FLUKE networks®

NetTool™ Series II

Inline Network Tester

Users Manual

September 2006, Rev. 1, 06/2007

LIMITED WARRANTY AND LIMITATION OF LIABILITY

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

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

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

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

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

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

4/04

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

Table of Contents

List of Tables

List of Figures

Chapter 1
Introduction

Using This Manual

This Users Manual is supplied with the NetTool™ Series II Inline Network Tester to help you learn to use your new tester quickly and more efficiently.

The manual introduces you to the key features and operation of the tester and shows you how to set it up and use it to resolve troublesome desktop-to-network connectivity problems. Descriptions of test functions, along with illustrations of typical menus and result screens, are provided to assist you with the operation of the tester and interpretation of results.

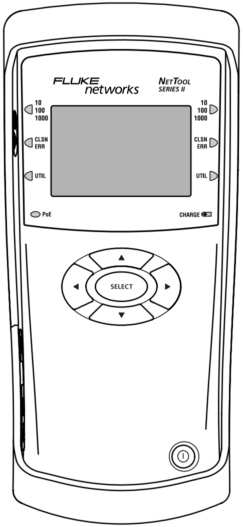
NetTool Series II Inline Network Tester

The NetTool Series II Inline Network Tester (hereafter referred to as the tester) is a handheld tester that combines cable, network, and PC configuration testing into a single device. The tester is designed to speed your frontline network troubleshooting, “moves, adds & changes”, and desktop-to-network connectivity work.

The tester provides support for monitoring and testing 10/100/1000 Mb Ethernet LANs. It also gives you the ability to check for the presence of Power over Ethernet (PoE) on an Ethernet LAN, identify supply pairs, and measure the associated electrical voltages and currents.

The tester is available in the following models:

- NetTool Series II Pro: provides single-ended testing and inline testing between two devices, such as a PC and a switch. Also includes the NetProve application, a Ping function, a Reporter function that enables you to create and save test reports, and the capability to display VLAN traffic and CDP (Cisco Discovery Protocol), LLDP (Link Layer Discovery Protocol), and EDP (Extreme Discovery Protocol) information.
- NetTool Series II Pro VoIP: includes all of the features available in the NetTool Series II Pro model plus the ability to monitor VoIP (Voice over IP) service.
- NetTool Series II Pro NetSecure: includes all of the features available in the NetTool Series II Pro model plus the ability to 802.1X authenticate and log authentication activity, and monitor ports. The NetSecure option requires a NetTool Series II with software version 4.50 or greater.



emt06f.eps

Figure 1-1. NetTool Series II Inline Network Tester

Features and Functions

The tester's features and functions enable you to do the following:

- Verify the reliability of cabling and cabling installations by testing for length, shorts, split pairs or opens, including pin-to-pin wiremapping.
- Check a PC's configuration and identify its network.
- Verify connectivity to network devices (PCs, routers, servers, VoIP phones, and printers).
- "Listen" to traffic and gather information about PC and link configurations, network health, and network key devices.
- Detect and measure PoE voltage and current for both power-supplying equipment (PSE) and powered devices (PDs).
- Verify service and monitor call quality on Voice over IP (VoIP) links.
- Generate resource reports to document network and PC performance.
- Verify Ping and TCP connectivity and response times to critical network resources (NetProve).
- Verify 802.1X authentication through inline transaction loggin as well as client emulation.
- Detect and log malware/spyware accesses inline between network and client PCs.

Care and Maintenance

Treat your tester with care to ensure the best performance. Clean the tester and LCD carefully by gently wiping them with a soft, slightly damp cloth. Never use harsh detergents, solvents, or abrasive cleaners.

Safety and Operational Information

To operate your tester safely, observe the usage and disposal warnings represented by the symbols that are found on your tester. The meanings of these symbols are given in the following table.

Table 1-1. International Electrical Symbols

⚠	Warning or Caution: Risk of damage or destruction to equipment or software.
⊘	This equipment not for connection to public communications networks, such as active telephone systems.
🗑	Do not put products containing circuit boards into the garbage. Dispose of circuits boards in accordance with local regulations.

Package Contents

Take a moment to check the shipping container to make sure that the contents match the list below. If any item is missing, contact your place of purchase.

- Four (4) AA alkaline batteries
- USB cable
- RJ-45 CAT5 cable (four feet long)
- WireView Cable ID #1
- *Getting Started Guide*
- CD-ROM, containing this *Users Manual*, a *Getting Started Guide*, and NetTool Connect (for updating the tester’s software)

NetSecure Bundle

- NetTool Series II (see above)
- IntelliTone
- Case
- NetSecure option (includes Port Monitor and 802.1X authentication and logging)

Optional Accessories

You can separately purchase the following accessories for your tester from Fluke Networks or from your local distributor:

- A/C adapter
- Rechargeable NiMH batteries
- Power kit, which includes an AC adapter and NiMH batteries

Registering the Tester

Please take the time to register your tester. Registration offers you access to support, training, software, and product updates.

Go to the Fluke Networks website at http://www.flukenetworks.com. From the **Find your product** list box, select **NetTool Inline Network Tester**. On the product page, click the **register** link and follow the instructions to log in and register your tester online.

Service and Adjustment

Service and adjustment of your tester should be performed by trained Fluke Networks service personnel only.

If you experience a problem with the tester, visit the Fluke Networks website at http://www.flukenetworks.com/NetTool and click the **Support and Downloads** link. You can also send email to support@flukenetworks.com, or contact your nearest Fluke Networks Service Center to report the problem (see "Contacting Fluke Networks" for a list of telephone numbers).

If the tester requires repair, service center personnel will provide you with shipping information and repair prices. If the tester is covered under warranty, it will be promptly repaired or replaced (at Fluke Networks' option) and returned to you, postage paid, at no charge. See the registration card for warranty terms. If the warranty has lapsed, Fluke Networks will repair the tester for a fixed fee and return it, postage paid, to you.

Contacting Fluke Networks

ℹ http://www.flukenetworks.com

✉ support@flukenetworks.com

☎ +1-425-446-4519

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

Visit our website for a complete list of phone numbers.

NetTool Connect

The CD-ROM that is packaged with the tester includes NetTool Connect, a PC-based software utility program.

NetTool Connect enables you to do the following:

- Generate HTML or PDF reports from live or saved data (click **Reports**)
- Download, edit, store, and upload device catalogs for the tester (click **NetProve**)
- Setup and upload port monitor configuration (Port Monitor is part of the NetSecure option)
- Configure and upload 802.1X authentication (802.1X is part of the NetSecure option)
- Update the tester’s software (click **Update**)
- Get screen shots (click **Capture**)
- Add your own splash screen (click **Personalize**)
- Set the date and time (click **Date/Time**)
- Enter a key code if you have purchased options for the tester (click **Options**)

To install NetTool Connect:

1. Insert the CD-ROM that comes packaged with the tester into your PC.
2. Run the setup program to install the software:
    a. Click **Next**.
    b. Click **Yes** to accept the license agreement.
    c. Select the destination folder and then click **Next**.
    d. Select the components you want to install and then click **Next**.
    e. Click **Next** to update the drivers.

Note

*On certain operating systems, you may be prompted with a message telling you that the driver has not passed Windows testing or be not certified. Press **Continue Anyway** to complete the installation:*

    f. Connect the supplied USB cable between the tester and the PC (see "USB Connection" in Chapter 2).

    In a few seconds, the **Found New Hardware Wizard** screen is displayed.

    g. To proceed through the series of screens, click **Next**, **Next**, **Continue Anyway**, and **Finish** to complete the installation.

You can now run NetTool Connect.

To run NetTool Connect:

1. From the **Start** menu, select **Programs | Fluke Networks | NetTool Connect**.

   The **NetTool Connect** startup screen (see Figure 8-3) is displayed.

2. Click the button for the function that you want to use.

For detailed information on how to use NetTool Connect and all of its functions, see the online **Help**.

Updating the Tester's Software

From time to time, updates to the tester's software become available.

To update the software:

1. Select the NetTool icon then select **About NetTool** to find out what version of software is installed on your tester.

2. Find out if there is a new software version available. To do this:

   a. Go to http://www.flukenetworks.com. Select **NetTool Series II Inline Network Tester** from the **Product Quicklink** list box.

   b. Click the **software** link to display the Software page. Check the version number to determine if it is later than the version installed on your tester.

3. Follow the web instructions to download the update file to your PC.

4. Make sure that NetTool Connect is installed on the PC.

Note

If NetTool Connect is not installed, do not connect the tester to the PC.

5. Connect the supplied USB cable between the tester and the PC (see "USB Connection" in Chapter 2).

6. From the **Start** menu, select **Programs | Fluke Networks | NetTool Connect** to start NetTool Connect.

7. Click **Update** and then follow the on-screen instructions to transfer the file from the PC to the tester.

Enabling Software Options

If you purchased a software option for your tester, you received a key code that enables you to use that option.

Note

If you need help obtaining your key code, contact Fluke Networks for assistance. See "Contacting Fluke Networks" for information.

To enable a software option, have the key code handy, and then do the following:

1. Make sure that NetTool Connect is installed on the PC.

Note

If NetTool Connect is not installed, do not connect the tester to the PC.

2. Connect the supplied USB cable between the tester and the PC (see “USB Connection” in Chapter 2).
3. From the Start menu, select **Programs | Fluke Networks | NetTool Connect** to start NetTool Connect.
4. Click **Options**.
5. Select the option you want to enable.
6. Type the key code in **Key Code** box and then click **Enable**.

Power Supply

To supply power to the tester, you can use the four AA alkaline batteries (supplied) or the (optional) rechargeable NiMH AA batteries.

Note

NiMH batteries are the only type of rechargeable batteries supported. Do not use any other chemistry of rechargeable batteries.

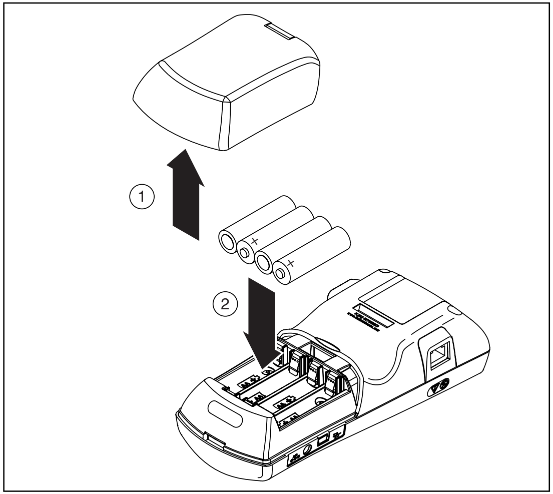
Alternatively, you can use the (optional) AC adapter or PoE power.

⚠ **Caution**

Use only the AC adapter supplied by Fluke Networks.

Using Battery Power

To install the batteries, remove the yellow boot to access the battery compartment. Open the door and insert the batteries, as shown in Figure 1-2.



ekd01f.eps

Figure 1-2. Installing the Batteries

Maximizing Battery Life

The life of batteries is strongly influenced by the care that they receive.

- The greatest enemy of batteries is heat. When using rechargeable batteries, avoid charging them when they are hot.

- Battery life can also be shortened if you frequently leave the tester in a hot place, such as a car on a warm day and then charge the batteries immediately upon returning to your office.

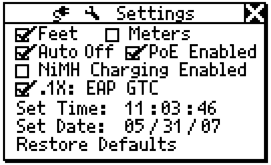
Using Rechargeable Batteries

The **CHARGE** LED, located on the tester’s front panel, indicates the status of the battery charge (see “CHARGE LED” later in this chapter.

To charge the batteries:

1. On the Main menu, select the NetTool icon to display the **NetTool** menu.

2. Select **Settings** to display the **Settings** menu (Figure 1-3):



```
Settings                          ☒
☑ Feet       □ Meters
☑ Auto Off   ☑ PoE Enabled
□ NiMH Charging Enabled
☑ .1X: EAP GTC
Set Time:  11:03:46
Set Date:  05/31/07
Restore Defaults
```

emt14s.bmp

Figure 1-3. Settings Menu

3. Select **NiMH Charging Enabled**.

Caution

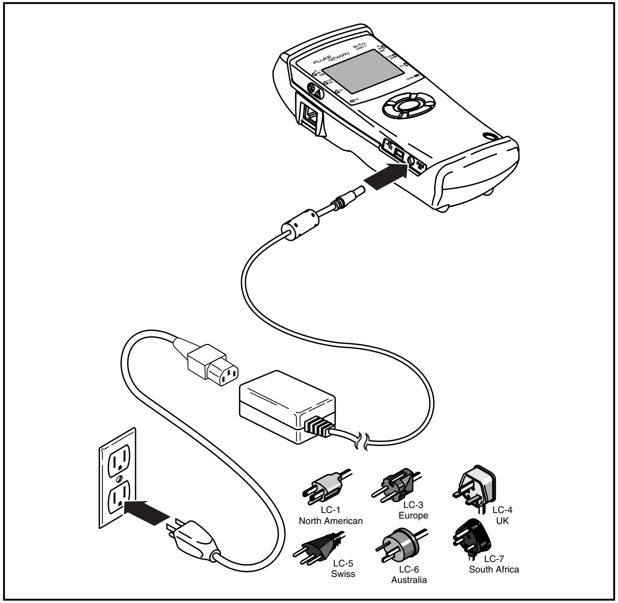
To avoid the risk of damaging the batteries and/or tester, you must have NiMH batteries installed if you have the NiMH Charging Enabled option checked.

4. Connect the tester to the (optional) AC adapter (see Figure 1-4) and plug it in to begin charging.

   A full charge takes approximately five hours.

Using the AC Adapter

To use AC power, connect the (optional) AC adapter to the tester as shown in Figure 1-4.



emt04f.eps

Figure 1-4. Connecting to the AC Adapter

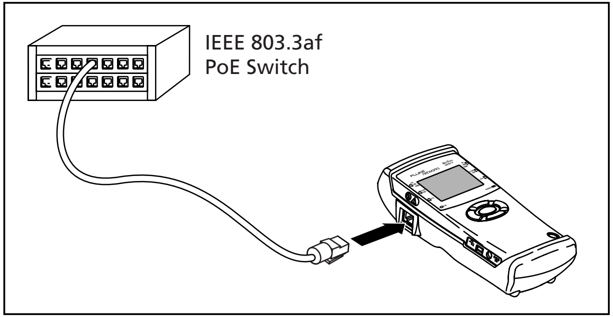
Using PoE Power

You can set up the tester to use power from power-supplying equipment (PSE).

To do this, you must enable the tester’s **PoE** (Power over Ethernet) feature. See “Changing the Tester’s Settings” in Chapter 2 to find out how to do this.

After the **PoE Enabled** option is set, if the tester is connected to power-supplying equipment (PSE) and has negotiated power from the device, it uses power supplied by the PSE.

Figure 1-5 shows you how to connect the tester to a PSE switch. Note that you must connect the cable to the tester’s left RJ-45 jack.



emt05f.eps

Figure 1-5. Using Power from a PoE Switch

The tester first attempts to pass Power over Ethernet (PoE) power through to a powered-device (PD). If such a device is not attached, the tester draws power from the attached PoE switch.

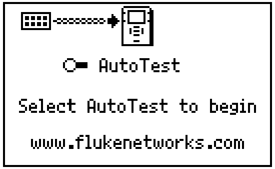
The **PoE** LED lights blue to indicate that power is being drawn from the PSE or that PoE power is being drawn inline.

Turning on the Tester

To turn on the tester:

1. Connect the tester (see Chapter 2 for details).
2. Press the green **Power** button firmly for one second.

   This initial screen (Figure 1-6) is displayed:



AutoTest

Select AutoTest to begin

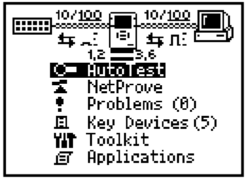
www.flukenetworks.com

emt15s.bmp

Figure 1-6. Initial Screen

3. Press **SELECT** to start AutoTest.

   After AutoTest ends, the Main menu (Figure 1-7) is displayed:



emt02s.eps

Figure 1-7. Main Menu

The Main menu has two areas:

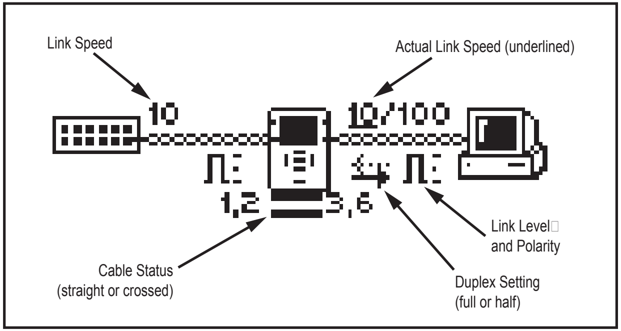
- At the top, a network diagram containing icons that represent elements of the connection.
- Below the diagram, a list of menu options.

User Interface

This section acquaints you with the network diagram, menus, and functions of the tester's buttons, navigation keys, and LEDs.

Understanding the Network Diagram

The network diagram, shown in Figure 1-8, gives you at-a-glance information about the connection.



ekd07f.eps

Figure 1-8. Network Diagram

In this diagram, the easily recognizable icons (see Table 1-2) represent the tester and the connected devices. If you move the cursor to an icon and then select it, you can obtain multiple levels of detail (e.g., IP address, frame counts, line speed) about your selection.

The network symbols (also in Table 1-2) provide additional link and cabling information

Table 1-2. Symbols Used in the Network Diagram

Connected device (PC, printer, IP phone)	Normal level, normal polarity
NetTool tester	Normal level, reverse polarity
Network	Low level, normal polarity
⇄ Full duplex ⇄ Half duplex	Low level, reverse polarity.
= Straight cable ✕ Crossed cable	AUTO-X Automatic MDI-X connection

Main Menu

The **Main** menu (Figure 1-7) is located under the connection diagram. From this menu, you can access the following features:

Note

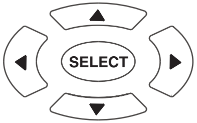
*To display these screens, move the cursor to the menu item, then press **SELECT**.*

- **AutoTest***:* starts the automatic tests.
- **NetProve**: automatically proves Ping and Application connectivity to servers and key devices. Indicates pass/fail based on ping and TCP response times. Information is downloaded to the tester with the NetTool Connect software.

- **Problems**: displays the Problem Log, which categorizes and alerts you to problems detected, such as errors, duplex mismatches, and duplicate IP addresses. See Chapter 6, “Common Problems”, for details.
- **Key Devices**: displays all key devices and categorizes them by type (for example, servers, routers, and printers).
- **Toolkit**: contains a group of support tools, such as Health, Protocols, Ping, and Reporter that help you troubleshoot and document your network.
- **Applications**: contains additional applications (if installed), such as VoIP and Security.

Navigation Keys

The navigation keys are the four directional arrow keys that encircle the **SELECT** key.



ahn310f.eps

Press these keys to move the cursor to the network diagram icons and menu options and to navigate the different screens.

Scrolling

To scroll through individual items on a menu, press the **Up** or **Down** arrow ▲▼ key.

Paging Up and Down

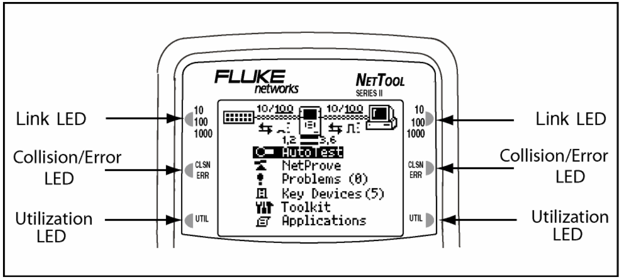
If a menu has several pages, press the Left arrow ◀ key to display the preceding page and press the Right arrow key ▶ to advance to the next page.

Closing the Current Screen

To close the current screen, press the **Up** arrow ▲key to move the cursor to the **X** (located in the top right corner). When selected, the **X** flashes. Press **SELECT.**

Understanding the LEDs

On each side of the LCD, the tester has a set of LED indicators (Figure 1-9) that provide information about the left and right RJ-45 connections. These LEDs combine to give you immediate insight and at-a-glance information about your network environment.



emt01f.bmp

Figure 1-9. LEDs

10/100/1000 (Link) LED

A tri-colored LED with these states:

- White: 1000 MB connection.
- Blue: 100 MB connection.
- Green: 10 MB connection.

CLSN (Collision/Error) LED

A bi-colored LED with the following states:

- Yellow: collisions are occurring.
- Red: errors are being detected.

UTIL (Utilization) LED

A tri-colored LED, with each color representing the following ranges of utilization:

- Blinking green: network utilization levels are below 50 %.
- Blinking yellow: network utilization levels are between
  50 % and 90 %.
- Blinking red: network utilization levels are higher than 90 %.

Additional LED Indicators

Below the LCD are these two LEDs: PoE and CHARGE.

PoE LED

Located on the left side, this LED lights steady blue when the tester is connected to and drawing power from a PSE or when PoE is being detected inline.

CHARGE LED

Located on the right side, this LED indicates the status of the battery charge:

- Blinking green: NIMH rechargeable batteries are installed, more than 50 % full, and charging.
- Blinking orange: NIMH rechargeable batteries are installed, less than 50 % full, and charging.
- Solid green: the tester is running off of AC or PoE power. If NiMH rechargeable batteries are installed, they are full.

Chapter 2
Connecting and Configuring the Tester

Introduction

The first half of this chapter shows you how to connect the tester to the network and to the device you want to test. You will also learn how to connect the tester to a PC so that you can download reports and screenshots.

The second half of this chapter shows you how to change your tester's settings. For example, you will learn how to set the date and time and how to manually configure the tester's IP address information. You will also find out how to locate important information, such as the tester's serial number.

Connecting the Tester

The tester has two RJ-45 jacks, one on each side. These jacks enable you to make two types of connections:

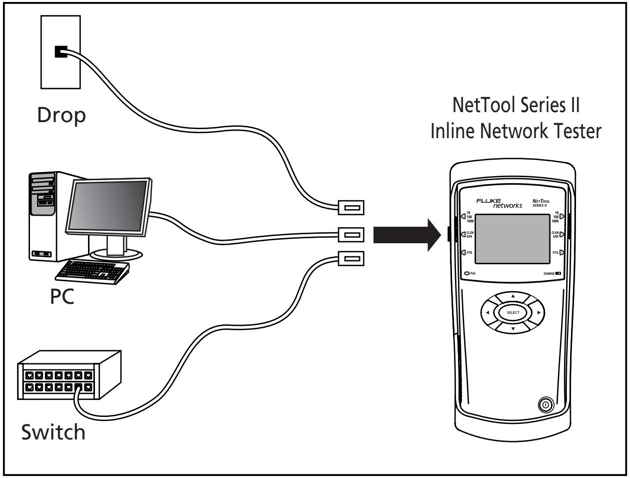
- Single-ended: plug one end of a cable into the tester's left RJ-45 jack and the other end directly into a wall plate or into a device such as a PC.

- Inline: use both jacks to plug the tester between two devices, such as a hub and a PC. The left RJ-45 jack is always connected to the switch and the right RJ-45 jack into the PC or client device.

The tester also has a USB port, which enables you to directly connect the tester to a PC and use the NetTool Connect program (described in Chapter 1).

Single-Ended Connection

For a single-ended connection, connect the device-under-test to the tester's left RJ-45 jack, as shown in the following diagram:



ekd08f.eps

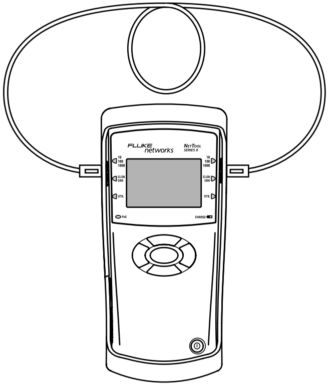
Figure 2-1. Single-Ended Connection

- Drop: when you connect the tester to a wall jack, you can check a network drop for activity and find out what services lie on the other side.
- PC: when you connect the tester to a PC, you can find out whether it is properly configured to take advantage of network resources.
- Switch: when you connect the tester to a hub or switch, it can simulate a PC and perform tests like Ping.

After you connect the tester, turn it on and run AutoTest on the cable. See "Running AutoTest" in Chapter 3 for details.

Patch Cable Test

Use a loopback connection (Figure 2-2) to assess the condition of the patch cables you will use.



ekd09f.eps

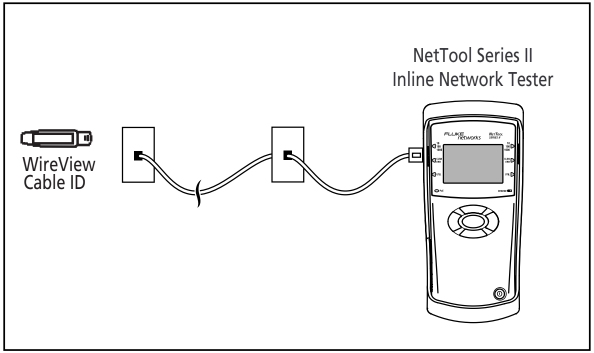
Figure 2-2. Patch Cable Test

After you connect the tester, turn it on and run AutoTest on the cable (see “Running AutoTest” in Chapter 3 for details).

The tester measures and displays connectivity between pins on both ends of the cable.

WireView Cable ID Test

When both ends of a cable cannot be connected to the tester (for example, if one end is in a wiring closet), connect the WireView Cable ID (supplied) to the far end (see Figure 2-3).



ekd10f.eps

Figure 2-3. Wiremap Test

After you connect the tester, turn it on and run AutoTest on the cable. See “Running AutoTest” in Chapter 3 for details.

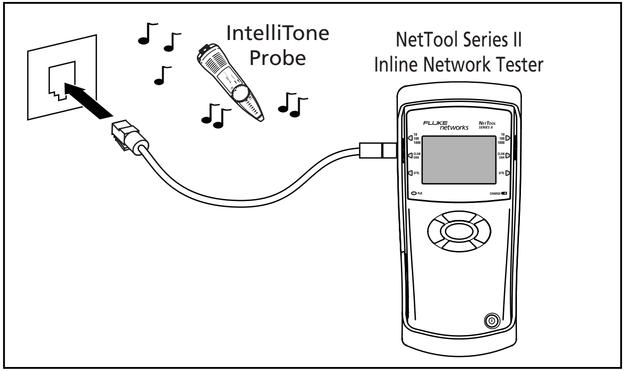
Tone Test

Connect a cable to the tester's left RJ-45 jack (Figure 2-4) when running a Tone test.

Note

> *See "Running a Tone Test" to find out how to run this test.*

The tester applies tones to a cable. These tones are picked up by a probe, such as the IntelliTone™ Probe, to help you trace cables and locate problems in a cable.



ekd11f.eps

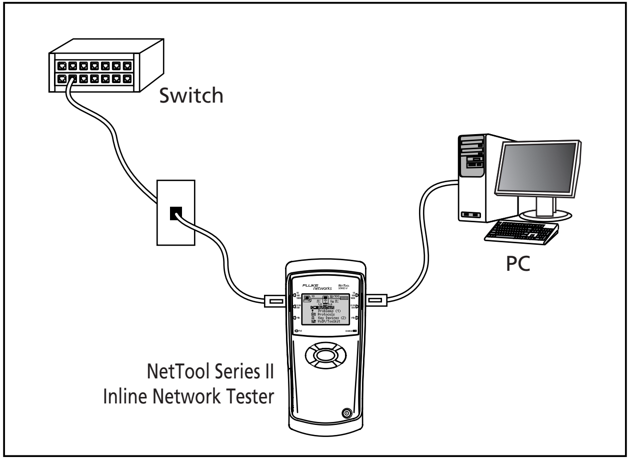
Figure 2-4. Tone Test

Inline Connection

An inline connection entails having the tester simultaneously plugged in between two network devices, such as a PC or a PoE-powered device and a network switch. Use this type of connection to verify whether the device can communicate properly with the network.

Use the left RJ-45 jack to connect the tester to the network and the right RJ-45 jack to connect to a PC or phone, as shown in Figure 2-5.

After you connect the tester, turn it on and run AutoTest. See "Running AutoTest" in Chapter 3 for details.



ekd12f.eps

Figure 2-5. Inline Connection

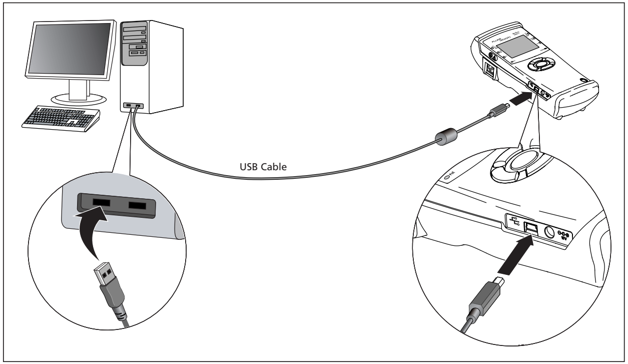
USB Port Connection

A USB port connection enables you to use NetTool Connect to do the following:

- Download software (see "Updating the Software")
- Enable options
- Save screens
- Upload and download NetProve catalogs
- Upload Report data

See "NetTool Connect" in Chapter 1 for installation instructions.

To connect the tester, use the supplied USB cable. As shown in Figure 2-6, connect one end of the cable to the USB port on the PC and the other end to the USB port on the left side of the tester.



emt17f.eps

Figure 2-6. Connecting to the USB Port

Configuring the Tester

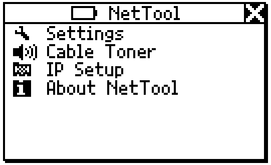
To configure the tester:

1. Turn it on and then press **SELECT** to run AutoTest.

   After AutoTest runs, the Main menu (Figure 1-7) is displayed.

2. Press the Up ▲ arrow key to move the cursor to the NetTool icon ▣, which is located in the network diagram at the top of the screen. Then, press **SELECT**.

The **NetTool** menu (Figure 2-7) is displayed:



emt08s.bmp

Figure 2-7. NetTool Menu

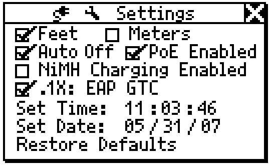
From this menu, you can access the tester’s setup menus, which are described in the following sections.

Note

*The battery level icon is displayed at the top of the **Setup** screen. It indicates the current state of the batteries.* 🔋 *indicates the batteries are fully charged.*

Changing the Tester's Settings

Select **Settings** to display the **Settings** menu (Figure 2-8):



```
Settings
☑ Feet      □ Meters
☑ Auto Off  ☑ PoE Enabled
□ NiMH Charging Enabled
☑ .1X: EAP GTC
Set Time:  11:03:46
Set Date:  05/31/07
Restore Defaults
```

emt14s.bmp

Figure 2-8. Settings Menu

- Select a unit of measurement (**Feet** or **Meters**) for testing.
- Enable/disable the **Auto Off** feature.

  When this feature is enabled, the tester automatically turns itself off after 10 minutes of no key activity. This helps to conserve the tester's battery power.
- Enable the **PoE** (Power over Ethernet) feature.

  When this feature is enabled, the tester searches for PoE power-supplying equipment (PSE) during AutoTest.

  Note

  Be aware that AutoTest requires more time if this feature is enabled. When using the tester in non-PoE-switched environments, you are advised to disable this feature to speed up AutoTest.
- Enable/disable charging of NiMH batteries.

  Caution

  If NiMH Charging Enabled is checked, you must have NiMH batteries installed in the tester. If you enable this option and non-rechargeable alkaline or lithium batteries are installed, you can damage the batteries and/or the tester.
- **.1X: EAP GTC**. The 802.1X authentication type "EAP GTC" has been uploaded from the PC NetTool Connect application. Check this box to enable 802.1X authentication.

  Note:

  If another authentication type such as "TTLS CHAP" had been uploaded to NetTool, this line would read ".1X: TTLS CHAP."
  Only one authentication type can be stored on the NetTool Series II at a time.

Set the time and date.

Notes

The format for time is hour:minutes:seconds. The format for the date is month:day:year.

The clock does not self-adjust for local time zones changes.

NetTool Connect allows you to set the time for the tester and even synchronize it with the PC clock (check the Help for NetTool Connect for assistance).

To change the time/date settings:

1. In the first field, press the **Up** ▲ or **Down** ▼ arrow key to select the desired number.
2. Press the **Right** ▶ arrow key to advance to the next position.
3. After the desired time and date are displayed, press **SELECT**.

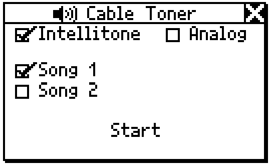
- Restore factory default settings.

Select **Restore Defaults** to restore all of the tester’s original settings.

Running a Tone Test

To run a Tone test:

1. Connect the tester, as shown in Figure 2-4.
2. On the **NetTool** menu (Figure 2-7), select 🔊 **Cable Toner**.
3. On the **Cable Toner** screen (Figure 2-9), select the type of probe you are using and song:



🔊 Cable Toner ☒

☑ Intellitone ☐ Analog

☑ Song 1
☐ Song 2

Start

emt09s.bmp

Figure 2-9. Cable Toner Screen

4. Select **Start** to run the test.

Manually Assigning a IP Address

Notes

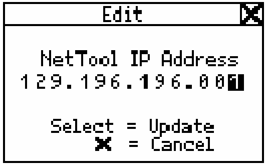
By default, the tester uses DHCP to obtain its IP address. If you have DHCP on your network, you can skip this section because no further configuration is required.

For manual configuration, make sure any IP address you assign to your tester is correct for the subnet you are on.

To manually assign an IP address:

1. Select **IP Setup** to display the **IP Setup** screen.
2. Select **Manual**.

3. Press the **Down** ▼ arrow key to highlight the IP address that you want to configure (in this case the tester's address). Then, press **SELECT** to display the **Edit** screen (Figure 2-10).



Edit ☒

NetTool IP Address
129.196.196.001

Select = Update
✖ = Cancel

afq47s.bmp

Figure 2-10. Edit Screen

4. Press the **Up** ▲ or **Down** ▼ arrow key to supply a number in the first field in the address. Then, press the **Right** ▶ arrow key to advance to the next position. Continue in this manner until the desired IP address is displayed.

5. Press **SELECT** to save the IP address.

   The tester lists the updated address with the subnet and router IP addresses.

Note

*To cancel the operation, press the **Right** ▶ arrow key to move the cursor to the **X** in the upper right corner of the screen. After the **X** flashes, press **SELECT**.*

6. In like manner, configure the subnet mask and router addresses.

   The tester assists you by entering the first parts of those addresses based on common addressing rules.

Obtaining Information about Your Tester

To view information about your tester, such as the software version, serial number, MAC address, options enabled, and other helpful information, select **About NetTool** from the **NetTool** menu (Figure 2-7).

Be sure to record the serial number and MAC address of your tester for future reference.

Chapter 3
AutoTest

Introduction

AutoTest provides a good starting point for trying to determine what devices are on your network and for making a quick assessment of your network's overall condition. Results from AutoTest can alert you to connectivity problems before they impact network performance.

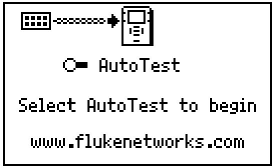
Running AutoTest

To run AutoTest:

1. Connect the tester, using one of the connection schemes documented in Chapter 2.

2. Turn on the tester.

3. The **AutoTest** screen (Figure 3-1) is displayed. **AutoTest** flashes to indicate that the tester is ready to run a test:


AutoTest

Select AutoTest to begin

www.flukenetworks.com

emt15s.bmp

Figure 3-1. AutoTest Screen

4. Press **SELECT**.

   The tester searches both RJ-45 connections to determine what it is connected to.

   Upon completion, Auto Test shows information about the connection and provides traffic statistics for connected devices.

Cable Test Results

Note

The cable must be connected to the tester's left RJ-45 connector.

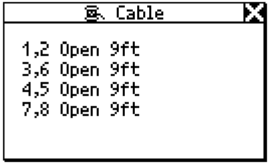
If the tester is connected to a patch cable, AutoTest evaluates the integrity of the cable and finds errors that might suggest a physical media problem.

If the (supplied) WireView Cable ID is attached or if the cable is connected to both RJ-45 connectors, the tester performs deeper testing of the cable by additionally verifying pin-to-pin connectivity.

Cable Length, Opens, Shorts, and Splits

To obtain information about the cable, move the cursor to the Spool icon, then press **SELECT**.

The **Cable** screen is displayed, as shown in Figure 3-2:



```
Cable
 1,2 Open 9ft
 3,6 Open 9ft
 4,5 Open 9ft
 7,8 Open 9ft
```

emt32s.bmp

Figure 3-2. Cable Screen

On this screen, the tester accurately measures wire lengths within the cable and indicates whether there are any opens, shorts, or split pairs present.

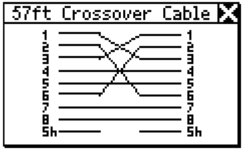
Wiremap

Note

If the tester is connected to the AC adapter, it cannot reliably detect the presence of a Cable ID.

If the (supplied) WireView Cable ID is attached, select (**Wiremap** icon).

The **Crossover Cable** screen (Figure 3-3) is displayed, which verifies the length of the cable and identifies the pinouts at each end:



57ft Crossover Cable

afq34s.bmp

Figure 3-3. Wiremap Details

Single-Ended AutoTest Results

AutoTest result screens vary depending on the device that the tester is connected to.

Note

The results described in this section are provided as examples of what information the tester provides.

Network Drop

If the tester is connected to a network drop, it displays one of the following icons to identify the service that is active on the jack:

- **Ethernet**: tells you if the jack is hot and what is on the other end (for example, a hub or a switch). It also provides the speed and duplex setting, level, polarity, and the segment ID so you can pick the right network to hook up to a PC (if there are multiple jacks).
- ☎**Telco**: indicates that analog telephone signals, ISDN signals, or dangerous power supply voltages are being detected on the line.

Caution

Although the tester can detect Telco and ISDN signals, it is not designed to be used on the public telephone network. Disconnect immediately.

- 🖥 **No Response**: A dangling, flashing power cord indicates that the tester senses an Ethernet device, but the device is not responding. This usually means that the device is powered off.

Table 3-1 lists the devices and services that the tester discovers.

Table 3-1. Discovered Services

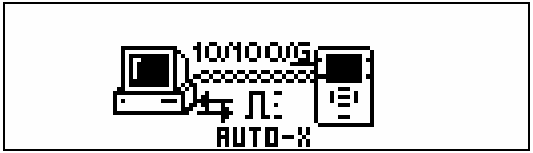
Device	Services
Servers	**IP Servers** (IP services discovered): DHCP, DNS, email (SMTP, POP, IMAP), Web (HTTP, HTTP proxy), WINS **NetWare Servers** (IPX service types): Nearest File Server, File Server, NetWare Access server, Time Synchronization Server, NetWare Directory Server (NDS), NetWare Management Server **NetBIOS Servers**: Primary Domain controllers, Backup Domain controllers, Master Browsers
Routers	**IP Routers**: RIP, IGRP, EIGRP, OSPF, IRDP, RIP2 **IPX routers**: RIP
Printers	**IP Printers**: IP Printers, IP Print Spoolers. **IPX Printers**: IPX Print services **DLC Printers**: Microsoft DLC, HP DLC

Network Device

If the tester is connected to a single network device, a diagram similar to that shown in Figure 3-4 is displayed:

Note

In the network diagram shown in Figure 3-4, the PC icon represents the single device (for example, a PC, printer, or VoIP phone).



emt317s.bmp

Figure 3-4. Connection Diagram Showing Connection to a Single Device

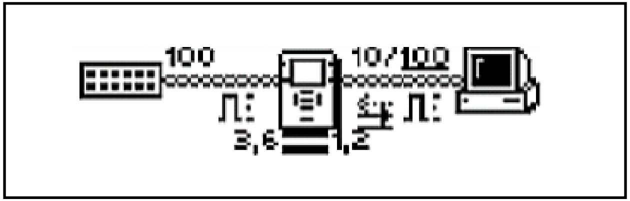
Select the PC icon to find out more about the connected device. Go to Chapter 4 “Troubleshooting a Network Device”.

Inline AutoTest Results

The diagrams at the top of the screen can give you a quick indication of what is going on with your network.

Inline between a Device and the Network

If the tester is connected inline between a device and the network, a diagram similar to that shown in Figure 3-5 is displayed at the top of the screen.



ahn020s.eps

Figure 3-5. Diagram of an Inline Connection

This screen reflects the tester’s connection to devices.

Note that the duplex settings and link speeds are underscored. The underscore signifies a determined or negotiated result while the non-underlined value signifies the advertised value.

The diagram also indicates the duplex settings (see Table 3-2) for each device. Duplex mismatches can cause communication between devices to be impeded.

Table 3-2. Duplex Settings

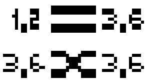
Symbol	Meaning
⇄	Full Duplex
→ ⇠	Half Duplex

Polarity information is also given. The waveform-shaped icons used in the diagram are listed in Table 3-3.

Table 3-3. Meanings of Link and Polarity Level Icons

Indicator	Definition
⊓:	Normal level, normal polarity
⊔:	Normal level, reverse polarity
ₙ:	Low level, normal polarity
ᵤ:	Low level, reverse polarity. Link level is displayed by the height of the waveform.

Under the NetTool icon 🖳, you can also obtain status information for the cables actively linked to the tester. For example:



ahn235f.eps

The tester detects whether the cables are straight or swapped. If it sees a swap cable problem, it swaps the cables internally, allowing you to troubleshoot past a simple swap cable problem.

The LEDs on either side of the tester indicate the status and utilization of the link and whether the tester discovers any errors.

To get detailed results, move the cursor to one of the following icons then press **SELECT**:

- PC icon : enables you to view results for the device. Go to Chapter 4 “Troubleshooting a Network Device” for details.
- Network icon : enables you to view network results. Go to Chapter 5 “Troubleshooting Networks” for details.

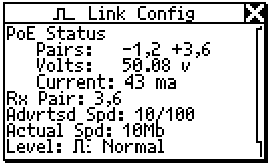
You can view additional results by selecting items from the **Main** menu (Figure 1-7), which is located below the diagram.

Inline between a PoE Powered Device and the Network

During AutoTest, when a PoE-supplying PSE is detected on the tester’s left RJ-45 and a PoE-powered device is detected on the right RJ-45, PoE power is passed through to the right side and the current is measured. If the device on the right side draws PoE current, it is determined to be a PoE PD.

When PoE is detected, the PoE LED on the tester’s front panel illuminates.

To obtain information about PoE voltage and current, select the device. Then, on the **Station** menu, select **Link Config** to display the **Link Config** screen, as shown in Figure 3-6:



```
PoE Status
   Pairs:   -1,2 +3,6
   Volts:   50.08 v
   Current: 43 ma
Rx Pair: 3,6
Advrtsd Spd: 10/100
Actual Spd: 10Mb
Level: ⎍: Normal
```

emt16s.bmp

Figure 3-6. Link Config Screen

To get detailed results on the network, select the Network icon ▦ .

For information on VoIP (Voice over IP), see Chapter 7 “Verifying Voice over IP Service”.

Chapter 4
Troubleshooting a Network Device

Introduction

The tester can provide information that you can use to determine whether a device is configured properly for your network. After you have confidence that all of the stations and devices on your network are configured correctly, you can move on to evaluate the entire network. This chapter shows you how to resolve device and configuration problems.

Verifying a Device’s Configuration

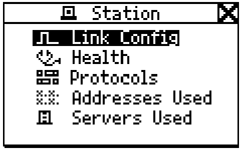
To find out whether a device is properly configured:

1. Connect the tester, using one of the connection schemes described in Chapter 2.

2. Run AutoTest (see “Running AutoTest” in Chapter 3 for details).

3. To get information about the device, click (PC icon) in the connection diagram at the top of the screen.

   The **Station** menu (Figure 4-1) is displayed:



afq16s.bmp

Figure 4-1. Station Menu

Four basic types of information about the device or network can be selected from this menu:

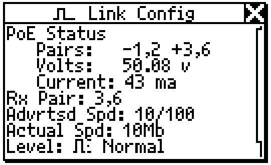
- **Link Config**: provides link pulse and PoE voltage and pair information.
- **Health**: lets you monitor frames and view errors that may indicate problems on the device or network.
- **Protocols**: displays the protocols running on the device or network.
- **Addresses Used**: enables you to verify a devices' IP address information, find out what VLAN a device belongs to, and obtain CDP (Cisco Discovery Protocol), LLDP (Link Layer Discovery Protocol), and EDP (Extreme Discovery Protocol) information.

4. To select an item, move the cursor to its name, then press **SELECT**.

   The following sections describe the detailed information you can obtain about your network.

Viewing Link Status Information

To view information about the cable and status of the connection, select **Link Config** from the **Station** menu to display the **Link Config** screen (Figure 4-2):



```
⎍ Link Config ☒
PoE Status
   Pairs:   -1,2 +3,6
   Volts:   50.08 v
   Current: 43 ma
Rx Pair: 3,6
Advrtsd Spd: 10/100
Actual Spd: 10Mb
Level: ⎍: Normal
```

emt16s.bmp

Figure 4-2. Link Configuration Details

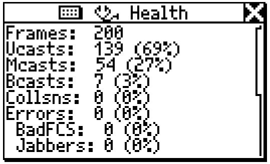
On this screen, the tester displays PoE current and voltage information.

The tester also identifies the wire pair it is connected to and reports the duplex, level, and polarity of the signal (see Table 3-3 for descriptions of the icons used). This information can help you troubleshoot poor quality in a connection.

The actual and advertised speeds of the link are also given. Monitoring this information can help you anticipate possible performance and connectivity problems.

Checking Frames for Errors

To find out how many frames have been transmitted and whether any errors were discovered in those frames, select **Health** from the **Station** menu display the **Health** screen (Figure 4-3):



```
Health
Frames:  200
Ucasts:  139 (69%)
Mcasts:  54 (27%)
Bcasts:  7 (3%)
Collsns: 0 (0%)
Errors:  0 (0%)
 BadFCS:  0 (0%)
 Jabbers: 0 (0%)
```

emt35s.bmp

Figure 4-3. Health Details

This screen enables you to look at the status of frames transmitted across the link since **AutoTest** began. As you can see, the tester provides a breakout of the types of errors it discovers:

- **Frames**: total count of unicast, multicast, broadcast, and error frames.
- **Unicasts**: count of unicast frames received (only one receiving host).
- **Mcasts**: count multicast frames received (many receiving hosts. (Does not include broadcast frames.)
- **Bcasts**: broadcast frames received by all hosts on the network. (Does not include multicast frames.)
- **Collsns**: collision fragments caused by simultaneous transmission and reception.

- **Errors**: total number of error frames (does not include collisions).

  Note

  The most likely cause of an error is faulty NIC hardware, corrupt NIC driver files, bad cabling, or grounding problems.

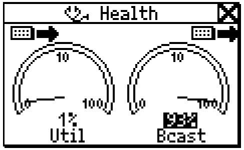
  - **BadFCS**: bad FCS (Frame Check Sequence), which is a frame containing an invalid checksum (also called a CRC error).
  - **Jabbers**: frames greater than 1518 bytes that have an invalid checksum.
  - **Ghosts**: energy (noise) detected on a cable that appears to be a frame but that has an invalid beginning-of-frame pattern. Must be at least 64 bytes long.
  - **Undersize**: frame less than 64 bytes long that is otherwise well formed.
  - **Oversize**: frame greater than 1518 bytes that also has a good checksum.
  - **RxSymbol**: frame with an invalid data symbol and a legal packet size.
  - **Alignment**: frame that does not end on a byte boundary.
  - **Length**: frame whose valid length field value does not match the actual number of bytes counted in the data field.

These detailed error statistics can help you isolate device- and network-related problems.

The **Health** screen shown in Figure 4-3 displays cumulative activity since you last ran AutoTest. You may also want take a look at what is going on now and simultaneously view the health of frames on both sides of a connection.

To do this:

1. Select **Toolkit** from the **Main** menu (Figure 1-7).
2. From the **Toolkit** menu, select **Health** to display the **Health** screen shown in Figure 4-4:



afq08s.bmp

Figure 4-4. Health Statistics

3. To change the view, move the cursor to **Util** or **Bcast**, then press **SELECT**.

   For example, selecting **Util** changes the view to broadcast traffic, collision levels, or errors coming from either device to which the tester is connected.

4. To change what the tester is viewing in real-time and to change the direction (that is, "to/from Network" or "to/from PC"), move the cursor to the desired device icon (located in the upper right or left). Then press **SELECT**.

   Use this information to make comparisons. For example, you may see a high percentage of network utilization and observe that the PC is also registering high utilization.

5. To measure what the PC is doing to contribute to a high utilization statistic (for example, broadcasts), move the cursor to **Util** then press **SELECT**.

6. To change how the data is expressed (in "per seconds" or as a percentage of current activity), move the cursor to the reading below a meter then press **SELECT.**

Notes

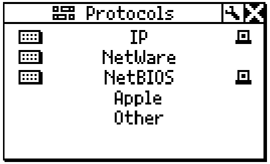
If you exit the ***Health*** *screen and return later without powering off the tester, the last-saved settings are displayed.*

If you power off the tester while viewing the ***Health*** *screen, readings are not saved. Display the* ***Setup*** *screen and select* ***Restore Defaults*** *to restore the factory settings.*

Tracking Protocols

To find out what protocols are associated with a device or running on the network:

1. Select **Protocols** from the **Station** menu to display the **Protocols** screen (Figure 4-5):



emt20s.bmp

Figure 4-5. Protocols Screen

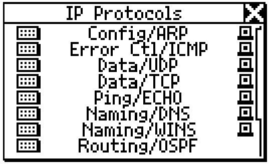
The **Protocols** screen lists groups of protocols present on the network. This information can help you find out if there are any protocol configuration mismatches. See Table 3-1 for a list of the protocols that the tester can discover.

The network icon appears next to the name of a protocol group to indicate that there are protocols of that type running on the network.

Note that some protocols also display the PC icon, which means that the tester sees them on both the PC side and the network side.

2. To view detailed information for a particular protocol group, move the cursor to its name, then press **SELECT**.

   For example, if you select **IP Protocols**, the **IP Protocols** screen (Figure 4-6) is displayed:



IP Protocols

Config/ARP
Error Ctl/ICMP
Data/UDP
Data/TCP
Ping/ECHO
Naming/DNS
Naming/WINS
Routing/OSPF

emt17s.bmp

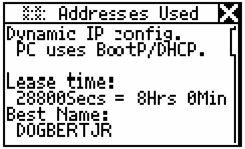
Figure 4-6. IP Protocols Screen

All of the IP protocols the tester sees are listed on this screen.

Obtaining a Device's IP Address Information

To obtain IP address information for a device:

1. Select **Addresses Used** from the **Station** menu to display the following screen:



```
Dynamic IP config.
 PC uses BootP/DHCP.

Lease time:
 28800Secs = 8Hrs 0Min
Best Name:
 DOGBERTJR
```

ahn25s.bmp

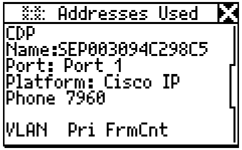
Figure 4-7. Addresses Used Screen

Use the information on the **Addresses Used** screen to verify IP address information. You can also find out the best-discovered name for the device as well as its IP, IPX, and MAC address.

The tester can also detect the following protocols:

- CDP (Cisco Discovery Protocol)
- EDP (Extreme Discovery Protocol)
- IEEE 802.1ab LLDP (Link Layer Discovery Procotol)

2. If a discovery protocol is found, press the **Down** ▼ arrow key to locate the section for the discovered protocol. For example, Figure 4-8 shows the information provided for CDP:



```
CDP
Name:SEP003094C298C5
Port: Port 1
Platform: Cisco IP
Phone 7960

VLAN  Pri FrmCnt
```

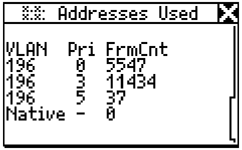
ahn323s.bmp

Figure 4-8. CDP Information

Discovery protocol information is reported for the most recent advertisement on that side. This information is updated every two seconds.

When plugged into a switch VLAN port, information for **Native VLAN** and **Appliance** (phone) **VLAN** are also given.

3. You can also find out what VLAN a device belongs to. To do this, press the **Down** ▼ arrow key to locate VLAN statistics, as shown in Figure 4-9:



```
Addresses Used

VLAN   Pri FrmCnt
196     0  5547
196     3  11434
196     5  37
Native  -  0
```

ahn322s.bmp

Figure 4-9. VLAN Information

The tester can provide information for up to five discovered VLANS. You can view the VLAN’s ID, its priority, frame counts, and the untagged frame count. This information is updated every two seconds.

You can also monitor VLANs during a VoIP call to see which ones are being used (see entries in the “VoIP Logs” in Appendix B).

Chapter 5
Troubleshooting Networks

Introduction

The tester provides comprehensive network diagnostics that can help you evaluate the health of your network and assist you with troubleshooting network problems.

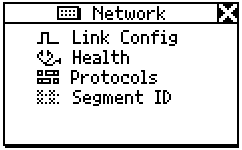
Two specialized tests, Ping and NetProve, enable you to accurately pinpoint sources of connectivity problems. Both tests emit ICMP ping packets to validate connectivity and provide results that you can save as a PDF or HTML document for archive or distribution.

Finding Out About Your Network

To obtain information about the network the tester is plugged into, do the following:

1. Run Autotest (see “AutoTest” in Chapter 3 for details).
2. To view details about the network, select ▦ (Network icon).

The **Network** menu (Figure 5-1) is displayed:



ahn200s.bmp

Figure 5-1. Network Menu

Four options are listed on this menu:

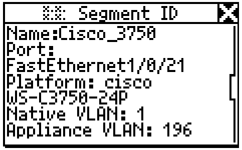
- **Link Config**: provides link pulse information about the network. See “Viewing Link Status Information” in Chapter 4 for details.
- **Health**: lets you monitor frames and view errors that indicate problems on the link. See “Checking Frames for Errors” in Chapter 4 for details.
- **Protocols**: displays the protocols running on the network. See “Tracking Protocols” in Chapter 4 for details.
- **Segment ID**: tells you what type of network you are plugged into. If there are multiple Ethernet drops, this screen can help you decide which jack to use for the correct configuration. See “Identifying the Network Type” in this chapter.

3. To view details, select an option and then press **SELECT**.

Identifying the Network Type

If you need to determine what type of network is active on a jack, select **Segment ID** from the **Network** menu.

The **Segment ID** screen (Figure 5-2) is displayed:



```
Segment ID
Name:Cisco_3750
Port:
FastEthernet1/0/21
Platform: cisco
WS-C3750-24P
Native VLAN: 1
Appliance VLAN: 196
```

ahn319s.bmp

Figure 5-2. Segment ID Screen

This screen gives you specific details about the connection. It tells you the type of network the tester is plugged into and identifies the port number.

Because not all wall plate connectors are labeled, this information can be especially useful for troubleshooting; for example, when a plate contains multiple jacks and you need to know what's at the other end of the connection.

This screen also tells you which VLAN the tester is connected to. If CDP, LLDP, and EDP information is found, it is also reported on this screen.

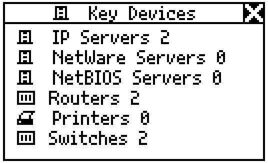
Note

The ***Segment ID*** *screen is identical to the* ***Addresses Used*** *screen documented in Chapter 4. For information on VLANs, LLDP, CDP, and EDP, see "Obtaining a Device's IP Address Information" in Chapter 4.*

Identifying Key Devices

To find out what servers, routers, and printers are available on the network segment, do the following:

1. From the **Main** menu (Figure 1-7), select **Key Devices** to display the **Key Devices** screen (Figure 5-3):



emt36s.bmp

Figure 5-3. Key Devices Screen

Use this information to verify whether a particular device is seen on the network. If there is a configuration problem, this list can help you pinpoint where the problem exists.

The tester always attempts to display the highest level address possible for a device, be it a NetBIOS name, DNS name, IP address or Mac address. This helps you determine which services or servers exist on the network.

2. Select any key device to “drill down” and view specific information (for example, its IP address and subnet mask).

Ping

Ping provides instant information about how a network device is connected and how it is acting on your local segment, making it easier for you to pinpoint connectivity problems.

The tester can automatically ping any single device on your network or a group consisting of up to 10 devices. This section shows you how to set up and run a Ping test.

Note

The Ping option works only in single-ended mode. If you want to ping and are in inline mode, the following message is displayed: "Ping not available when inline". Disconnect the right RJ-45 cable from the tester and then rerun AutoTest to put the tester in single-ended mode.

Assigning an IP Address to the Tester

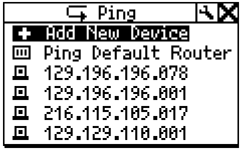
To run Ping, your tester must have a valid IP address. By default, the tester uses DHCP to configure itself. Therefore, if you have DHCP on your network, you do not need to configure the tester's IP address.

If you need to manually assign an IP address, go to "Manually Assigning an IP Address" in Chapter 2 for instructions. When manually configuring the tester's IP address, make sure that the address you assign is correct for the subnet you are in.

Pinging a Single Device

To ping one device, do the following:

1. From the Main menu select **Toolkit**.
2. Select **Ping** to display the **Ping** screen (Figure 5-4):



afq41s.bmp

Figure 5-4. Ping Screen

3. Do one of the following:

   - Select the IP address of the device from the list.

     OR

   - Select **Add New Device** to display the **Edit** screen. On this screen, supply the IP address of the device then press **SELECT** to update the list.

   The tester pings the device and, upon completion, displays results on the **Device Response** screen. To the left of the title of the screen, an icon is displayed that indicates the status of the test (see Table 5-2 for descriptions).

   The tester automatically adds the IP address of the device to a running list (up to 10) of recently pinged devices. If there are more than 10 addresses in the list, the oldest address is deleted to make room for the most recent addition.

NetProve

NetProve can help you troubleshoot connectivity problems by enabling you to determine whether they are caused by the network or some other source, such as a PC, router, or server.

To test connectivity, NetProve works through user-defined catalogs that consist of key devices. NetProve can validate connectivity at the network level (by pinging devices) and at the application level (by communicating with the application port).

Configuring Catalogs

You can define a catalog in any way you want. Following are two typical methods:

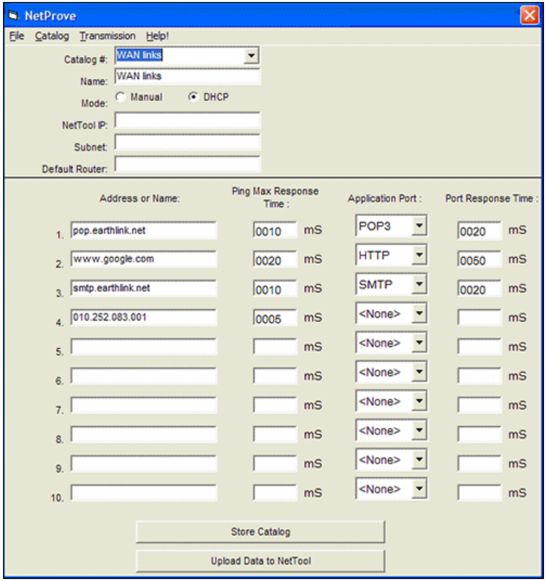
- Create a catalog based on location (premise) validation. In this case, the catalog can consist of email and application servers, routers, and printers as key devices.
- Create a list of key devices needed serially to reach a remote device. The remote device can be a central server at a main office or a server on the internet.

The tester enables you to create up to 10 catalogs, each consisting of up to 10 devices.

To configure a catalog:

1. On the PC, start NetTool Connect.

2. Click **NetProve** to display the **NetProve** configuration screen (Figure 5-5):



Catalog #: WAN links

Name: WAN links

Mode: ○ Manual ● DHCP

NetTool IP:

Subnet:

Default Router:

	Address or Name:	Ping Max Response Time :		Application Port :	Port Response Time :	
1.	pop.earthlink.net	0010	mS	POP3	0020	mS
2.	www.google.com	0020	mS	HTTP	0050	mS
3.	smtp.earthlink.net	0010	mS	SMTP	0020	mS
4.	010.252.083.001	0005	mS	<None>		mS
5.			mS	<None>		mS
6.			mS	<None>		mS
7.			mS	<None>		mS
8.			mS	<None>		mS
9.			mS	<None>		mS
10.			mS	<None>		mS

emt10s.bmp

Figure 5-5. NetProve Configuration Screen

3. Complete the following:

    a. In the top portion screen, supply descriptive information about the catalog.

    b. In the lower half, enter the IP address or DNS name for each key device and specify a ping response time (optional).

Note

***Ping Max Response Time** is used to determine a pass/fail outcome.*

c. If you are testing application connectivity, select an application port (optional) and supply a port response time (optional).

Note

If you supply a port response time, the average port response time of three TCP SYN/ACK cycles is used to determine a pass/fail outcome.

4. On the **File** menu, click **Save** to save the catalog to the PC or click **Transfer Data to NetTool** to download it to the tester.

Some common application ports are listed in Table 5-1. You can view the complete list of IANA registered port numbers at http://www.iana.org/assignments/port-numbers.

Table 5-1. Common Application Ports

Port Number	Port Name	Use
80	http	Web
21	ftp	Remote File Access
25	smtp	Email
23	telnet	Remote terminal
66	sqlnet	Oracle db
161	snmp	Network management

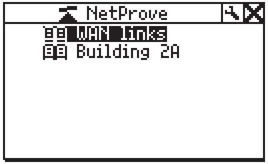
Running NetProve

To run NetProve:

1. Make sure that the desired catalog is transferred to the tester.

2. On the **Main** menu (Figure 1-7), select **NetProve**.

3. On the **NetProve** menu (Figure 5-6), select the desired catalog. For example:

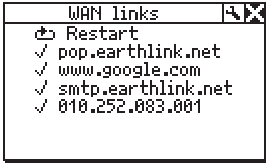


emt11s.eps

Figure 5-6. NetProve Menu

NetProve begins testing the devices in the catalog.

Upon completion, the list of devices is displayed. A check mark (✓) or exclamation (!) appears to the left of the device's name to indicate the status of the ping test (see Table 5-2 for descriptions).

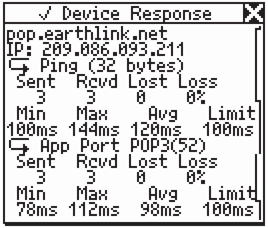


```
WAN links
 Restart
✓ pop.earthlink.net
✓ www.google.com
✓ smtp.earthlink.net
✓ 010.252.083.001
```

emt12s.eps

4. To view details for any device, select it from the list.

   The **Device Response** screen (Figure 5-7) is displayed:



```
 ✓ Device Response        ☒
pop.earthlink.net
IP: 209.086.093.211
↳ Ping (32 bytes)
 Sent  Rcvd Lost Loss
   3    3    0    0%
 Min   Max    Avg   Limit
100ms 144ms 120ms  100ms
↳ App Port POP3(52)
 Sent  Rcvd Lost Loss
   3    3    0    0%
 Min   Max    Avg   Limit
 78ms 112ms  98ms  100ms
```

emt13s.eps

Figure 5-7. Device Response Screen

Note

If you did not specify a Ping or Application response time, the ***Limit*** *field is replaced with --- and the response time is not used to determine a pass/fail outcome.*

Table 5-2. Ping Status Icons

Status Icon	Meaning
⧗	Running
✓	Ping Complete
❗	Problem with the ping. Corresponds with the severity level of problems.
!	Low severity: one packet lost.
!!	Medium severity: two packets lost.
!!!	High severity: three packets lost or the device was not found.

Chapter 6
Common Problems

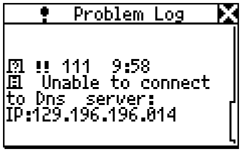
Introduction

The Problem Log includes a listing of all problems that the tester detects from the physical layer to application layer. Not every problem contained in this log is at the same level of severity; therefore, just because a problem is listed here does not imply that it is a catastrophic one.

This chapter shows you how to access the Problem Log and lists the problems that the tester detects. Possible causes and remedies for the problems are provided.

Displaying the Problem Log

Select **Problems** from the **Main** menu (Figure 1-7) to display the **Problem Log** (Figure 6-1):



```
!! 111  9:58
 Unable to connect
to Dns  server:
IP:129.196.196.014
```

afq60s.bmp

Figure 6-1. Problem Log

Understanding the Problem Log Display

There are nine types of problems listed in the Problem Log. Each type of problem has an icon associated with it. For example, a stethoscope 🩺 is used to identify health-related problems. As you become more familiar with using the log, you will learn which icon is associated with a particular type of problem.

Problems are also categorized by severity. A single exclamation mark (!) indicates a low level of severity, while two (!!) and three (!!!) exclamation marks indicate a moderate and high level of severity, respectively.

Each problem listed has a unique problem ID and a short description of the problem that was found.

Table 6-1 lists the types of problems you can see and their associated icons.

Table 6-1. Elements of the Problem Log

Element	Description
Type of Problem	Naming Health Server Host Cable Connectivity Link Configuration Network
Problem Severity	Categorized by three levels of severity: ! Low !! Medium !!! High
Problem ID	A unique identifier that enables you to reference the problem.
Problem Text	Provides a short description of the problem.

Things to Consider

You can think of problems fitting into one of two categories: link connectivity or network. Link connectivity problems relate to cabling or cabling properties while network problems involve PC/network configuration settings or PC-to-server interactions.

Generally, you encounter network problems while setting up or changing a PC’s connection to the network. These types of problems can often be resolved by checking the network settings on the PC.

With a single-ended connection, the tester can only report link connectivity problems. An inline connection is required for all other problems. The different types of connections are discussed in Chapter 2.

The tester enables you to see on which side the problem exists; that is, whether it is a problem between the PC and tester or whether it is between the tester and the network itself. Whether it is a cabling problem or a protocol mismatch, the tester helps you isolate a problem and keep things running.

Detected Problems

This section lists by category the problems that the tester can detect. For each problem, an explanation (if needed) is given and possible corrective steps are provided.

Every network is complex and the solutions given are meant to assist you with troubleshooting. This is not an exhaustive troubleshooting guide.

Link/Connectivity Problems

The problems listed in this section involve cabling or cabling properties.

- **Problem:** *Speed mismatch*

  Explanation: The network is running at 10 Mbps and the PC is running at 100 Mbps (or vice versa). This speed mismatch prevents connection to the network.

  Remedy: Correct the speed mismatch by making sure both devices are running at the same speed.

- **Problem**: *Pair mismatch*

  Explanation: The link pulse is being sourced on the same wire pair by both sides. This problem does not prevent connection to the network. The tester automatically swaps the pairs to correct this problem.

  Remedy: Check the cabling. It may be plugged into an uplink port. Also, there may be a crossover cable between the tester and the device.

- **Problem**: *Duplex mismatch*

  Explanation: One side is running at half duplex and the other side is running at full duplex. This mismatch prevents connection to the network.

  Remedy: Reconfigure the devices so the duplex settings match.

- **Problem**: *Polarity reversed*

  Explanation: The polarity of the detected link pulse is reversed.

  Remedy: This is most likely due to a reversed pair. Check cabling to ensure that the pairing is correct.

- **Problem***: Level low*

  Explanation: The link pulse detected from a device is low. This can negatively affect performance.

  Remedy: Replace the NIC card or change the hub/switch ports. This problem can also be caused by excessive cable attenuation.

- **Problem:** *Transmit pair open*

  Explanation: The wire pair used to transmit (1,2 or 3,6) has an open. This problem prevents connection to the network.

  Remedy: Isolate the cable and replace it.

Network Problems

This section lists all of the network problems. Keep in mind that this is not an exhaustive list of troubleshooting steps. If you know what you need, the network administrator for the network you are troubleshooting can provide you with a lot of information to correct these problems.

Health

- **Problem**: *Short Frames received (also jabber/FCS).*

  Explanation: A short frame is a frame that is smaller than the minimum legal size (less than 64 bytes after the preamble) with a good frame check sequence.

  Jabber is defined as frames longer than the maximum legal size (greater than 1518 bytes).

  Frame Check Sequence (FCS) Bad means that the Preamble and Start Frame Delimiter are correct. The frame is a valid size, but the checksum does not match the data that is in the frame.

  Remedy: Check the NIC card or NIC driver file. This problem can also be caused by cabling or grounding problems.

- **Problem:** *Excessive utilization seen (also collisions).*

  Explanation: Excessive utilization/collisions is defined as a collision rate of greater than 5 percent or a utilization rate of greater than 70 percent.

  Remedy: If this problem exists everywhere on the network, it is most likely caused by excessive traffic. If it is isolated to a single PC, you can suspect cabling.

  For collisions, suspect excessive traffic. Reduce traffic on the network. Check cabling. Change the NIC card or switch/hub port.

  For utilization, reduce the number of stations in the collision domain. Install a switch. Use a tool like the OptiView™ Network Analyzer, EtherScope™ Network Assistant, or OptiView™ Console to determine the top contributors to further segment this network.

NetWare

- **Problem**: *Ethernet frame-type mismatches*.

  Explanation: For the PC and network to communicate, they both must be configured for the same frame type (802.3-raw, 802.2, Ethernet II, and SNAP). You can configure a client for a single frame type. A server can optionally be configured to recognize some or all frame types.

  Remedy: Use the tester to determine the frame types used. If the client is suspected, determine the frame type of the client. Determine the frame types enabled on the server.

- **Problem**: *No nearest server replies seen on network.*

  Explanation: After a PC boots up, it sends a broadcast to initiate a connection with the closest server. If after three attempts there is no response, this problem is listed in the log.

  Remedy: Ensure that GNS (Get Nearest Server) is enabled on the server and check connectivity to routers by doing an IPX ping. Check the Key Devices list. If the routers are listed, the tester is seeing the routers, but the PC is not. You might suspect a bad NIC card or NIC card configuration file.

- **Problem**: *No first responder seen on network. Unable to configure PC network number*.

  Explanation: During boot up, a PC running IPX sends a query to the router asking for its network number. If there is no response after three queries, this problem is listed in the log.

  Remedy: Check connectivity from the PC to the network drop.

TCP/IP

- **Problem**: *PC using incorrect IP subnet mask.*

  Explanation: The tester has determined that the PC is not properly configured.

  Remedy: Access PC network properties and correct the IP subnet mask.

- **Problem**: *Router issued ICMP redirect. Hosts or devices using incorrect gateway/routers.*

  Explanation: The tester has determined that the PC is not properly configured.

  Remedy: Access PC network properties and correct the IP address. You should also make sure that the DHCP server is giving the correct addresses.

- **Problem**: *Duplicate IP detected.*

  Explanation: The tester has detected a duplicate IP address configured on a remote device. You should never have duplicate IPs running on the network. This problem prevents the PC from connecting to the network until it is resolved.

  Remedy: Identify at least one of the devices and change its address to a valid one that is not being used.

Host Configuration

- **Problem**: *BootP/DHCP server not responding.*

  Explanation: The PC is dynamically configured to find DHCP servers and none are found.

  Remedy: Check the router and the DHCP server itself to make sure that they are running. Either could be misconfigured. Check connectivity to the DHCP server.

- **Problem**: *DHCP server issuing IP address that causes duplicate IP on network.*

  Explanation: The DHCP server in question is not detecting an address and is provisioning a duplicate.

  Remedy: This problem can be caused by a statically configured PC. Find the statically configured PC on the network and change its IP address to a valid and unique IP address. Merging two unique networks into one can lead to this type of problem. The problem can also point to an issue with a DHCP server or an implementation bug.

Name Resolution

- **Problem***: No DNS server found on network to resolve names.*

  Explanation: The PC is configured to use DNS (Domain Name Server) and none can be found.

  Remedy: Make sure that the DNS server is up and running. Access the PC's network properties and make sure that the settings are correct.

- **Problem**: *DNS resolution failed.*

  Explanation: There are multiple DNS servers on the network and the PC is configured for the wrong one.

  Remedy: Find out the correct DNS information. Access the PC's network properties and configure the PC with that information.

- **Problem**: *WINS resolution failed.*

  Explanation: The DNS server cannot determine the NetBIOS names.

  Remedy: You can manually fix this problem in the DNS configuration section of network properties.

- **Problem**: *Incorrect WINS server xxx.xxx.xxx.xxx configured on PC.*

  Explanation: There are multiple WINS servers on the network and the PC is configured for the wrong one.

  Remedy: Find out the correct WINS information. Access the PC's network properties and configure the PC with that information.

- **Problem**: *No WINS server found on network to resolve names.*

  Explanation: The PC is configured to use WINS (Windows Internet Name Service) and none can be found.

  Remedy: Make sure the WINS server is up and running. Access the PC's network properties.

- **Problem**: *PC WINS incorrect.*

  Explanation: The tester sees a WINS server on the network but it is not the one configured on the PC in question.

  Remedy: View the details of the WINS server by accessing the **Key Devices** list. Change the PC's configuration to match.

NetBIOS

- **Problem**: *Incorrect Workgroup or Domain configured on PC.*

  Explanation: There are specific names and privileges needed for access to domains or workgroups. The name is not correctly configured or privileges are not set up.

  Remedy: Determine what domain names and privileges are required and correct the PC's configuration.

- **Problem**: *Unable to find Primary Domain Controller (PDC) for network*.

  Explanation: These domain controllers act as gatekeepers for domain access. If one of them is not found on the network, no access can be granted.

  Remedy: Various

- **Problem**: *xxx.xxx.xxx.xxx causing duplicate NetBIOS name.*

  Explanation: Only one unique NetBIOS name is allowed on a domain.

  Remedy: The name specified on the PC needs to be changed to eliminate duplication.

- **Problem**: *PC involved in MB elections*.

  Explanation: The tester sees packets from the PC that are generating master browser elections on the network. This problem can be the source of excessive traffic and slow performance.

  Remedy: Take preventive measures within the PC's configuration to stop the PC from generating Master Browser elections.

Web

- **Problem**: *Unable to connect to HTTP/proxy server*

  Explanation: The standard proxy port is 1080. The HTTP port is 80 on the server.

  Remedy: Correct the naming or port assignments in the setup area of the web browser software.

Email

- **Problem**: *Unable to connect to SMTP mail server*

  Explanation: The Simple Mail Transfer Protocol (SMTP) server information is either not configured or is not correctly configured on the PC. The server itself may be down as well.

  Remedy: Access the **Key Devices** list to view information about this server and then make corrections within the mail setup area of the PC.

- **Problem**: *Unable to connect to POP2 server*

  Explanation: The PC cannot find the POP2 server it is configured to find. The server itself may be down as well.

  Remedy: Access the **Key Devices** list to view information about this server and then make corrections within the mail setup area of the PC.

- **Problem**: *Unable to connect to POP3 server*

  Explanation: The PC cannot find the POP3 server it is configured to find. The server itself may be down as well.

  Remedy: Access the **Key Devices** list to view information about this server and then make corrections within the mail setup area of the PC.

- **Problem**: *Unable to connect to IMAP server*

  Explanation: The PC cannot find the IMAP server it is configured to find. The server itself may be down as well.

  Remedy: The IMAP server information is either not configured or is not correctly configured on the PC. Access NetTool's **Key Devices** list to view information about this server.

Printer

- **Problem**: *Unable to connect to IP print spool server*

  Explanation: NetTool is detecting that the PC is not able to connect to the configured IP printer server. The server itself may be down as well.

  Remedy: Access NetTool's **Key Devices** list to view a list of IP printers and correct the problem in the printer setup area on the PC.

- **Problem**: *Unable to connect to IP print spooler*

  Explanation: The print spooler configuration on the PC is either not correct or the spooler itself is down or offline.

  Remedy: Check the spooler itself and then access NetTool's **Key Devices** list to view a list of IP devices and correct the problem in the printer setup area on the PC.

Chapter 7
Verifying Voice over IP Service

Introduction

With the VoIP (Voice over IP) option enabled, you can verify VoIP service on a link. The tester can track SCCP/SIP and H.323 call control and measure RTP quality of service. The VoIP Log and VoIP Monitor capture call transactions, providing you with a step-by-step record of major events so that you can troubleshoot problems with VoIP service.

Note

Keeping your tester updated ensures that you have access to new call control protocols as they become available. For update instructions, see "Updating the Tester's Software" in Chapter 1.

Running AutoTest

To begin testing VoIP service, do the following:

1. Connect the tester inline between the network and the VoIP phone (see "Inline Connection" in Chapter 2).
2. Run AutoTest (see" Running AutoTest" in Chapter 3).

Viewing PoE Information (if applicable)

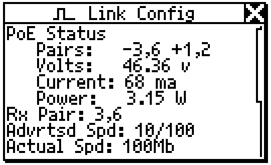
After you run AutoTest, you can obtain PoE voltage, current, and pair information for the network or phone side. Do the following:

1. Depending on which side you want to look at, select one of the following icons:

   - PC icon:
   - Network icon: .

   The **Station** menu (PC icon) or **Network** menu (Network icon) is displayed.

2. Select **Link Config** to display this screen:



```
    Link Config
PoE Status
   Pairs:   -3,6 +1,2
   Volts:   46.36 v
   Current: 68 ma
   Power:   3.15 W
Rx Pair: 3,6
Advrtsd Spd: 10/100
Actual Spd: 100Mb
```

fluke019 .bmp

Figure 7-1. Link Configuration Screen

PoE voltage, current, and pair information are displayed. This information is updated every two seconds.

Viewing VLAN, CDP, LLDP and EDP Information

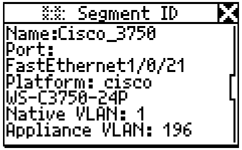
The tester reports VLAN, CDP, LLDP and EDP information (if found) for both the phone side and the network side.

- To look at the phone side, select the PC icon . Then on the Station menu, select Addresses Used.
- To look at the network side, select the Network icon . Then, on the **Network** menu, select Segment ID.

The **Addresses Used** and **Segment ID** screens show the same VLAN, CDP, LLDP, and EDP information. See “Obtaining a Device’s IP Address Information” in Chapter 4 for a description of the information on these screens.

VLAN, CDP, LLDP, and EDP information is updated every two seconds. You can monitor VLANs during a call to see which ones are being used (see entries in the “VoIP Logs” in Appendix B).

When plugged into a switch VLAN port, the native and appliance (phone) VLANs are also displayed along with the CDP information, as shown in Figure 7-2:



```
Segment ID
Name:Cisco_3750
Port:
FastEthernet1/0/21
Platform: cisco
WS-C3750-24P
Native VLAN: 1
Appliance VLAN: 196
```

ahn320s.bmp

Figure 7-2. VLAN Port Information

The VoIP Log

The VoIP Log is a per-call event log that records major SCCP/SIP and H.323 call control and RTP events and measurements.

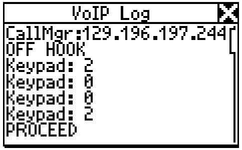
To access the log, do the following:

1. From the **Main** menu (Figure 1-7), select **Applications**.
2. On the **Applications** menu, select **VoIP Log** to display the **VoIP Log** screen.

You can use the VoIP Log to watch events that occur as the phone boots up and subsequently to monitor a call that is in progress.

During the boot process, the log captures the exchanges between the phone and the network. When the phone goes "off hook", the boot information is cleared and transactions between the parties are recorded. Call quality and QoS statistics are logged for both sides.

Figure 7-3 shows an example of a VoIP Log entry. Depending on the length of a call, the VoIP Log may have several pages of screens. To page up or down, press the Up ▲ or Down ▼ arrow keys.



```
CallMgr:129.196.197.244
OFF HOOK
Keypad: 2
Keypad: 0
Keypad: 0
Keypad: 2
PROCEED
```

ahn321s.bmp

Figure 7-3. VoIP Log

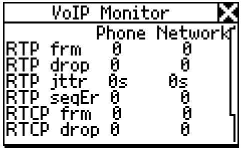
Appendix C contains sample SCCP and SIP boot and call logs. The logs are fully commented to give you idea of what happens during the boot process and while a call is in progress. You can also look at the parameters that are tracked from the start of a call until the far-end phone goes “on hook”.

Viewing Call Quality Measurements

The VoIP Monitor tracks call quality (RTP data). To display the VoIP Monitor, do the following:

1. From the Main menu (Figure 1-7), select **Applications**.

2. On the **Applications** menu, select **VoIP Monitor** to display the screen shown in Figure 7-4:



```
        VoIP Monitor
            Phone Network
RTP frm     0       0
RTP drop    0       0
RTP jttr    0s      0s
RTP seqEr   0       0
RTCP frm    0       0
RTCP drop   0       0
```

ahn309s.bmp

Figure 7-4. VoIP Monitor

The VoIP Monitor includes RTP statistics and RTCP information (when present) for both the phone side and the network side. You can view this data this while a call is in progress.

Table 7-1 defines the RTP and RTCP statistics seen on this screen.

Table 7-1. VoIP Monitor RTP/RTCP Statistics

Statistic	Meaning
RTP frm	The number of RTP frames.
RTP drop	The number of dropped RTP frames. An RTP frame is considered dropped when it does not arrive within 16 frames.
RTP jttr	The difference between the maximum and minimum frame inter-arrival time. This is an unbuffered measurement of the raw packet arrival times.

Table 7-2. VoIP Monitor RTP/RTCP Statistics (continued)

Statistic	Meaning
RTP seqEr	The number of frames that arrived out of sequence but within the 16-frame-drop window.
RTCP[1] frm	The number of RTP frames.
RTCP[1] drop	The number of dropped packets as measured, post buffer, by the endpoint.
RTCP[1] jttr	The amount of jitter as reported by the endpoint.

[1] RTCP is an optional control protocol that is sent from the RTP endpoints. It contains call quality information as reported by the two RTP endpoints involved in the conversation.

Chapter 8
Using NetSecure

Introduction

The NetSecure Option allows you to setup port monitoring, 802.1X authentication, and 802.1X logging (recording the connection log). The 802.1X logging feature allows you to view the inline or NetTool (client) 802.1X authentication sequence.

This chapter shows you how to setup ports to monitor, setup and enable 802.1X authentication, and view the 802.1X connection log.

Before You Begin

Make sure that you install the NetTool Connect PC application. This program is found on the CD that is packaged with the tester. See “NetTool Connect” in Chapter 1 for installation instructions.

Port Monitoring

Spyware/malware on a PC compromises security (theft of passwords, financial information, confidential files) and can degrade PC performance. This could include CPU and memory used to track internet usage and report it to an advertising agency.

Also, sometimes, it is difficult to verify whether a firewall is properly configured. An improperly configured firewall can compromise network security. Use the Port Monitor feature to verify the ports that are suppose to be enabled through your firewall settings.

Using NetTool Connect, you can configure the NetTool Series II with the application ports you expect the PC to utilize during routine operation. After ruling out the network as the source of the reported slow performance, you can connect the NetTool Series II inline between the PC under test and the network to determine if spyware is to blame. The NetTool Series II displays all port activity. Traffic to unexpected ports is a strong indication of an infected PC.

Setting Up Ports to Monitor

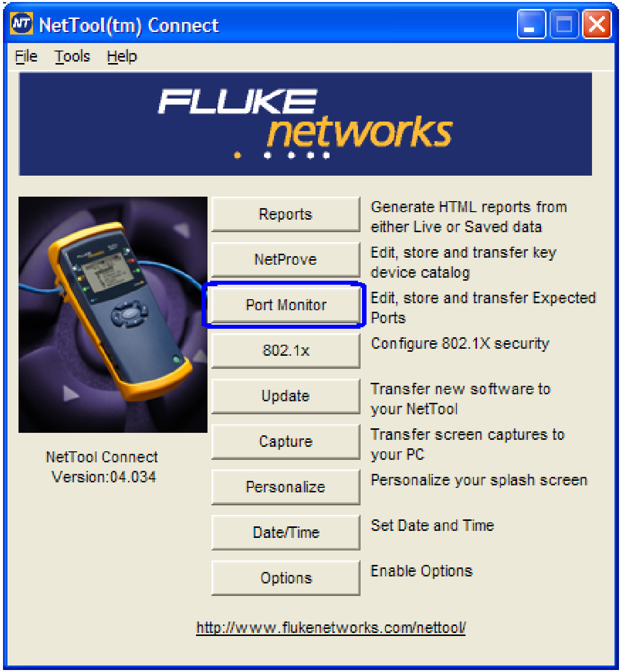
Note

> *It is assumed you have entered the option key in NetTool Connect to enable this option. The option is called NetSecure.*

To setup the ports to monitor on NetTool Series II:

1. Connect the NetTool Series II to your PC using the supplied USB cable.

2. Open the NetTool Connect application and select **Port Monitor**.

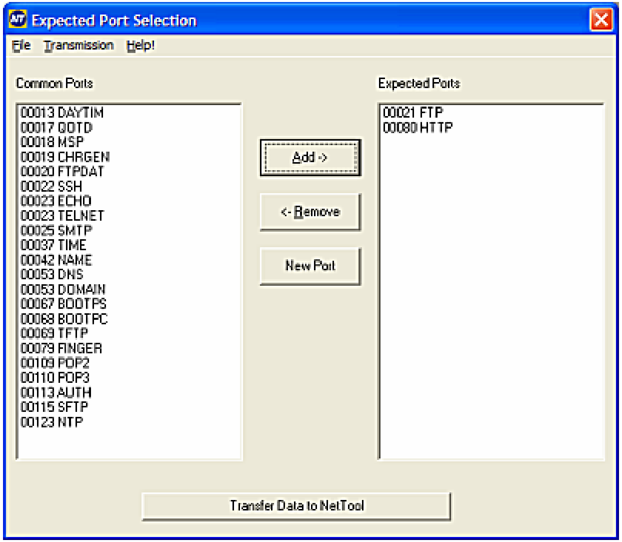


Reports	Generate HTML reports from either Live or Saved data
NetProve	Edit, store and transfer key device catalog
Port Monitor	Edit, store and transfer Expected Ports
802.1x	Configure 802.1X security
Update	Transfer new software to your NetTool
Capture	Transfer screen captures to your PC
Personalize	Personalize your splash screen
Date/Time	Set Date and Time
Options	Enable Options

nettoolconnect1.bmp

Figure 8-1. NetTool Connect Main Screen

3. Highlight each port in the list and select **Add** to move the port identifier to the Expected Ports column. You can also select **New Port** to add a custom defined port to the Expected Ports column.



Common Ports

00013 DAYTIM
00017 QOTD
00018 MSP
00019 CHRGEN
00020 FTPDAT
00022 SSH
00023 ECHO
00023 TELNET
00025 SMTP
00037 TIME
00042 NAME
00053 DNS
00053 DOMAIN
00067 BOOTPS
00068 BOOTPC
00069 TFTP
00079 FINGER
00109 POP2
00110 POP3
00113 AUTH
00115 SFTP
00123 NTP

Expected Ports

00021 FTP
00080 HTTP

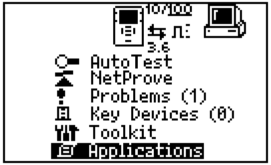
port2.bmp

Figure 8-2. Expected Port Selection Screen with Ports Added

4. Select **Transfer Data to NetTool** and the Expected Ports list is copied to the NetTool Series II. This may take a few minutes to complete.

Using Port Monitor on the NetTool Series II

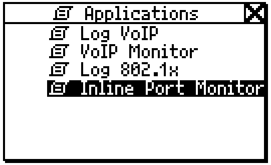
1. After **Autotest** has run, select **Applications** on the main screen.



fluke007.bmp

Figure 8-3. Main NetTool Screen

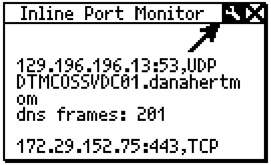
2. Select **Inline Port Monitor**.



fluke008.bmp

Figure 8-4. Applications Screen

3. Select the tool icon.



Inline Port Monitor

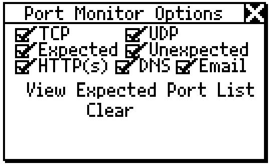
```
129.196.196.13:53,UDP
DTMCOSSVDC01.danahertm
om
dns frames: 201

172.29.152.75:443,TCP
```

fluke009.bmp

Figure 8-5. Inline Port Monitor Screen

4. Select the protocols and ports you want or don't want to display in the Port Monitor Options screen.



Port Monitor Options

☑ TCP ☑ UDP
☑ Expected ☑ Unexpected
☑ HTTP(s) ☑ DNS ☑ Email

View Expected Port List
Clear

fluke020.bmp

Figure 8-6. Port Monitor Options Screen

If you are NOT uploading a ports list from the NetTool Connect PC application, check **Unexpected**. All data that the NetTool Series II sees with be displayed with "unexpected" in the Inline Port Monitor screen.

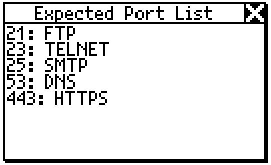
Expected displays the data that matches the uploaded port list and is pre-empted with "expected" in the Inline Port Monitor screen.

You may further filter with "only" **TCP** frames and/or only **UDP** frames for both the **Expected** and **Unexpected** settings.

HTTP(s), **DNS**, and/or **Email** are separate settings from the ones described above. If **HTTP(s)**, **DNS**, and/or **Email** are checked, frames that match their protocol will be displayed in the Inline Port Monitor screen.

HTTP: ports 80, 443
DNS: port 53
Email: ports 110, 143, 993, 995

View Expected Port List allows you to view the port list uploaded from the NetTool Connect PC application's Expected Port Selection screen. A sample is given on the next page.

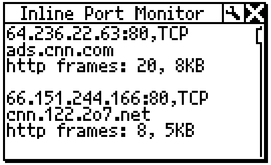


```
Expected Port List
21: FTP
23: TELNET
25: SMTP
53: DNS
443: HTTPS
```

fluke021.bmp

Figure 8-7. Sample Uploaded Port List

Clear empties the Inline Port Monitor 50 line capture buffer. New data is then captured. Running **Autotest** will also clear the buffer.



```
Inline Port Monitor
64.236.22.63:80,TCP
ads.cnn.com
http frames: 20, 8KB

66.151.244.166:80,TCP
cnn.122.2o7.net
http frames: 8, 5KB
```

fluke0010a.bmp

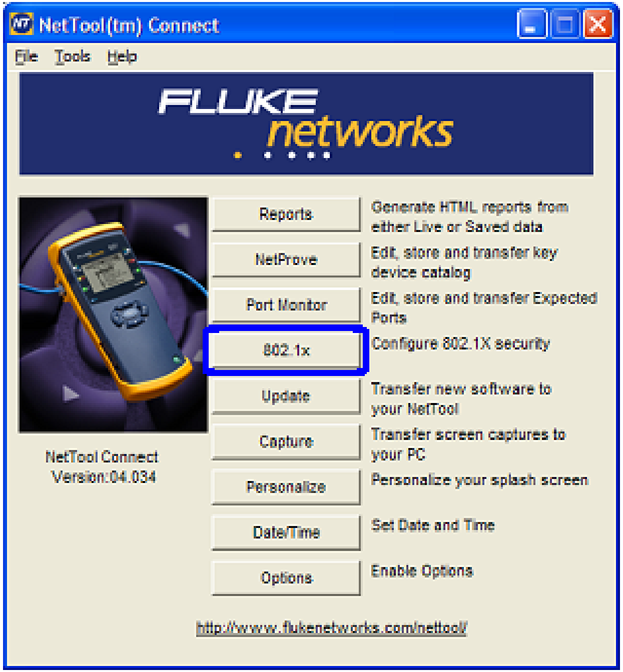
Figure 8-8. Inline Port Monitor Screen with Data

In Figure 8-8, the first list displays the IP address, port number and protocol. The second line displays the resolved DNS information (if available), and the third line displays the uploaded port information (if available) frame type, the number of frames, and the traffic size.

Configuring 802.1X on your NetTool Series II

To setup the NetTool Series II to 802.1X authenticate on your network:

1. Open the NetTool Connect application and select **802.1X**.



NetTool Connect
Version:04.034

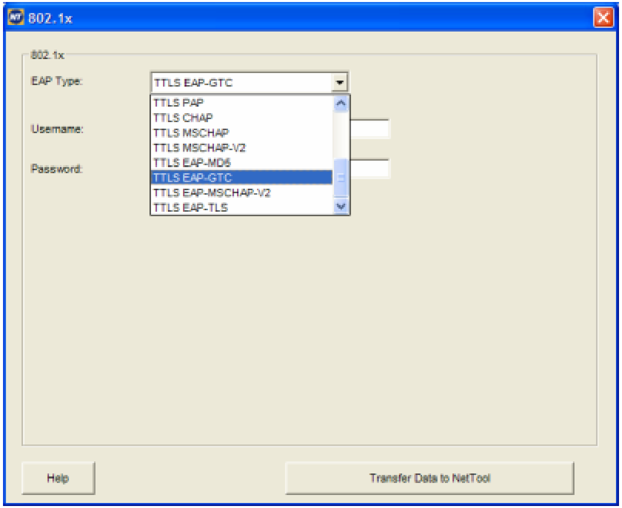
Reports	Generate HTML reports from either Live or Saved data
NetProve	Edit, store and transfer key device catalog
Port Monitor	Edit, store and transfer Expected Ports
802.1x	Configure 802.1X security
Update	Transfer new software to your NetTool
Capture	Transfer screen captures to your PC
Personalize	Personalize your splash screen
Date/Time	Set Date and Time
Options	Enable Options

http://www.flukenetworks.com/nettool/

netoolconnect4.bmp

Figure 8-9. Selecting 802.1X Security

2. In the 802.1X setup screen, select the **EAP Type**. This information is unique to each network. Some use certificates, others use login information.



802.1x

802.1x

EAP Type: TTLS EAP-GTC

- TTLS PAP
- TTLS CHAP
- TTLS MSCHAP
- TTLS MSCHAP-V2
- TTLS EAP-MD5
- TTLS EAP-GTC
- TTLS EAP-MSCHAP-V2
- TTLS EAP-TLS

Username:

Password:

8021x_setup.bmp

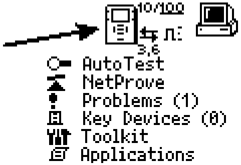
Figure 8-10. Selecting an EAP Type

3. When you have selected the correct authentication method and configured it correctly, select **Transfer Data to NetTool**.

Using the NetTool as an 802.1X Authenticated Client

Once you have successfully uploaded the 802.1X authentication setup from NetTool Connect, perform the following:

1. On the main screen, highlight and select the NetTool icon.

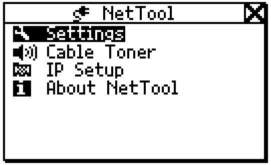


AutoTest
NetProve
Problems (1)
Key Devices (0)
Toolkit
Applications

fluke011.bmp

Figure 8-11. Select the NetTool Icon

2. Select **Settings**.



NetTool

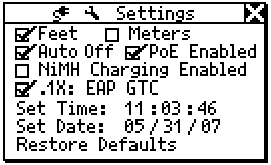
Settings
Cable Toner
IP Setup
About NetTool

fluke012.bmp

Figure 8-12. Select Settings

3. Select **.1X: (802.1X type)** to use 802.1X authentication.

Figure 8-13. Enabling 802.1X to Authenticate



Settings

☑ Feet ☐ Meters
☑ Auto Off ☑ PoE Enabled
☐ NiMH Charging Enabled
☑ .1X: EAP GTC
Set Time: 11:03:46
Set Date: 05/31/07
Restore Defaults

emt14s.bmp

Note

*In Figure 8-13, the 802.1X authentication type **EAP GTC** has been uploaded to the NetTool and is displayed as **.1X: EAP GTC**.*

*When connecting to a non-802.1X authenticated network, make sure the **.1X: (802.1X type)** checkbox is NOT checked. If you are experiencing problems with **Autotest**, this setting may need to be changed.*

Viewing the 802.1X connection Log

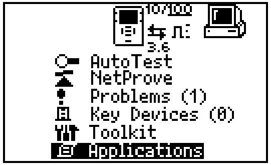
You may either connect the NetTool Series II inline and view the 802.1X connection sequence between a PC and your network, or connect the NetTool Series II single-ended to the network and view its' connection sequence as it tries to authenticate as a client.

Note

*When capturing an inline 802.1X connection sequence, make sure **.1X: (802.1X type)** is NOT checked in the Settings screen (see figure 8-13). If **.1X: (802.1X type)** is checked, the NetTool Series II will try to perform a single-ended 802.1X authenticate and interfere with capturing the inline 802.1X connection sequence between the two devices.*

To view the connection sequence:

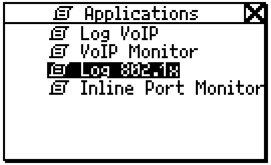
1. From the main screen, select **Applications**.



fluke007.bmp

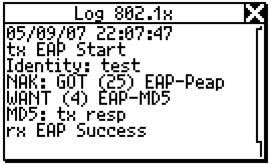
Figure 8-14. Select Applications

2. Select **Log 802.1X** to view the connection log.



fluke014.bmp

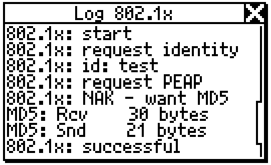
Figure 8-15. Log 802.1X



```
05/09/07 22:07:47
tx EAP Start
Identity: test
NAK: GOT (25) EAP-Peap
WANT (4) EAP-MD5
MD5: tx resp
rx EAP Success
```

log md5 .bmp

Figure 8-16. 802.1X Single-ended Connection Log



```
802.1x: start
802.1x: request identity
802.1x: id: test
802.1x: request PEAP
802.1x: NAK - want MD5
MD5: Rcv    30 bytes
MD5: Snd    21 bytes
802.1x: successful
```

fluke010a.bmp

Figure 8-17. 802.1X Inline Connection Log

In Figure 8-17, the server tries to request an 802.1X PEAP authenticate and the client sends an 802.1X MD5 authentication request, which the server accepts.

Chapter 9
Creating and Managing Reports

Introduction

The Reporter feature and NetTool Connect software enable you to capture device and network configuration data and save that information in a report.

This chapter shows you how to create and manage your reports. You can use these reports to do the following:

- Document configurations for groups of users (for example, Customer Service, Marketing, and Technical Support)
- Escalate trouble tickets by documenting a problem device
- View and print data you gather related to setups, moves, adds, or changes.

Before You Begin

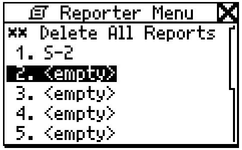
Make sure that you install NetTool Connect. This program is found on the CD that is packaged with the tester. See "NetTool Connect" in Chapter 1 for installation instructions.

Creating and Saving Reports in the Tester

You can create and save up to 10 reports in the tester's non-volatile memory.

To create a report:

1. Connect the tester to the device you want to check and run AutoTest.
2. After AutoTest is completed, select **ToolKit** from the **Main** menu (Figure 1-7).
3. Move the cursor to **Reporter**, then press **SELECT** to display the **Reporter Menu** (Figure 9-1):



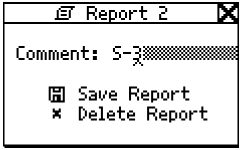
```
Reporter Menu
** Delete All Reports
 1. S-2
 2. <empty>
 3. <empty>
 4. <empty>
 5. <empty>
```

afq52s.bmp

Figure 9-1. Reporter Menu

4. Move the cursor to an **<empty>** slot. Then, press **SELECT.**

   A **Report** screen similar to that shown in Figure 9-2 is displayed:



Report 2

Comment: S-3

afq53s.bmp

Figure 9-2. Report Screen

5. In the **Comment** field, supply a name for the report. To do this:

   Note

   You can use up to 20 alphanumeric characters for the report name. Characters include spaces and special symbols, such as the period (.) and pound sign (#).

   a. Press the Down ▼ arrow key to move the cursor to the **Comment** field.

   b. Press the **Right** ▶ arrow key to move the cursor to the first position. Then, press the **Up** or **Down** ▲▼ arrow key until the desired alphanumeric character is displayed.

c. Press the **Right** ▶ arrow key to move to the next position and select the desired alphanumeric character. Continue in this manner until the desired name of the report is displayed.

d. Press **SELECT**.

The **Comment** field flashes.

6. To save the report, press the Down ▼ arrow key to move the cursor to **Save Report**. Then, press **SELECT** to save.

The **Reporter Menu** is displayed and the name you created appears in the list.

Note

If you inadvertently give two reports the same name on the tester, check the date/time stamp when you view the reports to differentiate between them.

Viewing Reports Saved in the Tester

To view a saved report:

1. Start NetTool Connect.
2. From the **Reports** menu, select **Get Saved.**
3. Select the desired report from the list of saved reports.
4. After the report is downloaded, select the information that you want included in the report.
5. Click OK to display the report.

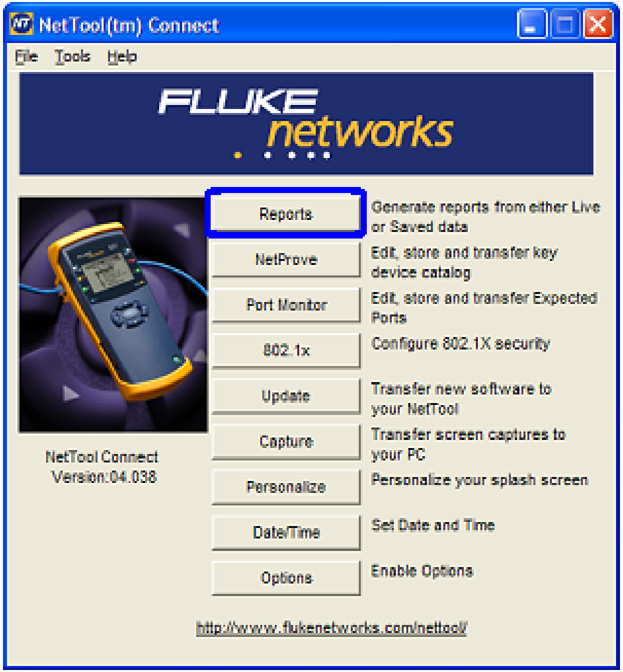
Generating a Live Data Report

You can use NetTool Connect generate a live data report. Live data reflects what the tester currently detects on the PC (or another device) and/or the network.

To generate a live data report:

1. Turn on the tester and connect it to a USB port on the PC.
2. Start the NetTool Connect program on the PC.

   The **NetTool Connect** startup screen (Figure 9-3) is displayed:



Reports	Generate reports from either Live or Saved data
NetProve	Edit, store and transfer key device catalog
Port Monitor	Edit, store and transfer Expected Ports
802.1x	Configure 802.1X security
Update	Transfer new software to your NetTool
Capture	Transfer screen captures to your PC
Personalize	Personalize your splash screen
Date/Time	Set Date and Time
Options	Enable Options

NetTool Connect
Version:04.038

http://www.flukenetworks.com/nettool/

fluke18.bmp

Figure 9-3. Selecting Reports

3. Click Reports to display the **NetTool Reports** screen.

4. From the **Reports** menu, select **Get Live.**

   Live data is downloaded to the tester.

5. On the **Report Contents** screen, select the data that you want to include in the report.

6. Click OK. to display the report.

Saving a Live Data Report to a PC

You can save a live data report to a PC in three file types: html, pdf, and raw.

1. With the live data report displayed, select one of the following from the **NetTool Reports File** menu:
   - **Save Report** to save the report as an .html file
   - **Save as PDF** to save the report as a .pdf file
   - **Save RAW** file to save the report as a .raw file
2. Click Save to save the file to the PC.

Viewing Reports Saved to the PC

To view a report saved to the PC:

1. Start NetTool Connect.
2. Click Reports to display the **NetTool Reports** screen.
3. From the **File** menu, select **Open**.
4. In the **Files of Type** box, select file type.

   A list of files of the type you selected is displayed.
5. From the list, select the desired file. Then, click Open to view the contents of the report.

Printing a Report

To print a report:

1. Start NetTool Connect.

2. Click Reports to display the **NetTool Reports** screen.

3. Display the file that you want to print.

   Note

   *Select **Reports** > **Get Live** or **Get Saved** or select **File** > **Open** to display the desired report.*

4. From the **File** menu, select **Print**.

Deleting a Report

You can use NetTool Connect or the tester to delete a report.

Using NetTool Connect

1. Click Reports to display the **NetTool Repor**ts screen.

2. From the **Reports** menu, select **Delete**.

3. Select the individual report that you want to delete or select **Delete All**.

Using the Tester

1. From the **Main** menu (Figure 1-7), select **ToolKit**.
2. Move the cursor to **Reporter**, then press **SELECT** to display the **Reporter Menu** (Figure 9-1).
3. Do *one* of the following;
   - To delete all reports, select **Delete All Reports**.
   - To delete a single report, move the cursor to the report. Then, select **Delete Report**.
   - To overwrite a report, move the cursor to the report. Then, select **Overwrite Report**.

Note

When you overwrite a report, its contents are replaced with current (live) data.

Appendices

Appendix **Title** **Page**

Appendix A
Specifications

General Specifications

Media Access	10/100/1000 Base-TX and PoE (802.3af)
Cable Tests	Internal wiremap, WireView Cable ID, cable length, opens, shorts, and split pairs
Cable Toner	IntelliTone or Analog (each with two songs)
Cable Length	Accuracy is +/- (10 % of reading plus 1 meter)
Ports	Shielded Hub/NIC connector (RJ-45) and USB input jack

General Specifications (continued)

Interface	Push button navigation of icon/menu-driven view
Battery	Removable alkaline batteries or optional rechargeable NiMH AA batteries
AC Adapter	Separately purchased option available from Fluke Networks. Input: 100-240 VAC, 50-60 Hz, 0.6 A. Output: 15 VDC, 1.2 A.
Dimensions	19.0 cm x 8.9 cm x 4.4 cm (7.5” x 3.5” x 1.75”)
Weight	0.54 kg (1 lb 3 oz.)
Warranty	One year (extended warranty available)
LED Indicators (8)	10/100/1000 (Link), CLSN/ERR (Collision/Error), UTIL (Utilization), PoE, and CHARGE

Environmental Requirements

Operating Temperature	10 °C to 30 °C with up to 95 % Relative Humidity 10 °C to 40 °C with up to 75 % Relative Humidity
Non-Operating Temperature	-20 °C to +60 °C
Approvals	The NetTool Series II tester has the following approvals: European Standard EN 60950, CSA/CAN C22.2 No. 950, and UL 1950.
Approvals (Accessories)	The optional Universal AC Adapter for NetTool has UL, CSA, and TÜV approvals or other approvals valid in the USA, Canada, and Europe.
Electromagnetic Interference	The NetTool Series II tester complies with European standard EN 61326 Class B.
Certifications	Complies with European CE directive: EMC directive 89/336/EEC and low voltage directive 73/23/EEC.
Connection to public telephone network	The NetTool Series II tester should never be connected to the public telephone network.

Appendix B
Sample VoIP Call Logs

Introduction

This appendix contains sample SCCP and SIP call logs. All of the logs contain running commentaries to familiarize you with the messaging and information that is exchanged during a call.

Typical Cisco Skinny (SCCP) Phone Bootup

```
>DHCP DISCOVER                 // the phone broadcasts an IP address request
00c017a00079                   // the MAC address of the phone
>DHCP OFFER                    // the DHCP server offers an address
129.196.197.016                // the offered IP address
>DHCP REQUEST                  // the phone requests the offered address
003094c4426f
>DHCP ACK                      //the server acknowledges the request
129.196.197.016

>DNS req:003094c4426f          // the phone requests the Call Manager IP
CiscoCM1.danahertm.com
<DNS response                  // the DNS server responds with the Call Manager's address
129.196.197.244
>TFTP file request             // the phone uses TFTP to get operating files
OS79XX.TXT
>TFTP file request
SEP003094C4426F.cnf.xml

>ALARM TO CM                   // the phone signals the Call Manager
25: Name=SEP003094C4426F
>REGISTER WITH CM              // and registers with the Call Manager
ip:129.196.197.016
name:SEP003094C4426F
```

Typical Cisco Skinny (SCCP) Phone Bootup (continued)

```
<REGISTER_ACK                  // the Call Manager acknowledges the registration
>CAPABILITY_REQUEST            // the phone asks about its capabilities
<CAPABILITY_RESULT             // the Call Manager replies
>TFTP file request             // the phone TFTPs down three more files
SEP003094C4426F.cnf.xml
>TFTP file request
RINGLIST.XML
>TFTP file request
DISTINCTIVERINGLIST.XML
>CDP                           // the phone sends out CDP packets periodically
SEP003094C4426F
Cisco IP Phone 7960
```

Typical Cisco Skinny (SCCP) Call Log

Following is a sample SCCP call log. Events in the exchange are shown on the left. Commentary appears on the right to help you follow the sequencing of the exchange. The log captures an entire phone transaction, starting with the phone going OFF HOOK:

```
CallMgr:129.196.197.244       // Call manager IP address
OFF HOOK                      // Phone goes off hook
Keypad: 2                     // x2002 is dialed
Keypad: 0
Keypad: 0
Keypad: 2

PROCEED                       // Call manager acknowledges
>2000,Blade Lab               / /the two parties in the call
<2002,

RING OUT                      // far end is ringing
CONNECTED                     // far end has picked up

>2000,Blade Lab
<2002,

START MEDIA XMIT              // media transmission is to start

G711 Ulaw64k                  // the CODEC being used
Call Setup: 104ms             // the time from CONNECTED to RTP
```

Typical Cisco Skinny (SCCP) Call Log (continued)

```
RTP streaming…                 // the conversation has started
129.196.197.023:30142          // phone 1 IP address and port number
VLAN:untag TOS:0xb8            // phone 1 VLAN and TOS being used
129.196.197.016:20828          // phone 2 IP address and port number
VLAN:untag TOS:0xb8            // phone 2 VLAN and TOS being used
Call Duration:9.51s            // the length of the call
ON HOOK                        // the phone is hung up

>RTP cnt:475frms               // phone 1 stats—the number of RTP frames
Jitter:994us                   // the inter-frame arrival jitter
Arrival Avg:19ms               // the average arrival of the frames
Min:19ms Max:20ms              // the minimum and maximum inter-arrival time
Drop:3fr                       // the number of dropped frames
DropBurst:61ms                 // the longest dropout
```

Typical Cisco Skinny (SCCP) Call Log (continued)

```
<RTP cnt:476fr                    // phone 2 stats
Jitter:1ms
Arrival Avg:20ms
Min:19ms Max:20ms
Drop:0fr
DropBurst:0s
Call Complete
```

Typical SIP Phone Bootup Log

```
  >DHCP DISCOVER                 // the phone broadcasts an IP address request
  000f66fc9e72                   // the MAC address of the phone
  >DHCP OFFER                    // the DHCP server offers an address
  129.196.196.202                // the offered IP address
  >DHCP REQUEST                  // the phone requests the offered address
  000f66fc9e72
                                 // the server acknowledges the request
  >DHCP ACK
  129.196.196.202
                                 // the phone uses DNS to look up the gateway
  >DNS req:000f66fc9e72
  atlas4.atlas.vonage.net
                                 // the DNS server responds with the IP address
  <DNS response
  216.115.025.056
  REGISTER sip:atlas4.atla       // the phone registers
  200 OK

>DNS req:000f66fc9e72          // the phone looks up the time server
time.vonage.net
<DNS response
216.115.031.140
REGISTER sip:atlas4.atla       // the phone does a periodic heartbeat register
200 OK
```

Typical SIP Phone Bootup Log (continued)

```
>DNS req:000f66fc9e72          // the phone looks up the FTP file server
ls.tftp.vonage.net
<DNS response
192.015.192.015                // the DNS server responds with the IP address

>TFTP file request             // the phone downloads its operating file
/uObE8NkRvq/spa000F66FC9
REGISTER sip:atlas4.atla       // the phone sends periodic heartbeat registration
200 OK                         // the gateway responds
REGISTER sip:atlas4.atla
200 OK
```

Typical SIP Call Log

```
INVITE sip:5983842@atlas            // the phone invites the other party
407 Proxy Authentication
ACK sip:5983842@atlas4.a            // the gateway acknowledges the number
INVITE sip:5983842@atlas

100 Trying                          // the gateway tries connecting
180 Ringing                         // the far end is ringing
180 Ringing
200 OK                              // we have a connection
SIP RTP port 12436                  // the RTP port number to be used
ACK sip:17195983842@216.
Call Setup:213ms                    // the call setup time

RTP streaming...                    // the conversation has started
129.196.196.202:10106               // phone 1 IP address and port number
VLAN:untag TOS:0xb8                 // phone 1 VLAN and TOS being used
216.115.023.031:12436               // phone 2 IP address and port number
VLAN:untag TOS:0x0                  // phone 2 VLAN and TOS being used
BYE sip:17195983842@216.            // the phone goes back on hook
```

Typical SIP Call Log (continued)

```
>RTP cnt:2186fr              // phone 1 stats—the number of RTP frames
Jitter:21ms                  // the inter-frame arrival jitter
Arrival Avg:19ms             // the average arrival of the frames
Min:7ms Max:29ms             // the minimum and maximum inter-arrival time
Drop:23fr                    // the number of dropped frames
DropBurst:21ms               // the longest dropout

<RTP cnt:2233fr              // phone 2 stats
Jitter:162ms
Arrival Avg:19ms
Min:830us Max:163ms
Drop:0fr
DropBurst:0s
Call Complete
```

Appendix C Glossary

10BASE2
Sometimes called ThinLAN or CheaperNet, 10BASE2 is the implementation of the IEEE 802.3 Ethernet standard on thin coaxial cable. The maximum segment length is 185 meters.

10BASE5
Sometimes called ThickLAN, 10BASE5 is the implementation of the IEEE 802.3 Ethernet standard on thick coaxial cable. The maximum segment length is 500 meters.

10BASEF

A point-to-point fiber link. This is the draft specification for IEEE 802.3 Ethernet over fiber optic cable.

10BASE-T

10BASE-T is the implementation of the IEEE 802.3 Ethernet standard on unshielded twisted-pair wiring. It is a star topology, with stations directly connected to a multi-port Hub, and it has a maximum cable length of 100 meters.

100BASE-TX

100BASE-TX is the implementation of the IEEE 802.3u Ethernet standard on two pairs of unshielded twisted-pair wiring. It is a star topology with a maximum cable length of 100 meters. The maximum network diameter is 205 meters with two class II repeaters.

802.2

This IEEE standard specifies Logical Link Control (LLC), which defines services for the transmission of data between two stations at the data-link layer of the OSI model.

802.3

Often called Ethernet, this IEEE standard governs the Carrier Sense Multiple Access/Collision Detection (CSMA/CD) networks. Typical cabling standards are 10BASE-T, 10BASE2, and 10BASE5.

Access Method

The set of rules by which the network determines what node has access to the network. The two most popular access methods are Carrier Sense Multiple Access/Collision Detection (Ethernet) and token passing (Token Ring and ARCNET).

Anomaly

An impedance discontinuity causing an undesired signal reflection on a transmission cable.

AppleTalk

AppleTalk is a networking protocol primarily used for communications between Macintosh computers and Apple printers. The AppleTalk network is segmented into zones.

ARP (Address Resolution Protocol)

A member of the TCP/IP protocol suite, ARP is the method by which a station’s MAC address is determined given a station’s IP (Internet Protocol) address.

Attenuation

A reduction in the strength of a signal; the opposite of gain.

Bandwidth

Bandwidth is the rate at which data can be transmitted over a channel, measured in bits per second. For example, Ethernet has a 10 Mbps bandwidth and FDDI has a 100 Mbps bandwidth. Actual throughput is almost always less than the theoretical maximum.

BPS

Bits per second. A measure of speed or raw data rate. Often combined with metric prefixes as in kbps (for thousands of bits per second) or Mbps (for millions of bits per second).

Bridge (Switch)

A device that links two or more networks that use the same OSI Data Link protocol. A bridge evaluates source and destination addresses to pass only frames that have a destination on the connecting network.

Broadcast

A message that is addressed to all stations on a network. For Ethernet networks, the MAC broadcast address is FFFFFFFFFFFF. Contrast with unicast and multicast.

Broadcast Storm

A situation in which a large number of stations are transmitting broadcast packets. This typically results in severe network congestion. This problem is usually a result of a misconfiguration.

Bus Topology

A bus topology is a network architecture in which all of the nodes simultaneously receive network traffic. Ethernet is a bus topology.

Byte

A collection of bits. A byte usually contains 8 bits.

Characteristic impedance

Characteristic impedance is the opposition (resistance and reactance) to signal propagation on a cable. It depends on the physical properties of a cable, which are determined at the time of manufacture. Manufacturing variations can cause slight differences in characteristic impedance for the same cable type.

Client

A client is a computer that makes requests of a server. A client has only one user; a server is shared by many users.

Collision

A collision is the result of two or more nodes transmitting at the same time. Excessive collisions are most often caused by a problem with the physical media.

Crossed Pair

A wiring error in twisted pair cabling in which a pair on one connector of the cable is wired to a different pair on the other end of the cable.

Crosstalk

Crosstalk is electrical interference generated by signal coupling between wires in a multiwire cable.

CSMA/CD (Carrier Sense, Multiple Access with Collision Detection)

In CSMA/CD, each node or station has equal access to the network. Before transmitting, each station waits until the network is not busy. Since each node has equal access to the network, a collision (two stations transmitting at the same time) can occur. If a collision occurs, the affected nodes will wait a random time to retransmit. Ethernet uses the CSMA/CD access method.

dBm

Decibels below 1 mW (1 milliwatt). The logarithmic measure of the ratio of the output power of a signal to an input signal of 1 mW.

DECnet

Digital Equipment Corporation's set of communication protocols for networking computers.

Destination Address

The address of the station receiving a frame.

DNS

Domain Name Services provides a mechanism that allows users to remember logical machine names rather than IP addresses. DNS provides mapping between a machine name (e.g., www.fluke.com) and its IP address (e.g., xxx.xxx.xxx.xxx).

EIA568

Electronic Industries Association Commercial Building Telecommunications Wiring Standard. Specifies maximum cable lengths, installation practices, and performance specifications for generic building wiring.

Encapsulation

Encapsulation is the method of placing one protocol into another protocol’s format. For example, in a Novell Ethernet environment there are four different methods to encapsulate IPX in Ethernet/802.3 frames: 802.3 raw, 802.2, Ethernet II, and SNAP.

Ethernet

Ethernet is a 10 Mbps topology that runs over thick coax, thin coax, twisted-pair, and fiber-optic cabling systems.

EtherTalk

EtherTalk is the AppleTalk network protocol running over the Ethernet network transport.

Fast Ethernet

Industry standard terminology for 100Base-T. Industry groups do not agree on using the term to refer to 100VG-AnyLAN; some call 100VG-AnyLAN a Fast Ethernet technology while others do not.

FCS (Frame Check Sequence)

A field transmitted in LAN frames that encodes error checking information.

Frame

A frame is a unit of data transmission divided into groups of bits. The header and a check sequence form the frame.

Full-Duplex

10Base-T and 100Base-TX network operation using a switching Hub to establish a point-to-point connection between LAN nodes that allows simultaneous sending and receiving of data packets. Full-duplex performance is twice that of half-duplex performance. A 10Base-T full-duplex network is capable of 20 Mb/s data throughput, while a full-duplex 100Base-TX network is capable of 200 Mb/s throughput.

Ghost

Energy (noise) detected on a cable that appears to be a frame but that has an invalid beginning-of-frame pattern. Must be at least 64 bytes long.

Half-Duplex

Network operation is one direction at a time only; either sending or receiving data packets, but not both at the same time.

Hops

Most commonly defined as the number of routers traveled by a frame to reach its destination.

Hub (Repeater)

Today, most often referred to in 10BASE-T networks. A 10BASE-T Hub is essentially a multiport repeater Hub with each segment dedicated to a single 10BASE-T connection.

ICMP (Internet Control and Message Protocol)

A communication protocol used by every device that uses IP. ICMP reports errors that occur during the delivery of packets on the network.

IP (Internet Protocol)

IP is the network layer protocol for the TCP/IP suite.

IP Address

An IP address is a series of four numbers separated by dots ("."), each of which is between 0 and 255. An IP address must be unique to a machine or the network will not be able to properly deliver network information to that machine. The address is made up of a network number, a subnet number, and a node number.

IP Network Number

The network number consists of the first two numbers of a device IP address on a network.

IPX (Internetwork Packet Exchange)

IPX is the network layer protocol for Novell's NetWare protocol suite.

Jabber

A frame greater than the maximum legal size (greater than 1518 bytes) with a good or bad frame check sequence. In general, you should not see jabbers. The most likely causes of jabbers are a faulty NIC/driver or perhaps a cabling problem.

Jitter

Variability in latency, or delay. If a network provides varying levels of latency (i.e., different waiting times) for different packets or cells, it introduces jitter, which is particularly disruptive to audio communications because it can cause audible pops and clicks.

LAN (Local Area Network)

A physical network technology used over short distances (up to a few thousand meters) to connect many workstations and network devices using a communication standard (Token Ring or Ethernet, for example).

Late Collision

A collision that occurs after the first 64 bytes in a frame. In 10BASE-T networks, late collisions will be seen as frames with a bad FCS. Causes of Late Collisions are a faulty NIC or a network that is too long. A too-long network is one in which the end-to-end signal propagation time is greater that the minimum legal sized frame.

Layer

One of seven levels in the Open Systems Interconnection (OSI) reference model. See OSI.

Link Pulse

A single-bit test pulse that is transmitted at least every 150 milliseconds during idle periods on 10BASE-T link segments to verify link integrity.

Manufacturer Prefix

The standard partial address used to identify a particular manufacturer. The prefix of the address is predefined uniquely for each manufacturer, while the remainder of the address uniquely identifies the station.

Master Browser

The Master Browser maintains the browse list, a list of all servers in the master browser’s domain or workgroup.

MBPS

Millions of bits per second. See BPS.

Multicast

Packets that are directed to a group of nodes rather than to a single node or all nodes. Contrast with unicast and broadcast.

NEXT

Near-end crosstalk; crosstalk between two twisted pairs measured at the same end of the cable as the disturbing signal source.

NIC (Network Interface Card)

A network interface card is the adapter card that plugs into a computer to provide a network connection.

Node Number

Node number identifies the device of interest.

NVP (Nominal Velocity of Propagation)

The speed that a pulse travels along a cable, expressed as a percentage of the speed of light in a vacuum.

Packet

A group of bits in a defined format, containing a data message that is sent over a network.

Ping

Packet Internet Groper (ping) is a common method of accessing devices on a network to see if they are active. Ping sends a packet from one device, attempts to “bounce” it off another device, and “listens” for a reply. A successful ping indicates that the network path to that device (including the routers in between) are up and functioning.

Protocol

A “language” that a device uses to communicate on a network. Examples of protocols are: TCP/IP or AppleTalk.

Primary Domain Controller

A device that manages the common security policy and user account databases for a group of NetBIOS servers. The election protocols are such that the primary domain controller has a tendency to become the master browser.

Remote Collision

A collision that occurs on the other side of a repeater. Since a 10BASE-T Hub is a multi-port repeater with a "segment" dedicated to each station, 10BASE-T collisions are remote collisions.

Repeater

A repeater is a layer-1 device that regenerates and retimes frames.

Router or Gateway

A router is a device that connects subnets together. Any packets destined for a device on a different subnet are given the subnet’s router. Routing between subnets can involve multiple routers. A user’s machine must be configured to know the IP address of the router for its subnet in order to communicate with machines on other subnets. Mis-identified gateways are a common problem for manually configured IP settings.

RJ-45 Connector

A modular connector used for UTP wiring. The RJ-45 connector has eight conductors to accommodate four pairs of wires, and it has become the dominant connector used in Ethernet and Token Ring UTP installations.

Router

A router is a network-layer device that connects networks using like network-layer protocols. Routers can span different network topologies. For example, a router can interconnect two IP subnets. For a router to pass traffic, unlike a bridge, it must be configured for the desired protocol. Routers are more difficult to configure but offer greater security.

RTP (Real-time Transport Protocol)

The protocol used for actual Voice data transmission.

RTCP (Real-time Transport Control Protocol)

A protocol that provides insight on the performance and behavior of the RTP media stream.

Runts

Typically defined as an Ethernet frame which is less than 64 bytes. Depending on what device is counting the runts, the frame check sequence may be good or bad.

SAP (Service Advertising Protocol)

A NetWare protocol used to request and broadcast information about file servers, print servers, and other services on a network.

SCCP (Skinny Client Control Protocol)

A Cisco proprietary VoIP control protocol that is used for control communications with the Cisco Call Manager.

Shorts or Short Frame

A frame less than the minimum legal size (less than 64 bytes) with a good frame check sequence. In general, you should not see Short Frames. The mostly likely cause of a Short Frame is a faulty adapter card or driver.

Signal/Noise Ratio

The ratio of worst-case received signal level to noise level measured at the receiver input (expressed in dB). The S/N ratio may be expressed as NEXT(dB) - Attenuation(dB), provided idle channel background noise is low. Higher S/N ratios provide better channel performance.

SIP (Session Initiation Protocol)

A text-based, IP-based protocol that is used for initiating a unicast session or for initiating and controlling a multicast session.

SNAP (Subnetwork Access Protocol)

An IP protocol that is an extended version of the IEEE LAN logical link control (LLC) frame. SNAP provides access to additional protocols and allows vendors to create their own protocol sub-types.

SNMP (Simple Network Management Protocol)

Designed by the Department of Defense and commercial TCP/IP implementers, SNMP is part of the TCP/IP protocol suite. SNMP operates on top of the Internet Protocol and can manage virtually any network type.

Source Address

The address of the station originating a frame.

Split Pair

The error of using wires from two different twisted pairs. This error cancels the crosstalk elimination characteristics of twisted pair wiring and produces crosstalk. Use a single twisted pair for Transmit and another twisted pair for Receive to minimize crosstalk.

Subnet

A subnet is a section of the TCP/IP network. Each subnet has a unique subnet number and is connected to a router, which enables connection to other subnets.

Subnet Number

The subnet number is programmed into the subnet router and follows the network number in an IP address.

TCP/IP (Transmission Control Protocol/Internet Protocol)

TCP/IP is the protocol suite originally developed by the Advanced Research Projects Agency (ARPA) to interconnect a research network. It later evolved into the Internet. The TCP/IP is an open standard not owned by any particular organization. The term TCP/IP is often used to refer to the entire suite of related protocols that includes IP, FTP, Telnet, RIP.

Topology

Topology is the organization of network components. The topology of Token Ring network components is a ring.

Transport

Transport refers to the physical method by which data is transmitted (e.g., Ethernet, Token Ring, etc.). Different physical network hardware and cable layout are required for different transports.

Transceiver

In Ethernet networks, a transceiver is used to couple electrical signals to and from an adapter to the transmission media. In ThinLAN and 10BASE-T networks, the transceiver is integrated directly onto the network adapter card.

Twisted Pair

A pair of wires that is twisted together to minimize crosstalk. Crosstalk is minimized with twisted pair wiring by canceling the magnetic fields generated in each of the twisted wires. Twisted pair cable (UTP or STP) is typically made up of several twisted pairs of wires.

Unicast

Packets that are directed to a single node. Contrast with broadcast and multicast.

Uptime

The amount of uninterrupted time that a resource (such as a print server) has been available.

UTP (Unshielded Twisted Pair)

Cable that is twisted by pairs but not shielded. This minimizes crosstalk by canceling the magnetic fields generated in each of the twisted wires, but only when a single twisted pair is used for Transmit or Receive.

VoIP (Voice over Internet Protocol)

The technology used to transmit voice conversations over a data network using the Internet Protocol.

Index