LAN connector (or a gigabit fiber cable into the 1000BASE-X) and the other end into your network.

**Note:** The instrument supports 10/100/1000 IEEE 802.3 (10BaseT, 100BaseTX, and 1000BaseT) on the RJ-45 interface and if the [Fiber Option](#) is enabled, the SFP interface supports 1000BaseSX, 1000BaseLX, and 1000BaseZX fiber.

Press the green power button to turn on the instrument (this can be done before or after connecting the network cable). In most cases, the EtherScope application will automatically configure the LAN instrument settings and start and display the **Test Results** (auto test) screen. Refer to the [Instrument Settings](#) topic for more information on configuring the instrument. The instrument will automatically verify cable characteristics, test the signal quality, and establish connectivity at the physical layer. By default, the instrument will auto-negotiate to the highest speed and duplex allowed by the link partner.

**Note:** If the [Fiber Option](#) is enabled on your instrument and both cable types are connected, the instrument will use the fiber interface on startup or when tests are restarted. If one interface is already active, inserting the other connection will have no effect. In order to switch interfaces, the active interface must be disconnected and the new cable inserted. This will cause the instrument to reset itself and restart testing. To conserve battery power, the fiber interface is powered off when not in use.

The **Link** LED at the top of the instrument will show solid green when link is established. The Link Button  , found on the left side of the Task bar at the bottom of the screen, indicates the cable type (Ethernet  or Fiber  ), the duplex mode and link speed. Two solid arrows indicate a full duplex connection. One solid and one outlined arrow  represents a

half duplex connection. Tap the Link button to check or modify the instrument's Ethernet settings on the [Instrument Settings - Ethernet](#) screen.

The various network tests performed by the Network Assistant are described under the **Tests** category in the Table of Contents.

#### Cable Test

See the [Connection](#) test topic for information on testing network cables.

## 4 Using the Network Assistant

The Network Assistant begins a series of automated tests simply by turning the instrument on and connecting a network cable. Insert an Ethernet cable into the LAN port found at the top left of the product (or, if the [option](#) is enabled, a gigabit fiber cable into the 1000BASE-X port) and the other end into your network. Power the instrument on and the Ethernet Network Assistant application automatically loads and runs.

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


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


The instrument automatically verifies the network cable characteristics, tests the signal quality, and establishes connectivity at the physical layer. The instrument will auto-negotiate to the highest speed and duplex allowed by the link partner. See [Configuring the Network Assistant](#) for information on how to force the instrument to link at a specific speed and duplex mode. Once link is established, the instrument begins monitoring the network interface for Utilization, Protocols, and Problems. By default, the instrument monitors the local network segment. You can also use the instrument to monitor remote device interfaces. See [Troubleshooting in a Switched Environment](#) for information on how to configure the instrument to monitor remote network devices and segments.

**Note:** If 802.1Q (VLAN tagging) is misconfigured on the instrument, DHCP will fail and active discovery will not work. Refer to the [802.1Q/IP TOS](#) for more configuration information.

The instrument attempts to become an active device on the network by obtaining an IP address and then begins a sequence of tests that discovers network devices, services, and VLANs. By default, the instrument will attempt to use DHCP to obtain an IP address and other network information. See [Configuring the Network Assistant](#) if your network requires the use of fixed IP addresses or to change other network configuration data. The instrument queries each device it discovers to learn more about the device's capabilities and possible problems. Default community strings are used to query network devices. To obtain the best results, the instrument needs to be configured with the SNMP community strings being used on your network. See [Configuring the Network Assistant](#) for more information on adding additional community strings.


As the automated tests are running, the instrument provides information about the status of each test and indicates the success or failure of a particular test. Using the stylus, tap any test to display a synopsis of the test results in the left panel of the screen. Tap the **Details** button to view more information about the selected test.

All blue text represents a hyperlink to a separate, related screen within the UI. Your Network Assistant instrument provides a set of tools commonly used in the network maintenance and troubleshooting process. Tap the **Tools** icon  located in the lower right of a screen for a list of tools available with the product. When troubleshooting a specific device, a relevant set of these tools is available directly

on the **Device Detail** screen. On most screens a **Report** button is available that will generate a report based on the information that has been discovered. Tapping the **Home**  icon will return you to the main **Test Results** screen.

## 5 Instrument Settings

The instrument is designed to provide as much automated configuration as possible, however, every network is different. You may need to manually change some of the configuration settings to optimize the performance for your network.

The [Connection](#) test result reports the configuration and link status of the instrument. When the **Connection** test is highlighted, tap the **Details** button to display the **Instrument Settings** screen, where you can view and modify the current instrument settings. The **Instrument Settings** screen is also directly accessible from the EtherScope application icon  located in the title bar at the top of the display.

The **TCP/IP** screen is the default. Tap one of the hyperlinks found on the left pane of the preview screen to view or change other instrument settings.

[TCP/IP Settings](#)

[802.1Q/IP TOS](#)

[802.1X Security](#)

[Active Tests](#)

[SNMP](#)

[Connection Log](#)



[Ethernet Settings](#)

[Instrument Security](#)


[General Settings](#)

[Options](#)

[Version](#)

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

### 5.1 TCP/IP Settings

By default, the instrument will use DHCP (Dynamic Host Configuration Protocol) to set its TCP/IP configuration. The **Instrument Settings - TCP/IP** screen will display the address that the instrument was able to obtain (the results are also shown on the preview pane of the **Test Results** screen). To use a static IP address or to change the subnet mask, tap the **Automatically configure TCP/IP settings** checkbox to disable auto-configuration of the IP address. Select the field that you wish to change, select the Keyboard icon  (or use the pull-down list) and enter an **IP address** or **Subnet**



**mask** as appropriate. You can use the pull-down list or keyboard to change the **Default router**, **Primary DNS**, or **Secondary DNS**. Tap the **IP** icon next to an address field to edit the address shown in the field.

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

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

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

**Note:** An instrument that is connected directly to a switch may experience up to a 40 second autoconfiguration delay.

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

## 5.2 802.1Q/IP TOS

The **Instrument Settings - 802.1Q/IP TOS** screen allows you to configure your instrument for tagged VLAN (802.1Q) and IP Type of Service operation.

### 802.1Q Settings

Tap the **Enable 802.1Q** checkbox to turn on VLAN tagging for the instrument. Use the **VLAN ID** field to designate the VLAN number that the instrument will use. Use the **Priority** field to set the user priority for frames generated by the instrument.

**Note:** If you select a **VLAN ID** that is unconfigured on the port to which the instrument is connected, the instrument might not be able to communicate on the network. DHCP will fail and active discovery will not work. You will see the same result if you enable 802.1Q and the instrument is not plugged in to an 802.1Q enabled port. If this happens, you can use [VLAN Statistics](#) to identify the VLANs that are active on the port. Try configuring the 802.1Q settings with the VLAN that has the highest packet count.

Frames belonging to the native VLAN are not modified when sent over the trunk.

### TOS (Type of Service)

You can select between:

- **TOS with IP Precedence** - Use the pull-down menu to set the property (**Delay**, **Throughput**, **Reliability**, or **Cost**) that you wish to prioritize and then set the **IP Precedence**. Select **Normal** (default setting) if you do not wish to select a property.
- **DSCP** - Set the DSCP (Differentiated Services Code Point) parameter.

Tap the **Apply** button when you are finished. The instrument restarts its tests with the new configuration.

## 5.3 802.1X Security

You can use the **Instrument Settings - 802.1X** screen to configure your EtherScope instrument for 802.1X security, which allows the instrument to establish connection with an 802.1X configured secure switch.

If 802.1X security is configured, then as part of the network link process, the instrument will try to authenticate with the port to which it is connected. The **802.1X** line on the **Test Results | Connection** preview screen indicates the configuration and authentication status of the instrument.

You can configure 802.1X security by selecting **Instrument Settings | 802.1X**.

**Note:** If 802.1X password security is turned on in [Instrument Security](#), then you will be prompted to enter the instrument password before you can view or change the 802.1X instrument settings.

On the **Instrument Settings - 802.1X** screen, you can configure the instrument (**EAP Type**, **Username**, and **Password**) to match the configuration of the switch port to which the instrument is trying to authenticate. Tap the **Apply** button to save the settings. The instrument will use the saved settings to authenticate each time it establishes link. If link has already been established, you can restart the link process by removing and reinserting the network cable to the instrument, tapping the **Restart All** button on the **Test Results** screen, or cycling power.

**Note:** If 802.1X security is configured, the instrument will try to authenticate to the port to which it links, regardless of whether the port is 802.1X enabled or not. The **802.1X** line on the **Test Results | Connection** preview screen will indicate a status of **OK (unneeded)** if 802.1X security is not configured on the port. You can turn off 802.1X security on the instrument by selecting **None** in the **EAP Type** field of the **Instrument Settings - 802.1X** screen and then tap the **Apply** button.

If the instrument fails to authenticate to a configured port, the **Connection** status on the **Test Results** screen will indicate a successful link and the preview screen will indicate **Failure** on the **802.1X** line. The Cable Verification test is the only test that will run successfully.

**Note:** The security status of a port is shown on the **Interface Detail** screen of [Device Details](#).

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

## 5.4 Active Tests

The **Instrument Settings - Active Tests** screen allows you to select which tests are run. By default, all tests are enabled. If you want to disable a test, uncheck the box next to it in the list. Select the **Apply** button to save your changes. The instrument will reboot to make the changes take affect. Any tests that are disabled will not appear on the **Test Results** screen.

**Note:** If you disable a test that has tests underneath it in the tree structure (e.g. **Local Statistics**), then the tests underneath it will also be disabled.

## 5.5 SNMP

The instrument queries SNMP agents to discover detailed information about your network configuration. The instrument supports SNMP v1/v2 and SNMP v3. SNMP v3 uses credential sets instead of community strings. You can configure SNMP information on the **Instrument Settings - SNMP** screen.

**Note:** Password control is implemented on the [Instrument Settings - Instrument Security](#) screen. If you

cannot access the **Instrument Settings - SNMP** screen, enter the instrument password on the **Instrument Settings - Instrument Security** screen.

### Configuring SNMP v1 and SNMP v2 Community Strings

The instrument uses the default community strings of **public**, **private**, and **security**. Enter SNMPv1 and SNMPv2 community strings in the space provided. Tap the **Apply** button to save your changes.

**Note:** The discovery process successively tries the community strings in the order in which they are listed. List the strings in order of frequency of use for a quicker discovery.

### Configuring SNMP v3

1. Tap the **Add** button to create a new credential set.
2. Select the credential set that you wish to change in the **SNMP v3 settings** window.
3. In the **Edit Credential Set** window you can set the following parameters:

**Set:** A name that you assign to this set of access credentials.

**Username:** The username for the SNMP v3 credential that is used in communicating with the device. It can be up to 32 characters.

**Authentication Protocol:** This can be **None**, **HMAC-SHA**, or **HMAC-MD5**. If you select HMAC-SHA or HMAC-MD5, you must enter an **Authentication Password**.

**Privacy Protocol:** When authentication has been configured, **CBC-DES** encryption may also be selected to protect the SNMP data. If you select CBC-DES, you must enter a **Protocol Password**.

After you have made your changes, select **Apply** to update the community strings or credential set profile.

## 5.6 Connection Log

The **Instrument Settings - Connection Log** screen shows the sequence of network events that occur as the instrument establishes connection to the network. DHCP (Dynamic Host Configuration Protocol), ITO (Internet Throughput Option), and 802.1X security events are logged. The log can be used to troubleshoot and verify network configuration.

The log shows which DHCP servers respond to a Discover request and which offers are ignored. This can be useful for identifying rogue servers. The log also shows the [802.1X security](#) authentication process and indicates its success or failure.


The log sequence starts at time 0.00 seconds and each event is time-stamped relative to the first event. The first part of each listing indicates the type of action or event, followed by information about the response to the event. The log is a static display of the events that have occurred up to the point that the menu selection is made; you have to exit the screen and reenter it to update the log. You can use the [Report](#) button on the task bar to save the log to the CompactFlash.


**Note:** The Connection Log will be empty if the **Automatically configure TCP/IP settings** checkbox on the [Instrument Settings - TCP/IP](#) screen is not enabled.

## 5.7 Ethernet Settings

In the event that you need to override the instrument's link auto-negotiation settings, tap the **Ethernet** hyperlink to open the **Instrument Settings - Ethernet** screen. You can select between two options:



**Use Auto-Negotiation** - Select the speeds and duplex that you wish the instrument to advertise during auto-negotiation. The instrument will use the highest selected speed/duplex that can be negotiated with the link partner. The link button  on the Tool bar indicates the negotiated link speed and duplex. Two solid arrows indicate a full duplex connection. One solid and one outlined arrow represent a half duplex connection. Tap the button to check or modify the instrument's Ethernet settings on the **Instrument Settings - Ethernet** screen.

**Use Forced Setting** - Select the speed and duplex that you wish the instrument to use. The instrument will use the selected setting and try to establish link. However, if the link partner does not support the selected setting, link will not be established. If link is established the link button  on the Title bar will have an \* next to the link speed, indicating that it is a forced setting.

**Note:** The [Signal Verification](#) test does a complete link auto-negotiation as part of the test regardless of the configuration settings.

A factory assigned MAC address is provided. You can change the MAC address to enable testing of switch forwarding tables or ARP caches as part of the troubleshooting process. Tap the **MAC address** field and use the keyboard to enter a new MAC. Select **Save MAC address** to change the MAC to the one you entered. Select **Restore factory MAC** to change the setting back to the factory default.

Select the **Apply** button to save any changes. If you do not select the **Apply** button before you exit the **Instrument Settings - Ethernet** screen then all changes will be lost.

**Note:** Selecting the **Apply** button disconnects the instrument from the network, stopping all tests that are currently running, and reconnects the instrument to the network with the new settings.

**Note:** If the active interface is the 1000BASE-X (gigabit fiber), then the **Auto-Negotiation** and **Use Forced Setting** options are not available.

## 5.8 Instrument Security

You can manage the SNMP community strings that are used by the instrument to query devices. You can also set or change a password for controlled access to the remote user interface and also to the SNMP community strings. Tap the **Security** hyperlink to open the **Instrument Settings – Security** screen.

### Password Control

Setting a password limits access through the remote user interface and access to view/change SNMP Community strings. To establish a password, tap **Create Password...** and enter a password in the **New password** field. Re-enter the password in the **Confirm password** field and tap **OK**. To change an existing password, enter the password and tap **Change password...**. Enter a new password and then re-enter it to confirm. Cycle power to the instrument to make the change take effect.

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

**Note:** You must create a password to enable the **Password Required** fields on this screen.

### Clearing a Password

To clear a password, you must enter the existing password. Press the **Change Password** button. In the new password entry field, enter nothing in either field of the **Change Password** dialog box and tap **OK**. Tap **OK** a second time on the warning popup. Cycle power to the instrument to make the change take effect.



### Remote User Interface

Use the checkbox to enable [Remote Access](#) to the instrument through the Internet Explorer web browser. Enable the **Password required** checkbox if you want to control access to the instrument. Anyone accessing the Remote User Interface will be required to enter the password before continuing. These check boxes are not enabled until a password has been established for the instrument.

### Performance Tests

- **Password required to run RFC2544/ITO tests** - If this check box is enabled, the password must be entered before the tests can be run.
- **Restrict test modifications** - If this check box is enabled, the password must be entered before the user can make any configuration changes or save a test script in the **Performance Tests**. Previously saved test scripts can be loaded and tests can be run without the password.

### Configuring SNMP Community Strings

The instrument queries SNMP agents to discover detailed information about your network configuration. You can configure SNMP Community strings on the [Instrument Settings - SNMP](#) screen. Enable the **Password required** check box if you want to hide the community strings and to control the editing of them. You will not be able to access the **Instrument Settings - SNMP** screen if this check box is enabled and the password is not entered.

### 802.1X Security Settings

Enable the **Password required** check box to control access to the [802.1X security](#) settings.

## 5.9 General Settings

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

- **Restore Defaults** - restores the instrument to factory settings. Discovery database and some user configured parameters (e.g. SNMP Community Strings) are reset.
- **Edit user-defined devices** - Allows you to edit or delete existing user-defined devices or [add a new device](#) to the list. You may want to add a device that is either outside of the local broadcast domain where the instrument resides, or add a device that is on the local broadcast domain that is not being discovered.
- **Remote RFC 2544/ITO Throughput Testing** - Enable the check box to allow the Network Assistant to be used as the remote unit in [RFC 2544](#) or [Throughput](#) testing. The instrument can be used in conjunction with another EtherScope Network Assistant, Fluke Networks OptiView Analyzer, or Fluke Network OneTouch Network Assistant to test the network throughput. The **Port** entry must match the **Port** setting of the other instrument involved in the test (Port 3842 is the default for ITO tests, Port 7 is the default for RFC 2544 tests). The **Timeout** period determines the length of time that the instrument will wait for a response from the other test unit before terminating the test. Tap the **Save** button to save your changes.

**Note:** The **Timeout** parameter set on the remote unit is independent of the timeout set on the local unit.

**Note:** **Remote Throughput Testing** does not have to be enabled in order for your instrument to

initiate an RFC 2544 or Throughput test (i.e. to be the local unit).

**Note:** The Upstream Frame per Second (FPS) on a OneTouch Network Assistant must be set to 1 or greater in order to work with the EtherScope Network Assistant.

- **Show vendor prefix with MAC address** - You can control how a device's MAC address is shown - either in raw hexadecimal format (e.g. 00c017c0000c) or with a vendor prefix (e.g. FLUKE-c0000c).
- **Enable paced discovery** - Some switches will shut down the port if the switch detects a Denial of Service (DoS) attack. The initial stages of discovery algorithm used by the EtherScope instrument generates a significant number of ARP requests and responses. This can cause the switch to shut down the port to which the instrument is connected. Turn on the **Enable paced discovery** feature to avoid this. When enabled, the instrument will not issue Broadcast packets and slows down its PING and ARP requests. The effect of this is that it will take longer to completely discover your network.
- **Enable fast connect mode** - Allows for a faster response time when you are repeatedly connecting the instrument to different networks. For example, select this mode when you are verifying the connectivity of multiple office cubicles in a new installation.

Normally, when the instrument is first plugged into a network, it tries to determine whether it is connected to the same broadcast domain as it was previously. If it is, it saves the data it had previously collected. If it is not connected to the same broadcast domain, it resets its discovery database and discovers the network to which it is connected. In fast connect mode, the instrument automatically resets its discovery database. This action can save time when you are quickly trying to determine connectivity for multiple network ports.

The discovery algorithm does not change for either configuration.

- **SNMP System Name** - You can specify the SNMP name for the instrument. The default name is **EtherScope-xxxxxx**, where xxxxxx is the last 6 digits of the instrument's MAC address.

## 5.10 Options

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

The available options are:

- **LAN Option (ES\_LAN\_OPT)** - enables you to monitor and test IEEE 802.3 Ethernet 10/100/1000 networks
- **WLAN Option (ES\_WLAN\_OPT)** - enables you to monitor and test IEEE 802.11 a/b/g wireless networks
- **Internet Throughput/Traffic Generation (ES\_ITO\_OPT)** - enables you to test network throughput and generate test traffic on your IEEE 802.3 network
- **Fiber Option (ES\_FIBER\_OPT)** - enables the 1000BASE-X gigabit fiber interface

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

## 5.11 Version

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

## 6 Status LEDs

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

- **Link**
- **Utilization**
- **Collision**
- **Error**
- **Transmit**

The LEDs represent the following conditions:

### Link

- **Green Solid** - a signal (NLP, FLP, or Data) has been detected on the cable
- **Off** - no cable or no link present

### Utilization

Represents traffic relative to the network segment where the instrument is connected (local traffic).

- **Green Blinking** = 0% to 50%
- **Yellow Blinking** = 51% to 89%
- **Red Blinking** = 90% to 100%

### Collision

- **Yellow Blinking** - collisions have been detected by the instrument on the local network. The more collisions that occur, the faster the light blinks.

### Error

- **Red Blinking** - errors have been detected on the local network segment.

The following errors are detected:

- **Undersized Packet** - a packet that is less than 64 bytes.
- **Oversized Packet** - a packet that is greater than 1518 bytes with a valid checksum.
- **Bad FCS** - a packet that has an invalid checksum.
- **Jabber** - a packet that is greater than 1518 bytes with an invalid checksum. In general, you should not see jabbers.
- **Ghost** - energy on the cable that appears to be a frame, but has an invalid start-frame delimiter. The ghost frame must be at least 64 bytes long.

The most likely causes of these errors are a faulty NIC and/or faulty or corrupt NIC driver files, bad cabling, or grounding problems.


### Transmit

- **Green** – the instrument is transmitting packets. Utilization is between 0 - 50%.
- **Amber** - utilization is between 50 - 90%.
- **Red** - utilization is greater than 90%.

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

- **Green Blinking** - (on EtherScope Series II instruments) indicates that the unit is powered off but AC power is applied and the battery is being charged.
- **Green** - the instrument is in full power mode, by either battery or AC power.
- **Amber** - the instrument is in [Suspend](#) mode

## 7 Desktop Settings

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

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

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

### 7.1 Language Support

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



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

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

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


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

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

2. Tap the Desktop  icon, located on the left side of the status bar, and select **Settings**.
3. Select the Language  icon.
4. You will see a popup advising you that there is a newer file available. Select **Yes** to copy the language file to the instrument. After the file is copied, the list of available languages is shown in the **Language** dialog window.
5. Select the language which you wish to use to view the user interface and help.
6. Select **OK** to close the dialog.
7. You must power cycle the instrument in order for the changes to take effect.

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

## 7.2 Touch Screen Recalibration

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

## 7.3 Battery Management

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

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


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

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

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

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

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

- Press the green power button until the power button LED turns amber (about 2 seconds), and then release.
- Tap the Desktop icon  icon, located on the left side of the status bar, and select **Suspend**.


- Use the [Light and Power](#) settings to configure the instrument to automatically enter suspend mode after a certain amount of inactivity.






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

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





## 8 Desktop Applications

The instrument includes several convenient applications in addition to the EtherScope Network

Assistant. To access these applications, tap the Desktop icon  found on the left side of the Status bar and select **Applications**. The **Applications** tab includes several tools, including a **Calculator**, **Calendar**, **Clock**, **EtherScope Console**, **File Manager**, **Report Viewer**, and [Web Browser](#).

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

The **EtherScope Console** application provides a user interface for the [Terminal](#), [Ping](#) and [Trace Route](#) tools.

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

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

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

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

### 8.1 Server Response Tool

The **Server Response Tool** is available from the **Desktop Applications** screen and provides two applications (select **Tools** on the menu bar) that allows you to test key application server connectivity and responsiveness:

#### Server Response Test

You can use the Server Response Test to verify the connection and response of server/port pairs. You can define, save and test up to 100 server/port pairs.

To add a new server port to the test:

1. Select **Edit | New Server** on the menu bar.
2. Enter the server name (use the DNS name, e.g. www.flukenetworks.com) or IP address in the **Name** field (use dotted-decimal format, e.g. 129.196.231.98). If you enter a valid DNS name, the application will resolve the IP address. If you enter the IP address, it will be also be used for the server name.
3. Select the check box next to each service that you wish to test. If the service uses a non-standard port or you wish to test a port that is not listed, use the **Custom** field(s) to add one or more ports to the list. You can either enter just the port number and it will be used as the **Service** name and **Port** number, or enter a name and then later enter the port number.
4. Select **OK** when done.
5. The new server will appear in the list.
6. If you did not enter a port number when adding the server, select **Edit | Change Port**.
7. The **Change Service** popup appears.
8. In the **Service(port)** field enter the desired port number in the parentheses. For example, if you entered *newname* in the **Custom** field, *newname (---)* will appear. Replace the --- with the desired port number and select **OK**.

Begin the test by selecting the **Start Test** button (it can be interrupted by selecting the **Stop Test** button). For each entry in the server list, a TCP SYN packet is sent to the specified endpoint. If the server responds with a TCP SYN|ACK, a service is available at that server/port endpoint and an open folder (📁) is displayed in the **Service Available** column to indicate the endpoint is available. If the server responds with a TCP RST, no service is available at the specified endpoint and a 🚫 icon is shown. If neither of these responses is received, no icon is displayed. The average round trip time that measures the mean packet response time for all request/replies used (including DNS) is displayed in the **Avg RTT** column. An \* appended to **Avg RTT** value means one or more accesses to the server/port pair did not succeed. If a SYN/ACK or RST is not received, the text **unreachable** is shown.

### TCP Trace Route

The **TCP Trace Route** tool shows the number of hops and IP path between the EtherScope Network Assistant and a server/port endpoint defined in the **Server Response Test**. Select the endpoint from the list in the **Server Response Test**, then select **Tools | TCP Trace Route** from the **Tools** menu. Select the **Start Test** button to begin.

When the **Start Test** button is selected, a TCP SYN packet with a time-to-live (TTL) of 1 is sent to the default gateway (if the endpoint is off-net) or to the endpoint. If the target is off-net, the default gateway will not forward the packet due to the TTL value of 1. Instead, it will send an ICMP time exceeded message back to the TCP Trace Route application. TCP Trace Route will continue to send TCP SYN packets with increasing TTL values to eventually identify the route to the endpoint. The name, IP address, average round trip time and % of total round trip time will be displayed for each intermediate router and final endpoint.

The **% RTT** (Percentage of total round trip time) column has a color bar to indicate the percentage. The colors have the following values:

- Blue** - less than 20% of total route time
- Yellow** - 20% to 50% of total route time
- Red** - 50% or greater of total route time

## 8.2 Service Performance Tool

The **Service Performance Tool** is available from the **Desktop Applications** screen and allows you to verify the existence and responsiveness of several standard network services. The **Performance**



**Tests/ITO Tests** option (RFC 2544/ITO ES\_ITO\_OPT on the **Options** screen) must be enabled for you to use the Service Performance Tool.

Service Performance Tool tests the following categories of devices:

- DHCP Servers
- DNS Servers
- E-mail Servers
- NT File Servers
- Web Servers
- User-Defined Servers
- WINS Servers

After adding and configuring the devices that you wish to test, apply your changes, and then start the test. After configuring the test, you can save the configuration in a script (file) that is stored on the CompactFlash. You can then load the script at a later date and the complete configuration will be loaded; including the test selections, test and device configurations, and which devices are selected for each test. You can save multiple configuration scripts.

Refer to the following topics:

- [Service Performance Tool Configuration](#)
- [Running Service Performance Tool](#)

## 8.2.1 Service Performance Configuration

After adding and configuring the devices that you wish to test, apply your changes and then start the test. After configuring the test, you can save the configuration in a script (file) that is stored on the CompactFlash. You can then load the script at a later date and the complete configuration will be loaded; including the test selections, test and device configurations, and which devices are selected for each test. You can save multiple configuration scripts.

### Adding a Device

You can globally add a device to all of the categories (except **Web Server**), or add a device to a single category.

Highlight the **Service Performance Tool** line (to add a device to all categories) or highlight an individual category (for example: **NT File Servers**) to add a device to that category only and tap the **Add Device** button. Use the pull-down menu in the **Remote Device** field of the **Add Device** screen to select a discovered device from the list, or select the **User Defined** entry and enter its IP address.

**Note:** The application populates the list of discovered Servers from a file on the CompactFlash. You must have saved a **Report** labeled **Devices.xml** in the **Device Discovery** test of the EtherScope application. If you are adding a device within a specific category, only devices that provide the service appear in the list.

Alternatively, if you select the **Service Performance Tool** line to add a device, you can use the **Servers** field to select which categories you wish to add the device. Tap the **OK** button when finished.

Repeat this procedure to add additional devices. You can add the same device multiple times. Each device has its own configuration that is stored separately.

### Removing a Device

Highlight a device and tap the **Remove Device** button to remove a device from the test.

**Note:** You cannot globally remove a device from all of the tests.

## Configuration

You can set global parameters that apply to all categories and devices, set parameters that apply to a single category, or set parameters that apply only to a single device selected in a specific category. Parameters set for a device override the parameters set for a test, and parameters set for a test override the global configuration settings made for all categories. Some device categories require parameters that apply only to the selected category; these parameters are set at the test level.

**Note:** When you set parameters at each level, all test results at that level and below are cleared. For example, if you change global parameters, test results at every level are cleared. If you change parameters for DHCP configuration, DHCP Server results are cleared.


### Global Configuration

Highlight the **Service Performance Tool** line and tap the **Configuration** button.

#### Test Control

- **Iterations** - the number of times each device will be queried.
- **Interval** - the amount of time between iterations.

**Refresh Device Discovery Information** - Tap the **Reload** button to read the **Devices.xml** file from the CompactFlash. Used to populate the device list when you select **Add Device**. The application populates the list of discovered Servers from a file on the CompactFlash. You must have saved a **Report** labeled **Devices.xml** in the **Device Discovery** test of the EtherScope application.

Tap the **Apply** button after making any configuration changes. All test and device results will be cleared. Press the **Defaults** button to restore factory settings. Press the back button  to return to the **Service Performance Tool** screen.

### DHCP Server Configuration

#### Override Test Control


Refer to the **Global Configuration** section for a description of the parameters in this section. You cannot configure these parameters at the individual device level.

#### DHCP Server Pass/Fail Criteria

- **PING Response Time** - set the maximum time that the server has to respond to a **PING** in order to pass the test.
- **DHCP Server Response Time** - set the maximum time that the server has to respond to a **DHCP** request in order to pass the test.

#### (Optional) BOOTP Parameters Requested

Select any or all of the listed BOOTP parameters to be returned as part of the verification. The number in parentheses after each parameter (for example: **Subnet Mask (1)**) is the BOOTP parameter tag as defined in RFC 1340. If any of these parameters are not returned, the test will fail and the reason will be shown on the device results screen.

Tap the **Apply** button after making any configuration changes. All test and device results will be cleared. Press the **Defaults** button to restore factory settings. Press the back button  to return to the **Service Performance Tool** screen.

## DNS Server Configuration

### Override Test Control

Refer to the **Global Configuration** section for a description of the parameters in this section. Not available at the device level.


### DNS Server Pass/Fail Criteria

- **PING Response Time** - set the maximum time that the server has to respond to a **PING** in order to pass the test.
- **DHCP Server Response Time** - set the maximum time that the server has to respond to a **DHCP** request in order to pass the test.

### DNS Lookup

- **IP Address** - enter the IP address of a device for the DNS server to resolve.
- **Host Name** - enter the device name for the DNS server to resolve. Use the format of *devicename.domainname.com*.

**Note:** The result of the **DNS Lookup** test does not affect the Pass/Fail status of the test. If the DNS Lookup test fails, it is indicated with an \* next to the entry in the **Status** column of the results.

Tap the **Apply** button after making any configuration changes. All test and device results will be cleared. Press the **Defaults** button to restore factory settings. Press the back button  to return to the **Service Performance Tool** screen.

## E-mail Server Configuration

### Operation Mode

Use the radio buttons to select the level of test.

### Override Test Control

Refer to the **Global Configuration** section for a description of the parameters in this section. Not available at the device level.

### E-mail Server Pass/Fail Criteria

- **PING Resp** - set the maximum time that the server has to respond to a **PING** in order to pass the test.
- **SYN/ACK** - set the maximum time for the combined TCP Syn/Ack sequence to complete.
- **POP3 Resp** - set the maximum time that the POP3 server has to respond.
- **Read Time** - set the maximum time to read from the server.
- **Write Time** - set the maximum time to write to the server.
- **SMTP Resp** - set the maximum time for the SMTP server to respond.

**Ports** - enter the **SMTP** server and **POP3** server port numbers.

**SMTP Server Connection (Send/Receive Mail mode only)** - enter an e-mail address to test the connection (for example: *username@your\_isp.com*)

### Device Configuration

When a specific device is selected, you can configure the SMTP and POP3 parameters.

**Server** - select **SMTP** or **POP3** to display the appropriate configuration fields.

#### SMTP Parameters

**Port** - enter the port number to use on the SMTP server.

**Send to (Send/Receive Mail enabled)** - enter an e-mail address to test.

**SMTP Login Required** - enable the check box and enter the appropriate **Username** and **Password** for the SMTP server.


#### POP3 Parameters

**Port** - enter the port number to use on the POP3 server.

**IP Address** - enter the IP address of the POP3 server. The default entry is the address of the SMTP server.

**Read Delay** - enter the maximum time.

**POP3 Authentication Parameters** - enter the appropriate **Username** and **Password** for the POP3 server.

Tap the **Apply** button after making any configuration changes. All test and device results will be cleared. Press the **Defaults** button to restore factory settings. Press the back button  to return to the **Service Performance Tool** screen.

### NT File Server Configuration

#### Operation Mode

Use the radio buttons to select the level of test:

- **Server Response** - check response time only.
- **Read** - read a file from the server.
- **Write/Read/Delete** - write a file to the server, read it back, and delete it when done.

#### Override Test Control

Refer to the **Global Configuration** section for a description of the parameters in this section. Not available at the device level.

#### NT File Server Pass/Fail Criteria

- **PING Resp** - set the maximum time that the server has to respond to a **PING** in order to pass the test.
- **Connect in** - set the maximum time to establish a connection.
- **Write Rate** - set the minimum rate for data transfer to the server.
- **Read Rate** - set the minimum rate for data transfer from the server.
- **Delete file in** - set the maximum time to remove a file from the server.


**NT File Server Parameters (Read or Write/Read/Delete mode only)**

- **Username** - enter the userid for the NT file server.
- **Password** - enter the password for the NT file server.
- **Share** - enter the sharename for the NT file server.
- **Path** - (for reading and writing a test file) Enter the complete directory path of a file on the NT file server.
- **File** - enter the filename that will be written to or read from the NT file server. The file is located in the **Path** defined above. If a file is written, it will be deleted at the end of the test.

**Note:** The Microsoft Windows drive mapping\directory format is \\servername\sharename\path\file. The sharename and path might be multiple levels, depending on how it is defined. For example, in \\servername\directory1\directory2\directory3\directory4\filename.ext, the sharename might be defined as *directory1\directory2* and the path would be *directory3\directory4*, or the sharename could be defined as *directory1* and the path would be *directory2\directory3\directory4*. Contact your system administrator if you need help determining these values.

You might also see *user1 on server02\home (H:)*. Here the server name is *server02*, the sharename is *home*, and the path is *user1*.

- **File Size** - enter the size of the file that will be written to or read from the NT file server.

Tap the **Apply** button after making any configuration changes. All test and device results will be cleared. Press the **Defaults** button to restore factory settings. Press the back button  to return to the **Service Performance Tool** screen.

**User-Defined Server Configuration****Override Test Control**

Refer to the **Global Configuration** section for a description of the parameters in this section. Not available at the device level.

**PING Test Pass/Fail Criteria**

- **Perform PING Test** - enable to run the PING test.
- **PING Response Time** - set the maximum time that the server has to respond to a **PING** in order to pass the test.

**SYN/ACK Test Pass/Fail Criteria**

- **Perform SYN/ACK Test** - enable to run the Synchronize / Acknowledge test
- **SYN/ACK Response Time** - set the maximum time for the combined TCP Syn/Ack sequence to complete.
- **SYN/ACK Port** - set the port number to use on the destination server.

**Web Server Configuration**

**Note:** Globally adding a device at the **Service Performance Tool** level does not add a device to **Web Server**.

**Override Test Control**

Refer to the **Global Configuration** section for a description of the parameters in this section.  
Not available at the device level.

### Web Server Pass/Fail Criteria

- **PING Resp** - set the maximum time that the server has to respond to a **PING** in order to pass the test.
- **First Reply in** - set the maximum time.
- **Receive Speed** - set the maximum time.
- **Name Lookup in** - set the maximum time.
- **Receive in** - set the maximum time.

### (Optional) Global Proxy Server Parameters


If you want to test using a proxy server, enter parameters here.

**IP Address / Name** - select the radio button and enter either the IP address or host name for the proxy server.

**Port** - enter the port number to use on the proxy server.

**Username** - enter the userid for the proxy server.

**Password** - enter the password for the proxy server.

Tap the **Apply** button after making any configuration changes. All test and device results will be cleared. Press the **Defaults** button to restore factory settings. Press the back button  to return to the **Service Performance Tool** screen.

## WINS Server Configuration

### Override Test Control

Refer to the **Global Configuration** section for a description of the parameters in this section.


### WINS Server Pass/Fail Criteria

- **PING Resp** - set the maximum time that the server has to respond to a **PING** in order to pass the test.
- **WINS Server Response Time** - set the maximum time that the WINS server has to respond.

### WINS Lookup

**Host Name** - enter the device name for the WINS server to resolve.

**Note:** The result of the **WINS Lookup** test does not affect the Pass/Fail status of the test. If the DNS Lookup test fails, it is indicated with an \* next to the entry in the **Status** column of the individual device results.

Tap the **Apply** button after making any configuration changes. All test and device results will be cleared. Press the **Defaults** button to restore factory settings. Press the back button  to return to the **Service Performance Tool** screen.

## Using Scripts

After configuring the Service Performance Tool, you can save the configuration in a file that is stored on the CompactFlash. You can then load the script at a later date and the complete configuration will be loaded; including the test selections, test and device configurations, and which devices are

selected for each test. You can save multiple configuration scripts.

To save configuration information in a script, insert a CompactFlash card in **Slot 2** and select the **Save Script** button on the **Service Performance Tool** screen. From the **Save Script** screen, tap the **Save As** button. Enter a descriptive name on the **New Test** popup and select **OK**. The script will now be saved on the CompactFlash in the **Tests** directory.

To load a script, select the **Load Script** button on the **Service Performance Tool** screen. On the **Load Script** screen, select the script that you wish to load and tap the **Load** button. The configuration information will be loaded and the title bar will show the script name. You can now **Start** the tests.

## 8.2.2 Running Service Performance Tool

You can select which tests are to be run by using the check boxes next to each test on the **Service Performance Tool** screen. An enabled check box indicates that the test will be run when you tap the **Start** button. If you enable the check box next to the **Service Performance Tool** line, then the tests will be run against the devices listed below each category. Clearing the **Service Performance Tool** check box will disable all tests. You can enable (or disable) a single test and enable selected devices under each test.

### Results

Highlight a test and tap the **Results** button to view the output of a test. You can also tap the **Results** button when a test is running to view the progress.

The **Status** column indicates the results for each category. If one device test doesn't pass, the summary at the test level will indicate **Failed**. Likewise, the overall pass/fail status at the **Service Performance Tool** level is a summary of all of the individual test results.

Tap the **Report** button to save the results to a file on the CompactFlash.

## 9 Troubleshooting in a Switched Environment


Getting the right visibility into switched VLAN environments can ease or speed the process of network troubleshooting. Use your Network Assistant's features to provide visibility.

**Device Discovery** is one of the instrument's automated tests. This test provides the foundation for troubleshooting connectivity and performance problems. Your Network Assistant automatically detects the switch slot/port/VLAN to which a device is connected. Select the **Device Discovery** test to see the type and number of devices discovered on your network. Tap the **Details** button or one of the device categories in the preview screen to obtain a list of the devices and their network configuration. Highlight a specific device in the list to see device utilization information in the preview screen. Tap the **Tools**



icon to access tools that you can use to further troubleshoot connectivity or performance problems.

In addition to automatically reporting where a particular device is connected in a switched environment, the instrument determines and reports the physical path between itself and another device through the **Trace Switch Route** test. From the **Device Details** screen, tap the **Trace Switch Route** hyperlink. The instrument displays the switches in the path between itself and the selected device. Trace Switch Route results can be used to further understand the potential source of a problem.

As part of the automated network discovery process, the instrument will discover VLANs configured within a broadcast domain. Tap the **Home**  icon and highlight **VLAN Discovery** for a preview of the VLAN inventory. Select the **Details** button to see a listing of discovered VLANs. When expanded, the



member switch interfaces are provided. Highlight an interface to get a preview of interface detail, utilization, and errors. Select the **Details** button to get a complete view.

An integral part of network discovery is to find and report the switches on the network. In particular, the instrument searches for the nearest switch. Once discovered, the nearest switch's active ports will be monitored for high utilization and errors. The **Switch Scan** test provides the capability to continuously monitor up to 2 switches on your network. A preview of the results is reported when **Switch Scan** is highlighted. Tap **Details** for a detailed tabular view and to configure this test for additional devices. Select the drop-down box for a list of discovered switches and highlight the desired device. Select the colored box to the left of the drop-down list to change the color representing that device. In addition to the instantaneous results, a longer term view of an interface can be obtained. Highlight an interface and tap the **Trend** button. The switch interface becomes the source for short term trending of port utilization and errors.

By default, the instrument will monitor the local network segment, however it can provide visibility into remote devices and segments without direct connection to the specific broadcast domain. To reconfigure the source for network statistics, highlight **Local Statistics** on the **Test Results** screen and select **Details**. Select a device and interface source from the drop-down **Source** and **Interface** boxes at the top of the **Utilization History** screen. The instrument will continue to monitor and trend this source throughout the session or until the source is changed. The network continues to monitor local utilization and errors in the background.

The instrument provides the means to change the configuration of switches and other network infrastructure devices through a web browser interface or Telnet session. You can select a device from the device list and use the **Tools** menu to initiate a Telnet session with the device.

## 10 Remote Access

You can use the Microsoft Internet Explorer web browser to access your EtherScope's web server. This provides you with the capability to run real-time reports, view Help, or launch the Remote User Interface. You can use the Remote UI to control your EtherScope Network Assistant instrument.

### Web Server

The instrument's web server provides a means to remotely access the EtherScope Network Assistant instrument.

To access the web server, start Internet Explorer on your PC, and enter the instrument's IP address. Use dotted-decimal format for the IP address (e.g. <http://112.129.137.12>).

**Note:** The instrument's IP address is located on the preview pane of the Test Results screen when the Connection test is highlighted.

**Note:** Do not use leading 0's in the IP address (i.e. enter 112.129.137.12 instead of 112.129.137.012). Using leading 0's can cause the browser to misinterpret the IP address.

This will display the **EtherScope Web Server** home page. From the home page, you can select the **Reports**, **Launch Remote UI**, **Support**, or **Help** buttons.

**Note:** You can bypass the web server and directly access the Remote User Interface as described in the Remote Control section below.

### Remote Control

The instrument contains a Virtual Network Connection (VNC) server that can be used for remote access. From your PC, start Internet Explorer and enter the instrument's IP address - **[http://\[IP address\]:5800](http://[IP address]:5800)** (5800 is the designated VNC port). VNC will be automatically invoked. From the VNC Authentication screen, click **OK**. By default, there is no password, but you can set a password for the

instrument on the [Instrument Settings – Security](#) screen.

When the EtherScope user interface is displayed, you can use your mouse to navigate the product. The instrument can be accessed by multiple users, but is controlled by one user at a time. You can disable remote access on the **Instrument Settings – Security** screen by clearing the **Enable remote user interface** check box.


#### User Interface Events that will Terminate a Remote Session

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

- If IP parameters are manually changed on the instrument and **Apply** is selected in the **Instrument Settings - TCP/IP** screen
- If the **Run Auto Configuration** button is selected on the **Instrument Settings - TCP/IP** screen
- If the **Start Test** button on the **Cable Verification** screen is selected
- If the **Start Test** button on the **Signal Verification** screen is selected
- If the instrument's MAC address is changed in the **Instrument Settings - Ethernet** screen
- If the Ethernet link goes down on either interface

## 11 Software Update

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

1. Tap the EtherScope icon  , located on the left side of the title bar.
2. On the resulting drop-down menu, select **Instrument Settings**. The **Instrument Settings** screen appears.
3. Tap **Version** in the Preview pane.
4. The **Instrument Settings - Version** screen displays the versions of currently installed software and hardware.
5. To check for updates, tap the **Check for software updates** button.
6. The application connects to the Internet and the Fluke Networks web site to check if a software update is available.
7. If a newer revision is available, follow the on-screen instructions to download the software and install the software.

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

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

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

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

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

given in the [Language Settings](#) topic.

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

## 12 Contacting Fluke Networks

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

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

Our offices are located at the following addresses:

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

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

## 13 Trademarks and Copyrights

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

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

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

## 14 Tests

### 14.1 Connection

The **Connection** test is automatically run when the instrument is powered on, the **Restart All** button is selected, or a network cable is plugged in. The instrument automatically detects when a cable is plugged in to it and determines the appropriate test to run based on the cable type (Ethernet or gigabit fiber optic), and what is on the other end of the cable - an Ethernet network, network interface card (NIC), unterminated cable, or Wiremap adapter.


If the [Fiber Option](#) (EtherScope Series II instruments) is enabled on your instrument and both cable types are connected, the instrument will use the fiber interface on startup or when tests are restarted. If one interface is already active, inserting the other connection will have no effect. In order to switch interfaces, the active interface must be disconnected and the new cable inserted. This will cause the instrument to reset itself and restart testing. To conserve battery power, the fiber interface is powered off when not in use.


The **Connection** test shows the instrument and network configuration information and link status of your Network Assistant in the left-side preview pane.

**Note:** (Ethernet cable) The **Advertised** field under the **Speed** category in the Preview pane indicates the speeds/duplex offered by the connection partner (far end unit, not the Network Assistant). The Network Assistant speed/duplex can be configured on the [Instrument Settings - Ethernet](#) screen.

**Note:** (Fiber cable) It is important that the fiber cable type being used to connect the instrument to the network matches the SFP module on the instrument and the GBIC module on the network device (e.g. if the instrument's fiber module is LX, use an LX fiber cable to attach the instrument to an LX module on the network device). Indeterminate results will occur if there is a mismatch. You can verify the instrument's module type on the [Version](#) screen.

You can customize the instrument, including specifying passwords, SNMP community strings, 802.1X authentication information, and other configuration information on the [Instrument Settings](#) screens.

Tap the EtherScope icon  on the Title bar and select **Instrument Settings** (or the **Connection** hyperlink in the preview pane) to view the instrument's **TCP/IP**, **802.1Q/IP TOS**, **802.1X**, **Ethernet**, **Security**, and **General** settings and configuration. Refer to the [Instrument Settings](#) topic for more information on these settings and configuring the instrument.



If the instrument is connected to the network with an Ethernet cable, tap the plus icon  next to the **Connection** test to expand the view for the [Cable Verification](#) and [Signal Verification](#) tests. If the instrument is connected with a fiber optic cable, the [Fiber Loss Test](#) is available.

### 14.1.1 Cable Verification

Cable testing can be a critical element for troubleshooting wiring problems. Your EtherScope instrument is capable of testing and verifying the integrity of your network wiring. The **Cable Verification** test can be found by expanding the [Connection](#) test and tapping **Cable Verification**. The results from the power-on test are shown. The preview pane shows a summary of the length of the individual wires of the cable.

**Note:** (Ethernet cable) It is not necessary to disconnect the far end of the cable for the length to be measured. Cable length can be measured while the cable is connected to a Wire Map adapter, connected to nothing (unterminated), or connected to a network device (hub, switch, NIC, etc.).

**Note:** (Fiber cable) It is important that the fiber cable type being used to connect the instrument to the network matches the SFP module on the instrument and the GBIC module on the network device (e.g. if the instrument's fiber module is LX, use an LX fiber cable to attach the instrument to an LX module on the network device). Indeterminate results will occur if there is a mismatch. You can verify the instrument's module type on the [Version](#) screen.

A  in the right-most column of the main screen indicates that a valid cable has been detected. A  indicates a problem with the cable has been detected. This test is rerun automatically if a cable change is detected.

**Note:** Running the Cable Verification test will disconnect the instrument from the network, which will stop other tests being run by the instrument. If you are using the remote control application, you will

lose connection to the instrument.

Select the **Details** button to display the **Cable Verification** screen. The full test automatically starts and the test results are shown. Tap the **Restart Test** button to rerun the test.

Use the radio buttons on the Title bar to select between **Copper** or **Fiber Optic** cable.

**Force wiremap test** - when enabled, the instrument runs the Wiremap test even if a wiremap device is not detected on the wiremap port.

### Copper Cable Testing

You can use **Cable Verification** to:

- Test a cable run
- Map a cable using a **Wire map** adapter (detected automatically)
- Discover the length of a cable
- Generate a tone on the cable so that you can locate it

By cable pair, results include:

- Color coded cable view
- Cable impedance
- Termination Impedance (if far end of cable is plugged into a device)
- Length
- Status (terminated, short, split pair)
- Problems

You can configure:

- Cable Type (use the pull-down menu)

**Note:** It is important that you select the correct cable type because it affects the reported cable characteristics.

- Units (Meters/Feet)
- Color Coding (T568A or T568B standard)

After initial setup or changes, tap **Restart Test** to rerun the test. The **Cable Verification** test is automatically rerun when a cable change is detected.

### Cable Toner

Tap the **Cable Toner** button to open the **Tone Generation** popup dialog. You can generate an analog tone or a digital tone specifically for the Fluke Networks IntelliTone Probe. The analog tone is compatible with any analog tone probe. The toner is turned off when you close the dialog.

### Fiber Loss Test

With a DDM SFP (Digital Diagnostic and Monitoring Small Form Pluggable) fiber adapter installed in the 1000BASE-X port and a fiber optic cable connected to the instrument, you can run the **Fiber Loss Test**. The use of the DDM SFP adds **Tx** and **Rx Power**, **Tx Bias**, **Vcc**, and **Temperature** readings over using the Fiber Optic Meter method described below.

This test measures optical power in units of dBm and microwatts. It also determines calculated optical power loss (attenuation). The loss value (in dB) is the difference between the level measured on a nearly lossless, short reference cable and the power level measured across the fiber cable under test.

You can measure optical loss and output power on multimode or singlemode cable.

## Configuration

1. With the power off, install a DDM SFP fiber adapter in the 1000BASE-X port and connect a fiber cable to the instrument. Turn on the instrument. After the instrument establishes link, expand the **Connection** test and select the **Fiber Loss Test**. The preview pane shows a summary of results.
2. Tap the **Details** button to begin the test.
3. The test automatically begins.
4. You can configure two variables:
  - **Loss Budget** - This value represents the amount of acceptable power loss. When testing a cable, the graph indicates the amount of loss and shows the **Loss Limit**. If the loss exceeds this value, a failure is reported. Use the Up or Down arrows to set the value. Different cabling standards carry different loss limits.
  - **Set Reference** - The reference power represents a baseline amount of power (Rx Power) on the cable. This value is used as a reference from a "known good" patch cable to test other cables. The **Set Reference** button records the current power reading as the new reference value. Run the test with a short, known good cable before pressing the **Set Reference** button.

## Results

The preview pane on the left side of the display shows the cable wavelength and the measurement results. The graph gives a quick visual representation of the quality of the cable under test.

## Fiber Testing with a DSP Fiber Optic Meter

If you do not have a DMM SFP fiber adapter, you can test fiber optic cable using a Fluke Networks DSP Fiber Optic Meter (FOM). The Fiber Optic Meter is an optical power loss meter. The instructions for configuring the FOM are included with it.

## Configuration

1. Connect an Ethernet cable from the FOM to the RJ-45 LAN connector on your EtherScope instrument.
2. Turn on the FOM to the appropriate setting for the cable type.
3. Tap the **Cable Verification** screen of the EtherScope instrument (expand the **Connection** test if needed) and press the **Details** button.
4. Select the **Fiber** radio button on the Title bar.
5. The test automatically begins.
6. You can configure two variables:
  - **Loss Budget** - This value represents the amount of acceptable power loss. When testing a cable, the graph indicates the amount of loss and shows the **Loss Limit**. If the loss exceeds this value, a failure is reported. Use the up or down arrows to set the value. Different cabling standards carry different loss limits.
  - **Set Reference** - The reference power represents a baseline amount of power (Rx Power) on the cable. This value is used as a reference from a "known good" patch cable to test other cables. The **Set Reference** button records the current power reading as the new reference value. Run the test with a short, known good cable before pressing the **Set Reference** button.

## Results

The preview pane on the left side of the display shows the configuration of the FOM and the measurement results including the power measurement and loss. The graph gives a quick visual representation of the quality of the cable under test.



### 14.1.2 Signal Verification

The **Signal Verification** test analyzes the signal quality of the Ethernet cable and establishes connectivity at the physical layer. You can observe the Ethernet cable signal levels and the 10/100/1000 BASE-T/TX connection process. Running this test will initially monitor the cable status, determine the device connection status, and initiate link auto-negotiation if appropriate.

To run Signal Verification, expand the **Connection** test and tap **Signal Verification**. A summary of the auto-negotiation process is displayed in the preview pane. Select the **Details** button to display the **Signal Verification** screen. The test will start automatically.

**Note:** Running the Signal Verification test will disconnect the instrument from the network, which will stop other tests being run by the instrument. If you are using the remote control application, you will lose connection to the instrument. Because of the loss of connection, duplex verification can not be measured during the Signal Verification test.

The test will continue to establish an Ethernet connection until successful. Once a successful Ethernet connection is reached, the signal level will be monitored and displayed. Tap the **Restart Test** button to repeat the test.

#### DC Voltage Scan

Cable line voltages are scanned for DC level content and overvoltage conditions. The voltage levels are displayed. The presence of high voltages may indicate telephone connections or Power over Ethernet (PoE).

#### Signal Levels

The presence of signals and their amplitudes are monitored. **No Signal**, **NLP**, **FLP**, and **Data** signals are detected and displayed. IEEE 802.3 and ANSI X3-263 standards are referenced for minimum signal levels along with additional references to typical market product signal levels.

The cable connection properties are analyzed to identify the types of devices that may be connected. These device connections include devices advertising link capabilities, office locators, test units, Token Ring, 802.11af Ethernet Power sources/sinks, and Telco.

Speed (Mbit)	Min. (0 to Peak Volts)	NLP/FLP/Signal (0 to Peak Volts)	Typical Signal (0 to Peak Volts)
10	0.585		1
100	0.5		1
1000	2 x 0.67		1.6

#### Auto-negotiation Signals

FLP signals from the auto-negotiation sequence display what the instrument advertised and what the cable connection source (partner) advertised. These signals indicate the speeds supported (10/100/1000) and the duplex supported (half or full).

#### Negotiation Results:

Completion of the Ethernet auto-negotiation sequence will display the final connection speed and duplex results. In addition, duplex will be verified against what was advertised and the signal amplitude will continue to be monitored for amplitude variations over time and temperature.

In order 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 only at 100 Mbit half-duplex, the **Signal Verification** test will temporarily override that configuration to measure the complete auto-negotiation process. When the test is exited, the previous link configuration will be restored.



### Power over Ethernet

Your EtherScope instrument (Hardware [Version](#) 105 or greater) can detect and measure voltage on a PoE (Power over Ethernet) enabled port. You must enable the **Solicit for 802.3af Power over Ethernet** check box on the **Signal Verification** screen and tap the **Start Test** (or **Restart Test**) button to test for PoE. When the check box is enabled and the instrument is connected to a port that supports PoE, it will signal the device to activate PoE and then measure and report the voltage on the line (in the **DC Voltage Scan** category). The measured voltage and polarity for each pin with PoE voltage is reported and a message will indicate either **802.3af PoE Power** or **802.3af PoE Probes Only**. The **Power** message indicates that a PSE (Power Sourcing Equipment) has been discovered and full PoE power is available. The **Probes Only** message indicates that a PSE has been discovered and is probing for PoE power. In both cases, the **Service** field in the **Signal Verification** preview pane will indicate **802.3af**. If PoE is not detected, the message (in the **DC Voltage Scan** category) **802.3af PoE not detected** is shown.

**Note:** The [Connection](#) test that is run when the instrument is started or when a cable is plugged in to the instrument may or may not discover PoE voltage on the port. The only reliable way to determine if PoE is available is to enable the PoE check box and run the **Signal Verification** test.

## 14.2 Local Statistics

**Local Statistics** provides a view of the amount and type of traffic found on the network segment under test.

Highlight **Local Statistics** on the Test Results page and tap the **Details** button to see **Utilization History**.

The Utilization (trending) graph shows a history of network activity. Use the radio buttons to select between displaying **Utilization Details** and **Error Details**. Change the **Update every** field to adjust the sample period for the graph. Tap a sample period on the graph to see a utilization summary in the table below the graph. Tap the **Hide Totals** button to hide the table and enlarge the graph.

The following errors are reported:

- **Undersized Packet** - a packet that is less than 64 bytes.
- **Oversized Packet** - a packet that is greater than 1518 bytes with a valid checksum.
- **Bad FCS** - a packet that has an invalid checksum.
- **Jabber** - a packet that is greater than 1518 bytes with an invalid checksum. In general, you should not see jabbers.
- **Ghost** - energy on the cable that appears to be a frame, but has an invalid beginning-of-frame pattern. The ghost frame must be at least 64 bytes long.

The most likely causes of these errors are a faulty NIC and/or faulty or corrupt NIC driver files, bad cabling, or grounding problems.

### Remote Statistics

By default, the instrument monitors the local network segment. You can collect statistics on a remote device. Select a discovered device and interface source from the drop-down **Source** and **Interface** boxes at the top of the **Utilization History** screen. The data for the selected device will be displayed. The instrument will continue to monitor and trend the selected source throughout the session or until the source is changed. It also continues to monitor local utilization and errors in the background. You can return to the **Local Utilization** view by selecting **This EtherScope** from the **Source** field. You can select and view utilization on a remote device and segment without direct connection to the specific collision domain(s).

**Note:** When you select a remote device in the **Utilization History** window, it will become the second monitored switch in the [Switch Scan](#) test.

**Note:** Trending information for the instrument continues to be collected in the background when a different device is selected. You can see the information by selecting **This EtherScope** in the **Source** field. Statistics for any other device are only collected while the device is selected, the data will be lost as soon as another device is selected.

### 14.2.1 Protocol Statistics

Expand **Local Statistics** on the **Test Results** page and highlight **Protocol Statistics**. The preview pane shows the top protocols and their percentage of total packets on the network. Tap the **Details** button to see a list of all the network protocols that have been discovered on the local network segment.

Use the radio buttons on the Title bar to select between viewing **Protocols** or **Summary** view.

The left side shows a summary of the devices sending the most packets. Highlight a protocol in the list on the right to see a summary of the top devices using the selected protocol. Tap the **Clear** button to reset the counts (this will also reset the [Top Talkers](#) counts). Select a device in the summary view to see [Device Details](#) for that device.

**Note:** It is possible that a device that is not part of the discovery database will appear in the summary view. If you tap the device, you will get a prompt that asks whether you want to add it to the discovery database. See [Add Device](#) for more information.

You can use **Protocol Statistics** to determine if there are unwanted or unexpected protocols on your network consuming network bandwidth.

### 14.2.2 Top Talkers

This test identifies the devices consuming the most network bandwidth. Expand **Local Statistics** on the **Test Results** page and highlight **Top Talkers**. The preview pane shows the devices consuming the most network bandwidth and their percentage of total packets on the network. Tap the **Details** button to see a list of all the discovered devices that are generating traffic on the local network segment. Use the radio buttons on the title bar to sort the list by packet type. You can use these results to make decisions about network reconfiguration, load balancing or expansion.

Highlight a device in the list on the right side of the screen to see the IP and MAC address for the device. Tap the **Details** button to open the **Device Details** view for the device. Tap the **Clear** button to reset the counts for all devices (this will also reset the [Protocol Statistics](#) counts). Select a column header to sort the table by the selected attribute.

### 14.2.3 VLAN Statistics

This test identifies the VLAN traffic on the port on which the instrument is connected and reports statistics on all packets detected. Highlight **VLAN Statistics** on the **Test Results** and the preview pane shows the top VLANs (by packet count) on the network segment (the VLAN ID selected in the instrument's 802.1Q configuration will always be included). The status line shows the total number of VLANs discovered and the top VLAN ID and its percentage of total packets. Tap the **Details** button to view the complete list of VLANs and statistics, including the Native or untagged VLAN traffic.

The detailed view shows counts broken down by priority for the first 127 VLANs discovered.

VLAN ID /	Octets	Packets	% of Pkts
508	1362928	7444	32.13%
.1p 0	1343052	7160	30.90%
.1p 6	456	6	0.03%
.1p 7	19420	278	1.20%

For example, the **.1p 0** entry indicates 802.1p, priority 0. The percentage count is based on all packets on all VLANs.

Activity on other VLANs after the first 127 are established is tracked in the **Other VLANs** category. If you are interested in seeing statistics for a VLAN that is not included in the first 127, change the instrument's configured **VLAN ID** ([Instrument Settings - 802.1Q/IP TOS](#)) to the desired VLAN and revisit **VLAN Statistics**.

**Note:** If the port to which the instrument is connected is configured with 802.1Q VLAN tagging and the instrument is not, or [802.1Q](#) is enabled on the instrument but not on the port, DHCP will fail and device discovery will most likely only show 1 device (**This EtherScope**). However, **VLAN Statistics** will show whether any VLAN tagged packets are on the network segment. You can use this information to 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).

**Note:** The number of VLANs discovered by **VLAN Statistics** and [VLAN Discovery](#) will frequently differ. This is because **VLAN Statistics** shows the number of VLANs detected by monitoring the local network segment, and **VLAN Discovery** is using active (SNMP) discovery to determine the number of VLANs on your entire network.

You can easily join a VLAN from this screen. Select (highlight) a VLAN from the list of discovered VLANs and tap the **Apply** button. Select **OK** on the **VLAN Reconfiguration** popup and the instrument will change its configuration settings to match the selected VLAN. All discovery data will be discarded and discovery will begin anew. The new configuration information will be saved in [Instrument Settings](#) and used for establishing network connections.

**Note:** The 802.1Q settings on the [802.1Q/IP TOS](#) screen will be set appropriately for the new VLAN.

### QinQ (VLAN Tag or VLAN Tunneling)

The IEEE 802.1 QinQ VLAN Tag expands the VLAN space by tagging the tagged packets, thus producing a "double-tagged" frame. This expands the VLAN space and allows a service provider to keep traffic from different customers segregated in the service provider infrastructure.

If a QinQ tagged frame is detected, it will be indicated on the **VLAN Statistics** preview pane:


**Last QinQ** - shows the VLAN ID of the last QinQ packet

**QinQ Found** - shows the timestamp of the last discovered QinQ packet

## 14.3 Device Discovery

The **Device Discovery** screen displays counts of network devices discovered by the EtherScope Network Assistant. The instrument automatically starts discovering devices as soon as it is connected to the network. **Device Discovery** presents near real-time results. As device names are resolved, IP addresses are replaced with the device names. Devices are discovered via traffic monitoring and by actively querying the hosts.

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

Highlight a device to display device summary information. Tap the **Details** button to open the [Device Details](#) view for the device. Tap the Back button  to return to the **Device Discovery** screen.

Use the **Find** window at the top of the display to locate a particular device. You can enter a partial name or address (MAC or IP) to find the entry. Use the pull-down menu to find a device that has been previously entered.

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

- ☒ Show IP Address
- ☐ Show MAC
- ☐ Show Switch Info
- ☐ Show Properties

**Note:** If a device is highlighted, tap the **X** in the upper left corner to display the radio buttons.

A slide-bar at the bottom of the screen allows access to the device information that can not be seen. Select a column header to sort the table. Columns can be resized by dragging the separating bar between columns in the header.

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

The Network Assistant discovers devices in the local broadcast domain to which it is connected. It is possible that a device in the local broadcast domain is not discovered because it does not generate much network traffic or does not respond to the active discovery methods employed by the instrument. You can add any device to the discovery database by using [Add Device](#). The device does not have to be in the local broadcast domain. For example, you can use **Add Device** to add a switch that is part of a separate management VLAN that is outside of the local broadcast domain.

Tap the Tools button to display a list of [Network Tools](#) that you can use to troubleshoot network problems or to connect to a device.

## 14.4 Network Discovery

Your EtherScope Network Assistant discovers IP and IPX networks and NetBIOS Domains. Highlight **Network Discovery** on the **Test Results** screen and tap the **Details** button to view the list of Subnets and Domains and the discovered Hosts in each one.

The following list defines the local network categories that can be discovered by the application:

- **IP Subnets:** This category consists of any discovered IP network information. The IP subnets use a 32-bit IP subnet mask in dotted-decimal format followed by an integer number that indicates the number of bits in the network mask followed by the number of hosts (in parentheses) that have been discovered in the subnet (e.g. 12.196.129.000/16 (7 hosts)).
- **NetBIOS Domains:** This category consists of any discovered NetBIOS domain information for the selected NetBIOS domain/workgroup.
- **IPX Networks:** This category consists of any discovered IPX network information. IPX networks can use any of the following encapsulated protocols: 802.3, Ethernet II, 802.2, or SNAP.

Highlight an IP Subnet to see the following summary information:

- **IP Subnet:** The local broadcast domain to which the device is connected.
- **IP Range:** The IP address range for the Subnet.
- **Broadcast:** The IP broadcast address for the Subnet.
- **Mask:** The network mask for the subnet and the number of network bits in the mask.

Highlight a NetBIOS Domain to see the following summary information:

- **Master Browser:** A Master Browser (MB) gathers all the announcements sent by other computers and creates and maintains the browser list from these announcements. An MB can then serve clients by sending them the browser list when they request it.
- **Primary Controller:** A Primary Domain Controller (PDC) contains a master copy of the user account database. All changes to the user account database are written to the PDC, and then replicated to the Backup Domain Controller(s). The PDC also authenticates logons.
- **Backup Controller:** A Backup Domain Controller (BDC) contains a backup copy of the user account database. It receives updates of the user account database from the PDC, and it also authenticates logons. It can be promoted to PDC if the PDC fails.


Highlight **IPX Networks** to see the list of discovered IPX networks. Expand an IPX network to see a list of devices in the network and their IPX address.

Use the **Find** window at the top of the display to locate a particular device. You can enter a partial name or address (MAC or IP) to find the entry. Use the pull-down menu to find a device that has been previously entered.

## 14.5 VLAN Discovery

As part of the automated network discovery process, the Ethernet Network Assistant will identify VLANs configured on the switches that are discovered in the broadcast domain to which the instrument is connected. This is useful for locating devices on the network and verifying network configuration. The **VLAN Discovery** screen provides a VLAN centric view of your network.

**Note:** It is possible that a switch could have VLANs configured in multiple broadcast domains. The instrument will show all the discovered VLANs, but discovery is only run on the broadcast domain to which the instrument is connected.

Highlight **VLAN Discovery** on the **Test Results** page for a preview of the VLAN inventory. Tap the **Details** button to see a detailed listing of discovered VLANs, including the number of interfaces on each VLAN. Select a VLAN and the preview screen shows the switches and routers that have interfaces that are part of the selected VLAN. Expand a VLAN (tap the  icon) and you see a list of the interfaces that are part of the VLAN, the switch/router slot/port that the interface is in, and the number of hosts that are on each interface. Highlight an interface and tap the **Details** button to open the **Device Details** screen for the selected interface. VLANs that have no associated member switch interfaces will display the switches that are configured for the VLAN.

**Note:** Normally, the instrument will not report the number of hosts that are on VLANs that are configured in different broadcast domains. Devices located in other broadcast domains that have been manually added to the database using [Add Device](#) will be reported.

**Note:** You must have the proper **SNMP Community String** configured for a particular switch or router in order to discover VLAN information. You can configure community strings on the [Instrument Settings - Security](#) screen. Verify that the instrument has access to the SNMP agent and that there are no security measures in place preventing SNMP discovery by the EtherScope. Also, ensure that the instrument is connected to the same broadcast domain as the Management VLAN of the switch, as this is where the SNMP Agent typically resides. Another option is to manually add the

device to the database.

The **Device Details** screen shows the hosts that are connected to the selected interface. You can select a different interface to see the hosts that are connected to that interface. You can also select a specific host and then tap the **Details** button to open **Device Details** for the selected host.

**Note:** Switches or routers may have proprietary MIBs that are not supported by EtherScope discovery. This may prevent the complete discovery of the device, including its VLAN configuration.

**Note:** The instrument identifies switches and routers that are running Cisco Discovery Protocol (CDP) and uses this information to discover and report switches and routers that are outside of the local broadcast domain.

**Note:** The number of VLANs discovered by [VLAN Statistics](#) and **VLAN Discovery** will frequently differ. This is because **VLAN Statistics** shows the number of VLANs detected by monitoring the local network segment, and **VLAN Discovery** is using active (SNMP) discovery to determine the number of VLANs on your entire network.

## 14.6 Nearest Switch

The EtherScope Network Assistant uses SNMP queries to search for the nearest switch. The nearest switch is discovered by examining the bridge forwarding tables of all the local switches. The port to which the instrument is connected is monitored for utilization and errors. Summary information and graphs of port utilization and errors are shown in the preview screen. Select the **Details** button to see more information on the switch and its interfaces.

**Note:** The proper SNMP community strings must be configured for the instrument to discover and query network switches. Refer to the [Instrument Settings - Security](#) topic for more information on configuring SNMP community strings.

**Note:** It may take several minutes or longer to fully discover the switches on your network. During this time, you may see that the **Nearest Switch** designation "bounces around" before the closest switch is finally determined. If you are performing a task such as verifying office connectivity where you are quickly changing the network connection of the instrument, the **Nearest Switch** results may be inaccurate.

**Note:** If you are using the instrument to verify office connectivity, you may want to switch to [Fast connect mode](#) in order to speed up the discovery.

**Note:** If the management ports of your network switches are configured on a separate VLAN and the Network Assistant is connected to a different broadcast domain, then it is likely that the instrument will report an incorrect **Nearest Switch**. You can solve the problem by adding the switch into the database using the [Add Device](#) feature. The instrument will always "discover" an added device until it is manually removed from the database.

## 14.7 Switch Scan

The **Switch Scan** test provides the capability to continuously monitor the discovered [Nearest Switch](#) and one additional user-selected switch on your network. A preview of the results is reported when **Switch Scan** is highlighted on the **Test Results** screen. Tap **Details** for a detailed graphical view and to select a second device to be monitored.



By default, the **Nearest Switch** is monitored. Disable the **Show** check box to remove showing the **Nearest Switch** statistics. Nearest switch statistics will still be collected, just not displayed. Enable the check box to restore the view. You can monitor a second switch by selecting one from the drop-down menu in the **Source** field.

In addition to the instantaneous results, a longer-term view of an interface can be obtained. Highlight an interface and tap the **Trend** button. This switches you to the [Utilization History](#) test. The selected interface becomes the source for short term trending.

**Note:** The proper SNMP community strings must be configured for the instrument to discover and query network switches. Refer to the [Instrument Settings - Security](#) topic for more information on configuring SNMP community strings.

**Note:** The instrument identifies switches that are running Cisco Discovery Protocol (CDP) and uses this information to discover and report devices that are outside of the local broadcast domain.

**Note:** When trending is selected on a "remote" device, i.e. one that has been added using the [Add Device](#) feature, statistics are based on the device's MIB2 traffic statistics.

**Note:** Trending information for the instrument continues to be collected in the background when a different device is selected. You can see the information by selecting This EtherScope in the Source field. Statistics for any other device are only collected while the device is selected, the data will be lost as soon as another device is selected.

## 14.8 Key Devices



You can designate one or more devices on your network as **Key Devices** and then test them to verify that they are responding to a [Ping](#). As an example, you can use the **Key Devices** test to quickly verify network connectivity when doing moves, adds, or changes in an office. Establish a list of important network devices that you want to ensure can be reached (e.g. the DHCP, e-mail, web and print servers, and the default router). As you plug the instrument into each network connection, just tap **Start Test** and verify that all designated key devices are detected.

The default condition is that no devices are designated. You must configure key devices specific to your network and troubleshooting needs. The **Key Devices** test is run once when the instrument is first connected to the network. It can be run subsequently from the **Key Devices** details screen.

Highlight **Key Devices** on the **Test Results** screen and select the **Details** button. Use the drop-down menu at the top of the **Key Devices** screen to select a discovered device and mark it as a key device, or select the **Add Device** button and enter the IP address of a device.

**Note:** If you enter the IP address only, the device will be monitored as a Key Device and not added to the Discovery database.

Enable the **Add to device discovery** check box and enter the MAC address for the device if you want the device to be included in the discovery database. This will cause the device to appear in other tests.






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

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

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



## 14.9 Problem Detection

Displays any network devices that may be experiencing problems. Tap the **Details** button to see a list of discovered problems. Problems are categorized as an **Error** , **Warning** , or **Info Message** . Resolved problems are indicated with a . You can remove a problem from the list by highlighting it in the list and tapping the **Delete** button. Select the  icon next to the **Deleted problems** entry in the list to see all deleted problems.

The problem conditions are given below:

### Errors

- [Duplicate IP](#)
- [Bad Subnet mask](#)
- [Bad IP address](#)
- [IP in use](#)
- [Lost lease](#)
- [Cable Run Possibly too long](#)
- [Possible bridge tap](#)
- [Possible split pair](#)

### Warnings

- [Router not responding](#)
- [Only device in subnet](#)
- [Only device in network](#)
- [Proxy ARP reply](#)

### Info

- [Only device in domain](#)

### 14.9.1 Errors

#### 14.9.1.1 Duplicate IP

This error indicates that the device associated with this error and another device on the network are both using the IP address specified in the error message. This condition confuses network routing. When a packet of data needs to be delivered, devices on the network do not know where to send it. This may cause corrupt ARP caches in routers and disable communication between the machines on the local network.

In the Windows environment, a machine checks for a duplicate IP address when it is first turned on, and it is usually flagged at this point. The machine that had the address first will continue to operate, but the second machine will disable TCP/IP networking. Also, the machine that had the address first will pop up a warning about the condition, and it will continue to do this as long as the condition exists. On other operating systems, there will be a variety of problems, all of them relating to poor or disabled networking.

To correct this problem, you must identify at least one of the devices, and change its address. The application identifies the IP address in use by each machine and creates a database record based on the MAC address. When it sees two machines using the same address, it performs several checks to make sure the error is valid and to make sure the first device did not change its address (which would allow the second device to use the address without problems).

**Note:** You should check the status column to determine if the condition still exists because these problems often get resolved shortly after they are detected.

#### 14.9.1.2 Bad Subnet Mask

This error indicates that the IP subnet mask specified for the device is wrong. This can be caused by incorrect configuration of the device's subnet mask.

In IP networking, devices must have some information about what devices are in the local network, and how to reach remote devices. The subnet mask allows a device to quickly determine if it needs to send a packet of information to the router for delivery or can directly reach a device. When the subnet mask is wrong, this decision cannot be made correctly.

The subnet mask separates the IP address into two parts: network and host. The subnet mask uses "1"s to indicate the network portion and "0"s to indicate the host portion. For example, a subnet mask of 255.255.192.0 is 11111111.11111111.11000000.00000000. A device's subnet mask can consist of only contiguous "1"s, and if it is not the same as that in use by the rest of the devices on the subnet, there will be networking problems.

If the subnet mask is misconfigured, sometimes communication to off-network devices fails, and sometimes local operation suffers. Sometimes everything still works, but there is extra traffic that is being generated by other devices on the network that are unaware that the device is misconfigured. Reconfigure the device generating the subnet mask error so that it has the correct subnet mask.

#### 14.9.1.3 Bad IP Address

The identified device's IP address is misconfigured and a different address should be used. The IP address is the same as the subnet address or the subnet broadcast address. The **Network Discovery** test shows the range of addresses which are valid for each of the discovered IP subnets.

If DHCP is being used to assign addresses, it may be misconfigured.

#### 14.9.1.4 IP in Use

While the instrument was running its autoconfiguration process, the DHCP server offered an IP address that is already in use by another device on the network.

A device may be using a static IP address that is part of the DHCP address space or the DHCP server may be misconfigured.

#### 14.9.1.5 Lost Lease

The DHCP lease on the IP address of the instrument has expired and the instrument was not successful in renewing the lease with the DHCP server.

Verify the DHCP server is running and functioning properly. Also, check if the network connection between the instrument and DHCP server has failed. Verify the instrument's TCP/IP settings on the [Instrument Settings - TCP/IP](#) screen.

#### 14.9.1.6 Cable Problems

The EtherScope Network Assistant will discover three types of cable problems:

- **Cable Run Possibly too long** - the cable exceeds 1000 feet.
- **Possible bridge tap** - there may be unterminated cable that extends beyond the terminated portion.
- **Possible split pair** - cable wire pairs may be crosswired on the terminal connector.

## 14.9.2 Warnings

### 14.9.2.1 Only Device in Subnet

This warning indicates that the device using the IP address specified is the only device in an IP subnet. Most likely, the device is not properly configured for IP operation. Furthermore, it is unlikely that any of the TCP/IP networking is operating correctly for this device. However, if some networking is still functional, it is most likely local networking using the NetBEUI or IPX protocol.

Common causes of this problem include the following:

- The device is connected into the wrong port in the wiring closet.
- The device has been reconfigured and not rebooted.
- A configuration mistake was made.
- The device is a printer and it still has its default configuration.

Find an unused IP address in the correct IP subnet, and then reconfigure the device to use this address or use DHCP to configure the IP address for the device.

### 14.9.2.2 Router Not Responding

This warning indicates that the instrument can not communicate with the default router for the specified host.

Check the network configuration for the specified host to see if it is using an incorrect default router. Also check if the default router is down or the connection between the instrument and router has failed.

### 14.9.2.3 Only Device in Network

This warning indicates that the device is the only device in the IPX network shown in the problem message. At bootup, most network devices send a request for network information. A server or router on the network provides this information to the devices. Networking may still operate as expected, but there will be unnecessary traffic on the network.

This warning can be caused by several things:

- A server or router is advertising a network number that no other device is using. This is usually due to a configuration error on the device.
- Some service device (like a hub or printer) picked up this network number when a change was being made on the network, and the device has not been rebooted since, and it may be advertising the wrong network number.
- The device is bound to the wrong network.
- The device was manually configured with the wrong network number.

If the device that is using this network number is a router or server, it must be reconfigured. For other devices (like printers), simply reboot the device.

### 14.9.2.4 Proxy ARP Reply

Routers with Proxy ARP enabled will respond to ARP requests for off-net hosts. Some vendors' routers will incorrectly respond to on-net ARP requests, which can create confusing network behavior. Some sites disable Proxy ARP, forcing end-nodes to have the proper subnet mask and router configurations. Other sites depend on Proxy ARP to add robustness to the network so that applications work even if the end-node is misconfigured. Use of Proxy ARP is mostly benign, although there may be a slight increase in ARP broadcast traffic, an increase in ARP cache table sizes, and possibly some decrease in performance.

Reasons that you may see a Proxy ARP reply for local IP ARP request include:

- Host IP may be misconfigured
- Host may have been moved to new subnet without changing its IP address
- Routers may be misconfigured
- Routing loops may exist
- Proxy ARP is enabled as a default on many routers

### 14.9.3 Information

#### 14.9.3.1 Only Device in Domain

This information message indicates that the device appears to be the only device in the specified NetBIOS domain. This can be caused by a misconfigured PC or a PC that is trying to join the wrong domain, because its domain name was mistyped when it was configured. When the PC does not see the domain for which it is configured, it becomes the Master Browser (MB) and will advertise this domain as a workgroup.

Domains are constructed to allow users to share information. If there is only one user in the domain, it is not adding any value to the network.

If the device is misconfigured, it might not be able to access the domains that you want it to be able to access (if access control or other security measures are in place). This condition will not adversely effect network operation. However, you need to be aware of any users that are setting up their own domains and workgroups, since Microsoft networking uses domains and workgroups for network administration. In domains, the network administrator has centralized control over network resources and users. Therefore, a single device in a domain can be a potential security hole.

## 14.10 Performance Tests

Your EtherScope Network Assistant provides a robust set of tools that allow you to turn up and test Ethernet networks independent of the core transport mechanism. The **Performance Tests** is an optional suite of tests (RFC 2544/ITO ES\_ITO\_OPT on the [Options](#) screen) and features a suite of RFC 2544 tests, a Jitter test, and the FrameBERT(tm) test. You can configure a test script and save it to the CompactFlash card. You can then easily reload the script and run the configured tests. Multiple configuration scripts can be created and saved. Refer to the [Performance Test Configuration](#) topic for more information.

**Note:** Network discovery is not active while the Performance tests are running.

### Remote Device

The Performance tests require a second (remote) device to communicate with on the network. The remote device can be a Fluke Networks instrument or a network switch in loopback mode (packet reflector). The remote device (but not a packet reflector) must be enabled to act as a remote device and must be configured with the same port number as the local device. The default port for the Performance tests is Port 3842. The default port for an EtherScope instrument configured as the remote device is Port 3842. You can change the port number (for an EtherScope or MetroScope acting as a remote device) on the [Instrument Settings - General](#) screen. Refer to the documentation of other devices for information on how to view/change the port number. You should also verify that the timeout parameter on the remote device is set appropriately (usually to match the setting on the sending device).

The following devices can serve as a remote device:

- Fluke Networks MetroScope Service Provider Assistant - Using a remote MetroScope server enables simultaneous upstream and downstream measurement of all Performance tests and the ITO Throughput test.

- Fluke Networks EtherScope Network Assistant V3 or later - Using a remote EtherScope server enables simultaneous upstream and downstream measurement of all Performance tests and the ITO Throughput test. The EtherScope server does not support the Jitter test.
- Fluke Networks OptiView Analyzer Series II or Series III - Using a remote OptiView Analyzer server enables simultaneous upstream and downstream measurement of all Performance tests and the ITO Throughput test. The OptiView Analyzer does not support the RFC 2544 Latency or Jitter test. Also, the maximum data rate is limited in OptiView series II.
- Fluke Networks OneTouch Series II Network Assistant - Using a OneTouch Network Assistant Series II server enables simultaneous upstream and downstream measurement of all Performance tests and the ITO Throughput test. The OneTouch Network Assistant does not support the RFC 2544 Latency or Jitter test. Measurement accuracy and maximum data rate are limited.
- Fluke Networks LinkRunner Pro Packet Reflector - Using a LinkRunner Pro Packet Reflector enables downstream measurement of all Performance tests and the ITO Throughput test. Set the filter mode to **FLUKE** for the packet type on the LinkRunner Pro reflector configuration mode screen. The LinkRunner Pro can be configured to swap or leave unchanged the received packet's source/destination MAC and/or source/destination IP. The EtherScope Network Assistant will attempt to automatically discover if the targeted device is a packet reflector, or an ITO server.
- Network Switch in loopback mode - This may be non-swapping, MAC swapping, or MAC/IP swapping Switch Loopback. Using a switch enables downstream measurement of all Performance tests and the ITO Throughput test. The switch can be configured to swap or leave unchanged the received packet's source/destination MAC and/or source/destination IP. The EtherScope Network Assistant will attempt to automatically discover if the targeted device is a packet reflector or an ITO server.

**Note:** When using a packet reflector remote device, there are no upstream results.

**Note:** Reflector mode will be determined automatically.

**Note:** When a performance test is run and the MAC address of the target is not known, the source MAC address will be used for the destination MAC. Similarly, if the destination IP address is not specified, the source IP will be used as the destination IP.

## RFC 2544 Test Suite

The suite of tests includes:

### Throughput

This test is a bidirectional test that compares the number of frames sent by one device to the number received by the second device. If the count of received frames is less than the count of sent frames, the sending rate is reduced and the test is rerun. The throughput is the fastest rate at which the count of test frames transmitted is equal to the number received.

Results are reported as Upstream (local to remote) and Downstream (remote to local). Results from this test will be used as default inputs for the Latency test below if a user chooses to run this test and the Latency test.

### Latency

This test measures the time delay of packets traveling through your network (between the local and remote instruments participating in the test) at various frame sizes as specified in the test configuration. The sending unit sends a stream of frames of a specified frame size to the remote

device at the specified throughput rate. The time at which the frames are fully transmitted is recorded (timestamp A). The remote unit returns the stream of frames, and the sending unit records the time at which the frames are received (timestamp B). The latency is timestamp B minus timestamp A. The RFC 2544 default specification is that the test is repeated 20 times. The test reports the minimum, average, and maximum values for each frame size.

### Loss

This test determines the highest frame rate that results in no lost frames on your network between the local and remote instruments participating in the test. The test sends a specific number of frames at a specific rate to the remote unit and then counts the frames that are received back.

The test begins by sending frames at the rate that corresponds to 100% of the maximum rate specified in the configuration. If any frames are lost, the transmission rate is decreased by the specified step size and the test is rerun. The test continues until there are two successive tests with no lost frames.

### Back to Back

This test measures the ability of the remote device to process back-to-back (as defined in RFC 1242) frames. A burst of frames with minimum inter-frame gaps is sent to the remote unit and the remote unit then sends them back. The count of the number of frames sent is compared to the number of frame received. If the count of transmitted frames is equal to the number of frames received, then the length of the burst is increased and the test is rerun. If the number of received frames is less than the number transmitted, the length of the burst is reduced and the test is rerun.

The back-to-back value is the number of frames in the longest burst that the remote unit will handle without the loss of any frames. The length of the test must be at least 2 seconds and is repeated N times (user configurable), with the average of the recorded values being reported.

### Jitter Measurement

Packets are sent to the remote unit in a continuous stream with the packets spaced evenly apart. The variance in the delay (due to network congestion, improper queuing, or configuration errors) is measured and reported.

### FrameBERT(tm) Bit Error Rate

This test does a bitwise inspection of in-stream frames, including the preamble/start frame delimiter, and does a comparison to the frame CRC. Errant frames are discarded. Discarded frames are assumed to have exactly one bit error for the purpose of calculating the Frame bit error rate.

## 14.10.1 Performance Test Configuration

You can set global test parameters that apply to all **Performance Tests** and devices, set parameters that apply to a single test, or set parameters that apply only to a single device selected for a specific test. Parameters set for a device override the parameters set for a test, and parameters set for a test override the global configuration settings made for all the **Performance Tests**. Some tests require parameters that apply only to the selected test; these parameters are set at the test level.

### Add Device

An added device will operate as the remote unit for the tests. Refer to the [Performance Tests](#) topic for a list of remote devices. You can add a device globally to all of the tests, or add a device to a single test. You can also add the same device multiple times and vary the configuration parameters in order to analyze the network performance under different conditions.

Highlight the **Performance Tests** line (to add a device to all tests) on the **Performance Tests** screen or highlight an individual test (e.g. **Jitter** to add a device to that test only) and tap the **Add Device** button. Use the pull-down menu in the **Remote Device** field of the **Add Device** screen to select a discovered device from the list, or select the **User Defined** entry and enter its IP address. Tap the **OK** button when finished. Repeat this procedure to add additional devices.

### Remove Device

Highlight a device and tap the **Remove Device** button to remove a device from the test.

**Note:** You cannot remove a device globally from all of the tests.

### Change Device

This feature allows you to configure the Performance Tests for one or more devices and then quickly substitute a different device without having to reconfigure the tests or save a separate script. This is useful if you are sequentially testing multiple networks using the same configuration parameters. You can load a single script, run the test on one network, change the device, and run the test on a different network.

When you select a device that has been added to a test, the **Add Device** button changes to **Change Device**. This allows you to enter a new IP address or use the pull-down menu to select a new device. All other configuration options remain unchanged. Enable the **Change all instances** check box if you want to substitute the new device in all tests where the old device is configured.

### Performance Tests Configuration

Highlight the **Performance Tests** line on the Performance Tests screen and tap the **Configure** button to set global parameters that will apply to all of the tests. Highlight an individual test and tap the **Configure** button to set parameters that apply only to the selected test, or highlight an individual device in the list under a test and tap the **Configure** button to set parameters that apply only to the selected device.

Press the **Defaults** button (on the **Configuration** screen) to restore the configuration to factory default settings. This will reset the configurations at the current level (global, individual test, or individual device) and below. For example, if you are on the **Jitter Configuration** screen and select **Defaults**, all devices under the **Jitter** test will be reset to their default level. The same devices listed under other tests will not be affected. You must tap the **Apply** button to make the changes take effect.

### Entering Values

Many fields on the configuration screens use a pull-down menu where you can select a value. You can also enter custom values; highlight the contents of the box and use the keyboard to enter a value that is within the acceptable range of values. If the entered value is outside of the permitted range, the value will be adjusted to the minimum or maximum value as appropriate. Use integers only, no decimal values. You can use shorthand to specify values. Use **K** to indicate Kbps, **M** for Mbps, and **G** for Gbps (e.g. 1M would be 1 megabits per second). For time based values, use **S**, **M**, or **H** (for Seconds, Minutes, and Hours), **ms** or **us** (for milliseconds and microseconds). The shorthand values are case insensitive.

### Global Configuration

Highlight the **Performance Tests** line and tap the **Configuration** button.



### Frame Defaults

- **Content** - Specify the content of the packets used for the tests. PRBS is a Pseudo Random Bit Stream. Incrementing Byte is a numerically incrementing byte stream (starting at 0, which is the RFC 2544 default).
- **Timeout** - Controls the hand-shaking timeout. If the timer expires, then it is assumed that contact has been lost between the two devices and the test aborts.  
**Note:** You can also set the timeout for the remote device. The timeout setting for an EtherScope Network Assistant or MetroScope Service Provider Assistant being used as a remote device is set on the **Instrument Settings - General Settings** screen. The remote device timeout is independent of the sending device, so you should verify its setting.
- **Size** - select the frame size to be sent (**RFC 2544 Sweep** cycles through frame sizes 64 - 1518 and Jumbo Sweep cycles through frame sizes 64 - 2024).  
**Note:** When [802.1Q](#) is enabled, 4 bytes (the VLAN tag) are added to frames that are transmitted by the EtherScope instrument. You will most likely notice this when selecting the frame size in pull-down menus (e.g. 64 -> 68, 1024 -> 1028, etc.).
- **Port** - You can use any port, but it must match on both devices.  
**Note:** The EtherScope Performance Tests default port setting is 3842. The port setting for an EtherScope Network Assistant or MetroScope Service Provider Assistant being used as a remote device is set on the **Instrument Settings - General Settings** screen.
- **Enable Priority Preservation** - If [802.1Q](#) is enabled for the instrument, then you can choose to count frames whose priority bits have not changed when sent through the network.
- **Priority** - If [802.1Q](#) is enabled for the instrument, then you can use the drop-down menu to set the user priority bits for transmitted frames.  
**Note:** When 802.1Q is enabled, 4 bytes (the VLAN tag) are added to frames that are transmitted by the EtherScope instrument. You will most likely notice this when selecting the frame size in pull-down menus (e.g. 64 -> 68, 1024 -> 1028, etc.).
- **DSCP** - (Differentiated Services Code Point) If [TOS with DSCP](#) is enabled, then you can set the DSCP parameter.

Tap the **Apply** button to save any configuration changes. All test and device results will be cleared.

**Note:** Any configuration changes made at this level will apply to all of the RFC 2544 tests, even if you have previously changed the default settings for an individual test.

**Note:** If the test traffic passes through a firewall, the selected port must also be open on the firewall.

### Throughput Configuration

Highlight the **RFC 2544 Throughput** line and tap the **Configuration** button.

You can override the global parameters set in the Performance Tests Frame Defaults by making changes at this level. Any changes made here will apply to the **Throughput** test only.

### Override Frame Defaults

Refer to the **Performance Tests Frame Defaults** section for a description of the parameters in this section.

### RFC 2544 Throughput Defaults

- **Duration** - The length, in seconds, of each trial. A trial is defined as the frame counting period at a given frame size and utilization level. There will be at least one trial for each selected frame size.
- **Maximum Rate** - Specify the maximum data rate for the trial.

**Note:** If the **Maximum Rate** is less than the **Pass/Fail Rate**, then the **Pass/Fail Rate** will be changed to match the **Maximum Rate**.

- **Measurement Accuracy** - Use this to select the *minimum* change in rate between successive iterations of the throughput test. The test will begin using the **Maximum Rate** value. If a small number of frames is lost, the test rate will be minimally reduced and the test rerun. The minimally reduced test rate is calculated by multiplying the current loss rate by **Measurement Accuracy** value; e.g.  $\text{nextRate} = \text{currentRate} * 0.995$  (99.5%). This process will continue until no frames are lost. This value affects the speed of the completion of this test; the lower the value in this field, the faster the test will complete.
- **Pass/Fail Rate** - Enable this check box if you want the results to indicate whether the test passed or failed. Pass/fail status is also indicated on the [Test Status LED](#). Use the pull-down menu to select the minimum rate (in bps) that the measured throughput must meet or exceed in order for the test to pass.

**Note:** If the **Pass/Fail Rate** is greater than the value entered in the **Maximum Rate** field, the Maximum Rate will be changed to match the **Pass/Fail** rate.

Tap the **Apply** button after making any configuration changes. All Throughput test and device results will be cleared.

**Note:** Any configuration changes subsequently made at the **Performance Tests Frame Defaults** level will override the configuration at this level.

## Latency Configuration

Highlight the **RFC 2544 Latency** line and tap the **Configuration** button.

You can override the global parameters set in the **Performance Tests Frame Defaults** by making changes at this level. Any changes made here will apply to the **Latency** test only.

### Override Frame Defaults

Refer to the **Performance Tests Frame Defaults** section for a description of the parameters in this section.

### RFC 2544 Latency Defaults

- **Duration** - The length, in seconds, of each trial. A trial is defined as the frame counting period at a given frame size and utilization level. There will be at least one trial for each selected frame size.
- **Rate** - Specify the data rate for the trial. The default setting is to use the results from the **Throughput** test to the maximum throughput rate. The **Latency** test is run at the maximum throughput rate or at the rate specified here.
- **Iterations** - The number of times that the test will be run. The test will be run the specified number of times at the specified frame rate.
- **Pass/Fail Latency** - Enable this check box if you want the results to indicate whether the test passed or failed. Pass/fail status is also indicated on the [Test Status LED](#). Use the pull-down menu to select the maximum time that the measured latency must not exceed in order for the test to pass.

Tap the **Apply** button after making any configuration changes. All Latency test and device results will be cleared.

**Note:** Any configuration changes subsequently made at the **Performance Tests Frame Defaults** level will override the configuration at this level.

### Loss Configuration

Highlight the **RFC 2544 Loss** line and tap the **Configuration** button.

You can override the global parameters set in the **Performance Tests Frame Defaults** by making changes at this level. Any changes made here will apply to the **Loss** test only.

### Override Frame Defaults

Refer to the **Performance Tests Frame Defaults** section for a description of the parameters in this section.

### Loss Defaults

- **Duration** - The length, in seconds, of each trial. A trial is defined as the frame counting period at a given frame size and utilization level. There will be at least one trial for each selected frame size.
- **Rate** - Specify the data rate for the trial.
- **Step Size** - The rate reduction (given as a percentage) between two trials.
- **Pass/Fail** - Enable this check box if you want the results to indicate whether the test passed or failed. Pass/fail status is also indicated on the [Test Status LED](#). Use the pull-down menu to select the minimum percentage of bits that must be received in order for the test to pass.

Tap the **Apply** button after making any configuration changes. All Loss test and device results will be cleared.

**Note:** Any configuration changes subsequently made at the **Performance Tests Frame Defaults** level will override the configuration at this level.

### Back to Back Configuration

Highlight the **RFC 2544 Back to Back** line and tap the **Configuration** button.

You can override the global parameters set in the **Performance Tests Frame Defaults** by making changes at this level. Any changes made here will apply to the **Back to Back** test only.

### Override Frame Defaults

Refer to the **Performance Tests Frame Defaults** section for a description of the parameters in this section.

### RFC 2544 Back to Back Defaults

- **Max Duration** - The maximum length, in seconds, of each trial. A trial is defined as the frame counting period at a given frame size and utilization level. There will be at least one trial for each selected frame size.
- **Min Duration** - The minimum length, in seconds, of each trial.
- **Rate** - Specify the data rate for the trial.
- **Iterations** - The number of times that the test will be run. The test will be run the specified

number of times at the specified frame rate.

- **Pass/Fail Duration** - Enable this check box if you want the results to indicate whether the test passed or failed. Pass/fail status is also indicated on the [Test Status LED](#). Use the pull-down menu to select the minimum time that the test must run in order for the test to pass.

Tap the **Apply** button after making any configuration changes. All Back to Back test and device results will be cleared.

**Note:** Any configuration changes subsequently made at the **Performance Tests Frame Defaults** level will override the configuration at this level.

### Jitter Configuration

Highlight the **Jitter** line and tap the **Configuration** button.

You can override the global parameters set in the **Performance Tests Frame Defaults** by making changes at this level. Any changes made here will apply to the **Jitter** test only.

#### Override Frame Defaults

Refer to the **Performance Tests Frame Defaults** section for a description of the parameters in this section.

#### Jitter Defaults

- **Duration** - The length, in seconds, of each trial. A trial is defined as the frame counting period at a given frame size and utilization level. There will be at least one trial for each selected frame size.
- **Rate** - Specify the data rate for the trial.
- **Pass/Fail Jitter** - Enable this check box if you want the results to indicate whether the test passed or failed. Pass/fail status is also indicated on the [Test Status LED](#). Use the pull-down menu to select the maximum time that the measured jitter must not exceed in order for the test to pass.

Tap the **Apply** button after making any configuration changes. All Jitter test and device results will be cleared.

**Note:** Any configuration changes subsequently made at the **Performance Tests Frame Defaults** level will override the configuration at this level.

### Bit Error Rate Configuration

Highlight the **Bit Error Rate** line and tap the **Configuration** button.

You can override the global parameters set in the **Performance Tests Frame Defaults** by making changes at this level. Any changes made here will apply to the **Bit Error Rate** test only.

#### Override Frame Defaults

Refer to the **Performance Tests Frame Defaults** section for a description of the parameters in this section.

#### Bit Error Rate Defaults

- **Duration** - The length, in seconds, of each trial. A trial is defined as the frame counting

period at a given frame size and utilization level. There will be at least one trial for each selected frame size.

- **Rate** - Specify the data rate for the trial.
- **Pass/Fail Bit Error Rate** - Enable this check box if you want the results to indicate whether the test passed or failed. Pass/fail status is also indicated on the [Test Status LED](#). Use the pull-down menu to select the maximum rate that the test must not exceed in order to pass.

Tap the **Apply** button after making any configuration changes. All Jitter test and device results will be cleared.

**Note:** Any configuration changes subsequently made at the **Performance Tests Frame Defaults** level will override the configuration at this level.

### Remote Device Configuration

These tests require a remote device or a packet reflector (downstream only results) to communicate with on the network. For a list of devices that can be used as a remote, refer to the [Performance Tests](#) topic. The remote device must be enabled to act as a remote device and must be configured with the same port number as the local device. The default port for the Performance tests is Port 3842. You should also verify that the timeout parameter on the remote device is set appropriately (usually to match the setting on the sending device).

The Performance tests require a second (remote) device to communicate with on the network. The remote device must be enabled to act as a remote device and must be configured with the same port number as the local device. The default port for the Performance tests is Port 3842. The default port for a EtherScope instrument configured as the remote device is Port 3842. You can change the port number on the [Instrument Settings - General](#) screen. Refer to the documentation of other device for information on how to view/change the port number. You should also verify that the timeout parameter on the remote device is set appropriately (usually to match the setting on the sending device).

### Using Scripts to Save and Load Configurations

After configuring the Performance Tests, you can save the configuration in a file that is stored on the CompactFlash. You can then load the script at a later date and the complete configuration, including the test selections, test and device configurations, and which devices are selected for each test. You can save multiple configuration scripts.

To save configuration information in a script, select the **Save Script** button on the **Performance Tests** screen. From the **Save Script** screen, tap the **Save As** button. Enter a descriptive name on the **New Performance Test** popup and select **OK**. The script will now be saved on the CompactFlash.

**Note:** Scripts are stored on the CompactFlash in the **Performance Tests** directory, however the filename used to save the script is generated by the EtherScope application. This allows you to use a more descriptive name than might otherwise be allowed by the file system.

To load a script, select the **Load Script** button on the **Performance Tests** screen. On the **Load Script** screen, select the script that you wish to load and tap the **Load** button. The configuration information will be loaded and the Title bar of the **Performance Tests** screen will show the script name. You can now **Start** the tests.

## 14.10.2 Running Performance Tests

You can select which tests are to be run by using the check boxes next to each test on the **Performance Tests** screen. An enabled box indicates that the test will be run when you tap the **Start** button. If you enable the check box next to the **Performance Tests** line, then all tests will be run against the devices listed below each test. Clearing the **Performance Tests** check box will disable all tests. You can enable (or disable) a single test and enable selected devices under each test.

### Results

The **Status** column of the **Performance Tests** screen shows whether results are available for a test or a particular device.

Highlight a test and tap the **Results** button to view the output of a test. You can also tap the **Results** button when a test is running to view the progress.

As appropriate, the preview pane of the **Results** screen will have radio buttons to select the **Display Mode** (**BPS** - Bits/Sec or **FPS** - Frames/Sec; **Upstream** or **Downstream**) and **View Mode** (**Table** or **Graph** - when one of the sweep modes is enabled).

At each test level, the pass/fail status (only available if enabled) is a summary of all of the devices tested. If one device test doesn't pass, the summary at the test level will indicate **Failed**. Likewise, the overall pass/fail status at the **Performance Test** level is a summary of all of the individual test results.

## 14.11 ITO Tests

The **ITO Tests** is an optional suite of tests (RFC 2544/ITO ES\_ITO\_OPT on the [Options](#) screen). Your EtherScope Network Assistant supports two ITO tests:

### Traffic Generator

The [Traffic Generator](#) consists of user selectable parameters that control packets transmitted to the network. You can select packet size, packet type, destination address (if applicable), transmit rate and transmit duration. Traffic generation can be manually started and stopped.

### Throughput Test

The [Throughput Test](#) is a bidirectional test (unidirectional when using a packet reflector) that compares the number of frames sent by one device to the number received by the second device. The achieved throughput rate is calculated using the frame size, received frame count, and the duration of the test.

### 14.11.1 Traffic Generator

The **Traffic Generator** test is an optional application (**Internet Throughput/Traffic Generator ES\_ITO\_OPT** on the [Options](#) screen) that allows you generate network traffic. Expand the

**Throughput Test** on the **Test Results** screen and highlight **Traffic Generator**. Tap the **Details** button to configure and run the test.

You can use the **Traffic Generator** to create different loads that can be used to test network performance. The protocol used, frame size, rate, and utilization are configurable along with the type of traffic, e.g. Broadcast, Multicast, or to a specific Device (Unicast). Traffic can be generated to devices on the local network or to devices specified outside of the local network.

**Caution:** Improper use of the **Traffic Generator** can cause serious network performance problems. The tool should be used with caution and by someone with a good understanding of the network.

## Frame Description

**Broadcast** - Select this for loading network and hosts on the local broadcast domain (up to the first router). Traffic is sent to hosts in the local broadcast domain. The destination MAC address of the frame is set to FFFFFFFF. All devices will process this packet.

**Multicast** - Select this for network loading only (no hosts). Traffic goes to the Host NIC card and stops. It is not processed by the NIC card. The frame is sent with a destination MAC Multicast address. The packet is forwarded by switches and routers. No other devices will process it.

**Note:** If an **IP/ICMP** or **IP/UDP** frame **Type** is selected, you can enter a multicast address in the range of 224.0.0.0 - 239.255.255.255. After entering an IP address and navigating away from the **IP** field, the **MAC** address will be automatically generated.

**Unicast** - Send traffic to a designated device. The choices vary by protocol **Type** selected. For IP protocols, the IP address or MAC address can be specified. Use the pull-down menus in the IP or MAC fields to select from the list of discovered devices and the MAC address will be automatically inserted.

**Note:** If you select a device that is not on your local subnet, or any device that the MAC address is unknown, the MAC address of the default router will be used.

If you select **User Defined** from the list, you can highlight the IP or MAC address fields and manually enter the addresses.

**Type** - Select protocol that is sent:

- **Benign Ethernet** (Ethernet type 1996 hexadecimal) - A legal, unroutable Ethernet frame with random data.
- **Benign LLC** - A legal, unroutable 802.2 frame that has unused DSAP and SSAP values.
- **NetBEUI** - NetBIOS over 802.2 (NetBEUI) with random data.
- **Benign IP** - A routable IP packet that has an unused value in the protocol field and random data.
- **IP/ICMP Echo** - A legal PING request (may cause bidirectional traffic).
- **IP/UDP Discard** - This packet should be discarded by any host that is listening to UDP ports.
- **IP/UDP CharGen** - Targeted at the "Character Generator" port. This service may not be implemented on all systems (may cause bidirectional traffic).
- **IP/UDP NFS** - This packet contains sample data to and from UDP ports that are often used for NFS traffic containing random data.
- **IP/UDP NetBIOS** - This packet contains sample data to and from the UDP ports used by NetBIOS over TCP/IP containing random data.

**Size** - Use the drop-down list to select the frame size (48 - 2024 bytes).

**Note:** When [802.1Q](#) (VLAN tagging) is enabled, 4 bytes (the VLAN tag) are added to frames that



are transmitted by the EtherScope instrument. You will most likely notice this when selecting the frame size in pull-down menus (e.g. 64 -> 68, 1024 -> 1028, etc.).

**Generate FCS errors** - create Frame Check Sequence errors.

**TTL** (Time to Live) - enter the maximum number of hops that the frame will encounter before being discarded. Each network device that handles the frame will decrement the count.

## Rate and Duration

Select between **Util (%)** or **Fr/Sec** and then use the drop-down list to select the value. Then select between **Seconds** and **Frames** and use the drop-down list to select the value.

Once you have configured the test values, tap the **Start** button to begin the test. The Preview pane shows the total number of frames sent, a summary table of the type and quantity of frames (**Unicast**, **Multicast**, **Broadcast**), **Collisions**, **Errors**, and **Total** frames (as a percent of bandwidth) seen. There is also a small graph showing the summary results.

**WARNING:** Sending any of these frames and packets directly to a host may cause unexpected and undesirable results that may include causing that computer system to fail.

**WARNING:** Sending IP traffic directly to a host may cause ICMP traffic to be sent back through the network. This traffic may have undesirable effects on the target node and/or intermediate switches and routers.

**WARNING:** When the Traffic Generator feature is used to send traffic through a router, and the traffic overloads the router, the router can lose its ability to forward traffic, and remote user interface sessions will disconnect.

## 14.11.2 Throughput Test

The **Throughput Test** allows you to measure the bidirectional data flow between your EtherScope Network Assistant and a remote device. The test runs on links up to 1 Gbps.

### Remote Device

The Throughput Test requires a second (remote) device to communicate with on the network. The remote device must be enabled to act as a remote device and must be configured with the same port number as the local device. The default is Port 3842. The default port for a EtherScope instrument configured as the remote device is also Port 3842. You can change the port number on the [Instrument Settings - General](#) screen. Refer to the documentation of other devices for information on how to view/change the port number. You should also verify that the timeout parameter on the remote device is set appropriately (usually to match the setting on the sending device).

The following devices can serve as a remote device:

- Fluke Networks MetroScope Service Provider Assistant - Using a remote MetroScope server enables simultaneous upstream and downstream measurement of throughput.
- Fluke Networks EtherScope Network Assistant V3 - Using a remote EtherScope V3 server enables simultaneous upstream and downstream measurement throughput.
- Fluke Networks OptiView Analyzer Series II or Series III - Using a remote OptiView Analyzer server enables simultaneous upstream and downstream measurement of throughput. The maximum data rate is limited in OptiView series II.
- Fluke Networks OneTouch Series II Network Assistant - Using a OneTouch Network Assistant

Series II server enables simultaneous upstream and downstream measurement throughput. Measurement accuracy and maximum data rate are limited.

- **Fluke Networks LinkRunner Pro Packet Reflector** - Using a LinkRunner Pro Packet Reflector enables downstream measurement only of the throughput test. The EtherScope Network Assistant will attempt to automatically discover if the targeted device is a packet reflector, or an ITO server.
- **Network Switch in loopback mode** - This may be non-swapping, MAC swapping, or MAC/IP swapping Switch Loopback. Using a switch enables downstream measurement of all Performance tests and the ITO Throughput test. The switch can be configured to swap, or leave unchanged, the received packet's source/destination MAC, and/or source/destination IP. The EtherScope Network Assistant will attempt to automatically discover if the targeted device is a packet reflector or an ITO server.

**Note:** When using a packet reflector remote device, the upstream results are dashed out in GUI results and reports. You do not need to configure a port for a packet reflector (Fluke Networks LinkRunner Pro or network switch) used as a remote device.

## Configuring the Throughput Test

### Frame Description

- **Remote Device** - use the pull-down menu to select a device to be used as the remote unit or select **User Defined** and enter the IP address of a device to be used as the remote unit.  
**Note:** When configuring for a packet reflector that is directly connected (without going through a switch or router) and does not have a configured IP address, use 127.xxx.xxx.xxx (where x can be any integer). This indicates to the EtherScope instrument to send an unrouted and unswitched packet for the test.
- **Content** - select what the data stream will contain (**PRBS** is a Pseudo Random Bit Stream).
- **Timeout** - set the length of time that the instrument will wait for a response from the remote test unit before terminating the test.
- **Size** - select the frame size to be sent (**Sweep** cycles through all the frame size choices).  
**Note:** When [802.1Q](#) (VLAN tagging) is enabled, 4 bytes (the VLAN tag) are added to frames that are transmitted by the EtherScope instrument. You will most likely notice this when selecting the frame size in pull-down menus (e.g. 64 -> 68, 1024 -> 1028, etc.).
- **Port** - For most devices, the port number can be any number, but it must match on both devices (Port 3842 is the default selection for the EtherScope instrument). The **Port** selection must be 3842 for communication with a OneTouch Network Assistant.

### Rate and Duration

- **Bits/Second** (transmit speed) - The maximum rate is determined by the link speed, duplex, and maximum transmit capabilities of the Service Provider Assistant.
- **Seconds** - Select the time period for the test to run.

## Running the Throughput Test

Tap the **Start** button to initiate the test. The preview pane gives configuration details of the **Remote Device**, a **Frame Description** of the frames sent by the EtherScope Network Assistant, and the **Rate and Duration** of the test. A table of results (use the radio button on the Title bar to switch to a graphical representation) shows the results of the test. The **Upstream Results** shows the number of **Frames Sent** by the local device, the number of **Frames Recd** (Received) by the remote device, the upstream data **Rate**, and the **Percent Loss**. The **Downstream Results** shows the same parameters but for traffic from the remote device to the local device.

**Note:** A busy network can limit the data rate.

**Note:** The **Throughput Test** uses the default router (see [TCP/IP Settings](#)) to reach off-net (i.e.

non-local) routed devices.

## 15 Add Device

The Network Assistant discovers devices on the local broadcast domain to which it is connected. It is possible that a device in the local broadcast domain is not discovered because it does not generate much network traffic or does not respond to the active discovery methods employed by the instrument. You can add a device (including a device that is outside of the local broadcast domain) to the discovery database by using **Add Device**. A device that has been added to the database will remain until it is removed.

**Note:** For [Device Discovery](#) to actually find an added device, there must be a network route from the Network Assistant to the device.

A common network design is to configure some or all of the network switches as part of a management VLAN. The Network assistant will only discover devices in the local broadcast domain to which it is connected. You can use the **Add Device** function to add those switches that are outside of the local broadcast domain. This provides port/slot/VLAN visibility for connectivity verification, accurate [Nearest Switch](#) reporting, and troubleshooting purposes.

The **Add Device** button is located on the [Device Discovery](#), [User-defined Devices](#), and [Key Devices](#) screens. You must enter the device's IP address. If you do not enter the MAC address, the instrument will use 000000000000. If the added device is an SNMP agent, the instrument will discover the MAC address. User-added devices are saved in the instrument database and will persist between troubleshooting sessions. You can use [Edit user-defined devices](#) to remove a device from the list.





## 16 Device Details

Highlight a device (e.g. in the [Device Discovery](#) list) and select the **Details** button to bring up the **Device Details - Overview** screen. This gives you specific information about the device, access to **Interface** (for Routers and Switches) information, and network tools that you can run that give you more information or help you troubleshoot your network.


**Note:** The **Interfaces** screen (accessible when a router or switch is selected) shows configured VLANs with a port number of 0. Highlight the VLAN and the preview screen shows the IP address of the port and other configuration information.

**Note:** The preview screen of a switch port that is performing Layer 3 switching will show the IP address of the port.

**Note:** The **Interfaces** screen (accessible when a router or switch is selected) has an 802.1X column that uses icons to show 802.1X security for each interface. The icons indicate the following interface status:

-  - 802.1X security is not available
-  - 802.1X security can not be determined
-  - 802.1X security is enabled but authentication has not been established
-  - 802.1X security is enabled and the connected device has established authentication

## 17 Network Tools

Your EtherScope instrument incorporates a set of utilities that can be used for network troubleshooting and configuration. These **Network Tools** are available by tapping the  icon on the Task bar, or tools

that are appropriate to a particular test can be accessed directly from the Preview pane of a test.

The tools that are available are:

[Ping](#)  
[Trace Route](#)  
[Web Browser](#)  
[Telnet](#)  
[SSH Telnet](#)  
[Terminal](#)  
[FTP](#)  
[TFTP](#)  
[xDP Reporter](#)  
[Report](#)

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

**Note:** Not all of the tools are available for every device.

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

## 17.1 Ping

**PING** (Packet InterNet Groper) is a simple IP query and response process. Ping is an easy method to verify IP-level connectivity between the EtherScope instrument and another device. Highlight a device in a device list and run the **Ping** tool or select the tool and enter the IP address of the device.

## 17.2 Trace Route

Trace Route is a tool that determines the IP path used to reach a device. Trace Route shows the number of hops and the IP addresses of devices used to reach the destination device. Highlight a device in a device list and run the **Trace Route** tool or select the tool and enter the IP address of the device.

## 17.3 Trace Switch Route

You can use **Trace Switch Route** to determine the MAC data path between your EtherScope instrument and another device. The MAC data path includes all devices that have a MAC address on the switched LAN. This includes the starting and ending devices and any switches in the path. Highlight a device in a device list and run the **Trace Switch Route** tool or select the tool and enter the IP address of the device.

**Note:** The proper SNMP community strings must be configured for the Trace Switch Route to work. Refer to the [Instrument Settings - Security](#) topic for more information on configuring SNMP community strings.

**Note:** The test may not work if the switch is not supported by the instrument or if the switch is part of a management VLAN.

## 17.4 Traffic Generator

The **Traffic Generator** test is an optional application (**Internet Throughput/Traffic Generator ES\_ITO\_OPT** on the [Options](#) screen) that allows you generate network traffic. Expand the **Throughput Test** on the **Test Results** screen and highlight **Traffic Generator**. Tap the **Details** button to configure and run the test.

You can use the **Traffic Generator** to create different loads that can be used to test network performance. The protocol used, frame size, rate, and utilization are configurable along with the type of traffic, e.g. Broadcast, Multicast, or to a specific Device (Unicast). Traffic can be generated to devices on the local network or to devices specified outside of the local network.

**Caution:** Improper use of the **Traffic Generator** can cause serious network performance problems. The tool should be used with caution and by someone with a good understanding of the network.

### Frame Description

**Broadcast** - Select this for loading network and hosts on the local broadcast domain (up to the first router). Traffic is sent to hosts in the local broadcast domain. The destination MAC address of the frame is set to FFFFFFFFFF. All devices will process this packet.

**Multicast** - Select this for network loading only (no hosts). Traffic goes to the Host NIC card and stops. It is not processed by the NIC card. The frame is sent with a destination MAC Multicast address. The packet is forwarded by switches and routers. No other devices will process it.

**Note:** If an **IP/ICMP** or **IP/UDP** frame **Type** is selected, you can enter a multicast address in the range of 224.0.0.0 - 239.255.255.255. After entering an IP address and navigating away from the **IP** field, the **MAC** address will be automatically generated.

**Unicast** - Send traffic to a designated device. The choices vary by protocol **Type** selected. For IP protocols, the IP address or MAC address can be specified. Use the pull-down menus in the IP or MAC fields to select from the list of discovered devices and the MAC address will be automatically inserted.

**Note:** If you select a device that is not on your local subnet, or any device that the MAC address is unknown, the MAC address of the default router will be used.

If you select **User Defined** from the list, you can highlight the IP or MAC address fields and manually enter the addresses.

**Type** - Select protocol that is sent:

- **Benign Ethernet** (Ethernet type 1996 hexadecimal) - A legal, unroutable Ethernet frame with random data.
- **Benign LLC** - A legal, unroutable 802.2 frame that has unused DSAP and SSAP values.
- **NetBEUI** - NetBIOS over 802.2 (NetBEUI) with random data.
- **Benign IP** - A routable IP packet that has an unused value in the protocol field and random data.
- **IP/ICMP Echo** - A legal PING request (may cause bidirectional traffic).
- **IP/UDP Discard** - This packet should be discarded by any host that is listening to UDP ports.
- **IP/UDP CharGen** - Targeted at the "Character Generator" port. This service may not be implemented on all systems (may cause bidirectional traffic).
- **IP/UDP NFS** - This packet contains sample data to and from UDP ports that are often used for NFS traffic containing random data.
- **IP/UDP NetBIOS** - This packet contains sample data to and from the UDP ports used by NetBIOS over TCP/IP containing random data.

**Size** - Use the drop-down list to select the frame size (48 - 2024 bytes).

**Note:** When [802.1Q](#) (VLAN tagging) is enabled, 4 bytes (the VLAN tag) are added to frames that are transmitted by the EtherScope instrument. You will most likely notice this when selecting the frame size in pull-down menus (e.g. 64 -> 68, 1024 -> 1028, etc.).

**Generate FCS errors** - create Frame Check Sequence errors.

**TTL** (Time to Live) - enter the maximum number of hops that the frame will encounter before being discarded. Each network device that handles the frame will decrement the count.

## Rate and Duration

Select between **Util (%)** or **Fr/Sec** and then use the drop-down list to select the value. Then select between **Seconds** and **Frames** and use the drop-down list to select the value.

Once you have configured the test values, tap the **Start** button to begin the test. The Preview pane shows the total number of frames sent, a summary table of the type and quantity of frames (**Unicast**, **Multicast**, **Broadcast**), **Collisions**, **Errors**, and **Total** frames (as a percent of bandwidth) seen. There is also a small graph showing the summary results.

**WARNING:** Sending any of these frames and packets directly to a host may cause unexpected and undesirable results that may include causing that computer system to fail.

**WARNING:** Sending IP traffic directly to a host may cause ICMP traffic to be sent back through the network. This traffic may have undesirable effects on the target node and/or intermediate switches and routers.


**WARNING:** When the Traffic Generator feature is used to send traffic through a router, and the traffic overloads the router, the router can lose its ability to forward traffic, and remote user interface sessions will disconnect.

## 17.5 Web Browser

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

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

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

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

## 17.6 Telnet

Telnet is a program that lets you access a remote computer. When you run **Telnet**, the **Set Tool Target** popup opens where you can enter the IP address of the device to which you are trying to connect (the IP address is automatically entered if a device is already selected on a test screen). An

EtherScope Console window opens where you can log in to the device and then work from the instrument as if it were a terminal that is hardwired to the remote device.

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


## 17.7 SSH Telnet

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

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

## 17.8 Terminal

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

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

## 17.9 FTP

Opens an **FTP** (File Transfer Protocol) session with a device. Highlight a device in a device list and run the **FTP** tool or select the tool and enter the IP address of the device. **FTP** can be used to move files between computers.

## 17.10 TFTP

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

Trivial File Transfer Protocol is a simple form of the File Transfer Protocol (FTP). TFTP uses the User Datagram Protocol (UDP) and provides no security features.

## 17.11 xDP Port Reporter

The xDP Port Reporter parses all Cisco Data Protocol (CDP) and Link Layer Discovery Protocol (LLDP) packets received by the application. From each packet, the following information is extracted and displayed:

**EtherType** - CDP or LLDP packet

**Device ID** - the SNMP system name of the packet originator



**Addresses** - the IP address of the packet originator

**Platform** - the name of the device sending the packet

**Port ID** - the identity of the port (on the originating device) used to transmit the packet

**Vlan ID** - the identity of the VLAN of the packet originator

## 17.12 Report

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

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

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

You can also remotely generate (and then view) reports using the [Remote Access](#) feature of the instrument. From the EtherScope Web Server home page, tap the **Reports** button. The EtherScope reports web page will display. Select the report that you wish to generate from the menu under **EtherScope Real-Time Reports**. The report will be displayed in your web browser (Microsoft Internet Explorer). Reports generated by this method are not stored on the CompactFlash.

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

### User Supplied Graphic

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

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

### User Supplied Comment


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

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

### Job Comment

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

### Viewing Reports

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

Reports stored on the CompactFlash can be viewed on your PC by using the [Remote Access](#) feature of the instrument. With the CompactFlash containing the reports installed in the instrument, from the EtherScope Web Server home page, tap the **Reports** button. The EtherScope reports web page will display. Select the **View Saved Reports** link to see the list of saved reports. Select the report that you wish to view and it will be displayed in your web browser.

# Index

## - 8 -

802.1Q 4, 5, 31, 40  
802.1X Authentication 7  
802.1X Configuration 4, 6, 25  
802.1X security 8, 53  
802.3af 29

## - A -

Add an undiscovered device 53  
Auto-negotiation of link 7

## - B -

Battery 13  
Bit Error Rate Test 40  
Browser 56

## - C -

Cable test 25  
Cable Testing 26  
Cable Toner 26  
Calibrate the touch screen 13  
Cisco Discovery Protocol 57  
Clock 14  
Community strings 6, 8  
Configuration 25  
Configure 4  
    Ethernet settings 7  
Configure Performance Tests 40  
Configure security settings 8  
Configure TCP/IP settings 4  
Configuring Performance Tests 42  
Configuring Service Performance Tests 16  
Connection Log 4, 7  
Copyrights 25

## - D -

Date 14

Denial of Service 9  
Device appears in multiple categories 32  
Device count 32  
DHCP Log 7  
Differentiated Services Code Point 5, 40  
DiffServ 5, 40  
DSCP 5

## - E -

Enable Options 10  
Enable RFC 2544/ITO Throughput remote 9  
Enabling Options 8  
Errors 37  
Ethernet Settings 4

## - F -

Fast-connect mode 9  
Fiber optic 2, 3, 10, 25  
Fiber Optic Cable Testing 26  
Fiber option 10  
File Manager 58  
Forced link setting 7  
FrameBERT 40  
Front panel 11  
FTP 53

## - G -

Gigabit fiber 2, 3, 10, 25  
GNU Public License 25  
GPL 25

## - H -

Hardware version 10

## - I -

Icons 1  
Information 37  
Instrument Security 4, 8  
Interfaces 53  
Internet access 23, 56  
Internet Throughput 51

Internet Throughput Option 10  
IP configuration 4  
IP Network 33  
IPX Network 33  
ITO tests 8  
ITO Throughput test 9

## - J -

Jitter Test 40  
Join a VLAN 31

## - K -

Key Code 10  
Konqueror browser 56

## - L -

LAN Tests 1, 3  
Language settings 12  
Latency Test 40  
Layer 3 Switching 53  
LEDs 11  
Light and Power settings 12  
Link Layer Discovery Protocol 57  
Linux 25  
LLDP 57  
Loading Scripts 16, 42  
Locate Cable 26  
Loss Test 40

## - M -

MAC address 7

## - N -

NetBIOS domain 33

## - O -

Off segment devices 53  
Operating mode 11  
Options 10

## - P -

Paced Discovery 9  
Packet errors 11, 30  
Password protection 8  
Passwords 4, 25  
Performance Tests 40  
Ping 53  
PoE 29  
Power over Ethernet 29  
Power saving mode 13

## - R -

Radio Card 3  
Remote access to the EtherScope 23  
Remote statistics 30  
Removing the Radio Card 3  
Report Viewer 58  
Reports 53, 58  
RFC 2544 tests 8, 9, 40

## - S -

Saving Scripts 16, 42  
Scripts 16, 42  
Security 4  
Server response tool 14  
Set the RFC 2544/ITO Throughput port number 9  
Set the SNMP System Name 9  
Set the time/date 14  
SNMP Community Strings 4, 6, 8, 25  
SNMPv1 6  
SNMPv2 6  
SNMPv3 6  
Software update 24  
Software version 10  
Sort Device List 32  
SSH Telnet 53  
Status LEDs 11  
Suspend mode 13  
Switch LAN / WLAN Tests 1, 3

## - T -

Tagged VLANs 5  
TCP trace route 14  
TCP/IP Configuration 4  
Telnet 53  
Terminal 53  
TFTP 53  
Throughput 51  
Throughput Test 10, 40  
Throughput tests 8  
Time 14  
Toner 26  
TOS 5  
Touchscreen calibration 12  
Trace Route 53  
Trace Switch Route 53  
Trademarks 25  
Traffic Generation 10  
Traffic Generator 8, 49, 53, 55  
Transmission errors 11, 30  
Turn off the instrument 13  
Type of Service 5

## - U -

Undiscovered devices 53  
User defined devices 9  
Utilization 11, 30

## - V -

Vendor prefix 9  
Version settings 10  
VLAN Discovery 34  
VLAN Statistics 31, 34  
VLAN Tagging 4, 31

## - W -

Warnings 37  
Web browser 23, 53  
WLAN Tests 1, 3

## - X -

xDP Port Reporter 53  
xDP Reporter 57

